CAJA DE PREVISIÓN SOCIAL MUNICIP
Vigencia: 2024
Folios: 1
Anexos: 0
Radicado No.: Radicado No.: 0000690
Fecha de Radicado: 03/DIC/2024 08:00 AM
Remitente: Control Interno - Leon Villalba Nubia Esther
Destinatario: Oficinas: 100,300,400
Asunto: Informe
Radicador: JANNETH

ALCALDÍA DE BUCARAMANGA
Caja de Previsión Social Municipal

COMUNICACIÓN

FECHA: Bucaramanga, noviembre 29 de 2024

PARA: Dra. SONYA ALEJANDRA SERRANO RUEDA
Directora General

Dra. ADRIANA ALEXANDRA CARREÑOSANCHEZ
Subdirectora Administrativa

DE: NUBIA ESTHER LEON VILLALBA
Jefe Oficina de Control Interno

ASUNTO: INFORME DE SEGUIMIENTO A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DEL 1 DE ENERO AL 31 DE OCTUBRE DE 2024.

Cordial saludo:

Con mi atento saludo, remito a su despacho, el informe de seguimiento realizado por la Oficina de Control Intemo, a la Seguridad y Privacidad de la Información del 1 de enero al 31 de octubre de 2024, el cual genero el siguiente reporte:

CONCLUSIONES Y RECOMENDACIONES:

Recomendación:

Se sugiere continuar con el monitoreo continuo de la seguridad y privacidad de la información, para detectar accesos no autorizados, manipulaciones de datos o comportamientos sospechosos en tiempo real que permitan detectar incidentes en la tecnología de la información con el propósito de tomar las medidas correctivas necesarias para su protección.

Conclusión:

Una vez realizado el seguimiento a la seguridad y privacidad de la información, se concluye que la Caja de Previsión Social Municipal, cumple de manera adecuada con los lineamientos establecidos en su política de seguridad de la información, implementando un entorno seguro y robusto para la gestión de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos, este compromiso se alinea con el cumplimiento de los objetivos misionales de la CPSM, garantizando la protección de la información y

fortaleciendo la confianza de los afiliados y comunidad en general en los procesos informativos.

El Informe será publicado en la página web de la entidad.

Cordialmente,

NUBIA ESTHER LEON VILLALBA
Jefe de Oficina de Control Interno

INFORME DE SEGUIMIENTO A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

OFICINA PRODUCTORA	SUBDIRECTORA ADMINISTRATIVA
FECHA	NOVIEMBRE 29 DE 2024
PROCESO	SEGUIMIENTO A LA SEGURIDAD Y PRIVACIDAD DE INFORMACION.
PERIODO	DEL 01 DE ENERO AL 31 DE OCTUBRE DE 2024

1. INTRODUCCIÓN:

El Modelo de Seguridad y Privacidad de la Información (MSPI) enmarcado en el Sistema de Gestión de Seguridad de la información, protege preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad de la información que opera mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales reglamentarios, esenciales para el funcionamiento de la entidad.

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 31 de octubre de 2024.

4. MARCO NORMATIVO:

Ley 87 de 1993 Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado.

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 Publica Nacional y se dictan otras disposiciones.

Ley 1978 de 2019. Por la cual se moderniza el sector de las Tecnologías de la información y las comunicaciones TIC, se distribuyen competencias, se crea un regulador único 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

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:

5.1.1 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

5.1.2 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.

5.1.3 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.

5.1.4 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:

5.2.1 Accesos no autorizados: Uso indebido de credenciales por parte de terceros o internos malintencionados.

5.2.2 Ataques cibernéticos: Como Malware, Ransomware, phishing y ataques de denegación de servicio (DDoS).

5.2.3 Fallos en la infraestructura tecnológica: Hace referencia a la Vulnerabilidad derivada de configuraciones inseguras o desactualización del software.

5.2.4 Riesgo en la protección de datos personales: Hace referencia a las posibles amenazas y vulnerabilidades que puedan comprometer la privacidad y la seguridad de los datos personales almacenados procesados o transmitidos al sistema.

5.3 Monitoreo realizado por el área de sistemas:

Se realiza monitoreo continuo con herramientas automatizadas para identificar vulnerabilidades y anomalías en la infraestructura tecnológica (antivirus), para lo cual utiliza el software Karspersky es una licencia vigente que se renueva anualmente.

Se brinda asesoría para reaccionar ante cualquier ataque cibernético que se presente específicamente con posibles ataques de Phishing, relacionadas con correos mal intencionados y la forma como se puede dar solución a estos incidentes.

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:

5.5.1 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.

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

5.6 Estado actual de la privacidad de la información

En Este apartado se centra en la privacidad de la información gestionada por la entidad, con énfasis en la protección de los datos personales, y contiene los siguientes puntos:

5.6.1 Protección de Datos Personales:

5.6.2 Tipo de Datos Manejados: Información de la entidad, que es pública y privada que se encuentra en la página web y en cada uno de los equipos de las dependencias datos financieros que son públicos ubicados en la página web y los privados que son manejadas por la dependencia financiera., históricos laborales son datos privados que se encuentran reservados en el archivo digital y físico de la entidad

5.6.3 Políticas Vinculadas: Adopción de políticas de privacidad y tratamiento de datos en concordancia con la Ley 1581 de 2012.

5.6.4 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.

5.7 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 31 de octubre de 2024 se registró 0 incidentes.

5.8 Capacitaciones:

En el periodo comprendido entre el 1 de enero al 31 de octubre de 2024, la CPSM realizo a los funcionarios de la entidad, las siguientes capacitaciones:

5.8.1 Capacitación seguridad de la información:

Relacionadas con la identificación y mitigación de riesgos en especial sobre que es el Phishing y porque es importante reconocerlo para evitar que los funcionarios sean víctimas del mismo.

5.8.2 Modelo MGGTI, actualización de políticas y formatos TICS, presentación Intranet y diagnostico de IPV4 a IPV6.

En el cual se socializo y se aprobó el Modelo de Gestión de Tecnología de Información (MGGTI), que tiene como objetivo mejorar la administración y eficiencia de los recursos tecnológicos de la municipalidad asegurando que los procesos sean estandarizados y optimizados.

Estas capacitaciones se encuentran evidenciadas y firmada por cada uno de los participantes en las Actas No. 19 del 26 de octubre de 2024 y Acta No.042 del 28 de junio de 2024.

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

De acuerdo al ultimo seguimiento de Riesgos de Gestión, Corrupción y Seguridad de la información realizado en el trimestre de mayo a agosto de 2024, se obtuvieron los siguientes resultados.

Tipo de Riesgo	Descripción del Riesgo	Acciones Preventivas	Observación
GESTIÓN	Perdida de Información Física y Digital.	Solicitud a la oficina TIC acciones preventivas tomadas o a tomar para garantizar la salvaguarda de la información.	En este trimestre En cuanto al posible riesgo "Perdida de Información Física y Digital", de acuerdo al cronograma de backups, se programaron 5 copias de seguridad Una copia de seguridad para el equipo de la profesional de calidad y otra copia de seguridad para el equipo del profesional de sistemas y tres copias de seguridad a correos corporativos de sistemas, financiero, y gestión de calidad de correos. La Valoración del Riesgo tiene una probabilidad BAJA.
GESTIÓN	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	En este trimestre 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 48 publicaciones de contenidos solicitados por medio de correo electrónico a las diferentes áreas de la institución. También se han realizado actualizaciones puntuales a la página web, toda modificación que se realiza se descarga una copia de seguridad de la página web y se encarpeta a nivel digital local; para el siguiente periodo se realizara control físico de las publicaciones. La evaluación del Riesgo tiene una Probabilidad BAJA.
GESTIÓN	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	Para mitigar el riesgo del uso de los equipos que puedan afectar software, hardware, acceso a internet de las diferentes plataformas, la entidad periódicamente hace revisiones del estado actual del antivirus que se encuentra instalado en cada uno de los equipos, así como el estado de cada uno de ellos. Teniendo en cuenta que su evaluación es anual, existe un avance del 70%, ya que los equipos cuentan con antivirus y los equipos de cómputo se encuentran en buen estado. La valoración del riesgo es BAJA
GESTIÓN	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.	En aras de mitigar el riesgo de pérdida de disponibilidad de los sistemas de información, la entidad realizo una adecuación a la infraestructura física: cableado, racks, servidor, computadores, en las nuevas instalaciones donde opera la CPSM, por lo tanto se considera que la probabilidad de riesgo es BAJA, y el avance de cumplimiento es del 100%
	Pérdida de Confidencialidad de la información almacenada y gestionada en los sistemas de información de la entidad por parte de los exfuncionarios de la	Revisar de manera periódica y actualizar (si es necesario) los accesos a	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

GESTIÓN	Entidad	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.	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 cuanto a la "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" , el ing. de Sistemas recibe vía correo electrónico las solicitudes para publicar en la página web de las distintas áreas de la CPSM,. El funcionario envía documento a subir y link de la página donde debe ir alojado. El ingeniero de sistemas realiza las actualizaciones solicitadas por el funcionario y le responde vía correo electrónico con la evidencia de la publicación realizada, se está creando un formato para llevar un control el cual quedara como evidencia de la información que solicitara para la publicación en la página web. La valoración del Riesgo tiene probabilidad BAJA

6. CONCLUSIONES Y RECOMENDACIONES

Recomendación:

Se sugiere continuar con el monitoreo continuo de la seguridad y privacidad de la información, para detectar accesos no autorizados, manipulaciones de datos o comportamientos sospechosos en tiempo real que permitan detectar incidentes en la tecnología de la información con el propósito de tomar las medidas correctivas necesarias para su protección.

Conclusión:

Una vez realizado el seguimiento a la seguridad y privacidad de la información, se concluye que la Caja de Previsión Social Municipal, cumple de manera

adecuada con los lineamientos establecidos en su política de seguridad de la información, implementando un entorno seguro y robusto para la gestión de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos, este compromiso se alinea con el cumplimiento de los objetivos misionales de la CPSM, garantizando la protección de la información y fortaleciendo la confianza de los afiliados y comunidad en general en los procesos informativos.

NUBIA ESTHER LEON VILLALBA
Jefe de Oficina de Control Interno.