CAJA DE PREVISION SOCIAL MUNICIPAL DE BUCARAMANGA

POLÍTICA DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

SUBDIRECCIÓN ADMINISTRATIVA - SISTEMAS

TABLA DE CONTENIDO

INTRODUCCIÓN

La política de privacidad y seguridad de la información de la Caja de Previsión Social Municipal de Bucaramanga está basada en las definiciones, recomendaciones y 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. Además de la política de Seguridad Digital y continuidad del servicio. 2. ALCANCE El Plan de Seguridad y Privacidad de la Información establece los lineamientos para fortalecer la seguridad de la información de los usuarios de la Caja de Previsión Social Municipal de Bucaramanga, mediante la identificación de los activos de información, la identificación de los riesgos, la valoración de riesgos y la implementación de controles para mitigar los mismos, buscando garantizar los principales objetivos de la seguridad informática como son: la Integridad, Confidencialidad y Disponibilidad de la información 3. OBJETIVO Definir las estrategias de protección de la información de los usuarios de la Caja de Previsión Social Municipal de Bucaramanga, mediante el uso de estándares, políticas y recomendaciones del Sistema de Gestión de Seguridad de la Información.

POLITICA GENERAL SEGURIDAD Y PRIVACIDAD DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES DE LA CAJA DE PREVISIÓN SOCIAL MUNICIPAL DE BUCARAMANGA

La Caja de Previsión Social Municipal de Bucaramanga acoge la implementación del modelo de privacidad y seguridad de la información con el objetivo principal de preservar sus activos de información, mediante el uso de las buenas prácticas y recomendaciones de las normas vigentes que le permitan asegurar la privacidad, confidencialidad, integridad, disponibilidad y la autenticidad de la información.

DEFINICIONES (MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MIN TIC - DEFINICIONES [ISO 27000:2013]):

• Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.
• Activo crítico: Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectaran el cumplimiento de los objetivos estratégicos del Ministerio.
• Administración de Riesgos: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y deberá llevarse a cabo en forma periódica.
• Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.
Análisis de Impacto al Negocio: Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en

un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.

• Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

• Centro de cableado: El centro de cableado es el lugar donde se ubican los recursos de comunicación de Tecnología de información, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos).

• Ciberactivo crítico: Ciberactivo que es crítico para la operación de un activo crítico.

• Ciberactivo: Se identifica como foco de la ciberseguridad los activos digitales como datos, dispositivos y sistemas que permiten a la organización cumplir con sus objetivos de negocio.

• Ciberseguridad: Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

• Comité de Seguridad de la Información: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Ministerio, destinado a apoyar el cumplimiento de las normas, procesos y procedimientos de seguridad de la información.

• Confiabilidad de la Información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

• Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

• Datacenter: Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.

• Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
• Dispositivos móviles: Equipo celular smartphone, equipos portátiles, tablets, o cualquiera cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.
• DMZ: Sigla en inglés de DeMilitarized Zone hace referencia a un segmento de la red que se ubica entre la red interna de una organización y la red externa o internet de VPN.
• Equipos activos de red: Son todos los dispositivos que hacen la distribución de las comunicaciones a través de la red de datos.
• Evaluación de Riesgos: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la entidad.
• Incidente de Seguridad: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.
• Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
• Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
• Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad.
• Medio removible: Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente. Los dispositivos móviles más comunes son: Memorias USB, Discos duros extraíbles, DVD y CD.

• Mesa de Servicios: Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de Servicios que la Oficina de Tecnologías de la Información recolecta las necesidades que tienen dependencias en cuanto a los recursos tecnológicos.
• No repudio: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.
• Paneles de conexión (patch panel): Elemento encargado para la organización de conexiones en la red.
• Plan de Continuidad de Negocio: Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.
• 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.
•Propietario del riesgo: Persona o proceso con responsabilidad y autoridad para gestionar un riesgo.
• Protección a la duplicación: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
• Oficial de Seguridad de la información: Es la persona que cumple la función de supervisar el cumplimiento de la Política, coordinar el Comité de Seguridad de la Información y de asesorar en la materia a los integrantes de la entidad que así lo requieran.
• Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
• Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados

procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso del Ministerio.

• Tecnologías de la Información: Las tecnologías de la información y las Comunicaciones - TIC, Nuevas Tecnologías de la Información y de la Comunicación - NTIC, agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, internet y telecomunicaciones.

• Test de penetración: Es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables.

• VPN: Red virtual privada por sus siglas en ingles Virtual Private Network.

• Alta Dirección: Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad (Ministro, Viceministros, Secretaria General y Direcciones).

• Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

• Cifrado: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

• Control: Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

• Control Correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

• Control Detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

• Control Disuasorio: Control que reduce la posibilidad de materialización de una amenaza, por ejemplo, por medio de avisos disuasorios.

• Control Preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.
• Código malicioso: Es un código informático que crea brechas de seguridad para dañar un sistema informático.
• Dato Personal: Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables. Debe entonces entenderse el "dato personal" como una información relacionada con una persona natural (persona individualmente considerada).
• Dato Personal Público: Toda información personal que es de conocimiento libre y abierto para el público en general.
• Dato Personal Privado: Toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general.
• Dato Semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general.
• Datos Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así´ como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
• Evento: Es el suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.
• Evento de Seguridad de la Información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una

situación desconocida previamente que puede ser pertinente a la seguridad.

• Fiabilidad: Se define como la probabilidad de que un bien funcione adecuadamente durante un período determinado bajo condiciones operativas específicas (por ejemplo, condiciones de presión, temperatura o velocidad).

• Impacto: Resultado de un incidente de seguridad de la información.

• Partes interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

• Privacidad de la información: El derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

• Terceros: Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad.

• Teletrabajo: Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.

• Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

POLÍTICA DE PRIVACIDAD

Esta política contempla la protección de los datos y la confidencialidad de la información, de todos los usuarios que ingresan de forma voluntaria en los formularios dispuestos en la página web de la Caja de Previsión Social Municipal de Bucaramanga. El sitio web de la Caja de Previsión Social Municipal de Bucaramanga cuenta con un certificado SSL, el cual garantiza el intercambio seguro de información, transportando los datos de forma encriptada de extremo a extremo. La Caja de Previsión Social Municipal de Bucaramanga, cuenta con una política de confidencialidad y protección de la información de sus clientes y usuarios. Si bien el sitio web de la Caja de Previsión Social Municipal de Bucaramanga posee un sistema de protección de la información que se registra, ninguna transmisión por Internet puede garantizar su seguridad al 100%. Por esta razón, no se puede garantizar que la información ingresada en el sitio web o transmitido en él, sea completamente segura, con lo cual el usuario debe tomar sus medidas de prevención. además se pide tener en cuenta las siguientes recomendaciones:

RECOMENDACIONES PARA EL USO SEGURO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Evitar el uso de redes wifi públicas No utilice este tipo de redes públicas si no son confiables. Evite su uso para servicios que requieran información sensible, como por ejemplo la realización de transacciones bancarias o compras, dado que delincuentes pueden emular una red pública para tener acceso a sus datos. Realizar copias de seguridad de la información almacenada Es recomendable realizar periódicamente copias de seguridad de la información almacenada en su dispositivo (como contactos, fotos, notas). Puede usar servicios de almacenamiento en la nube. Evite registrar información sensible como contraseñas en forma de recordatorios o mensajes de texto y configure servicios que tenga su dispositivo para facilitar su recuperación en caso de pérdida, o efectuar el borrado remoto

de datos de ser necesario. CONSEJOS PARA MANEJO DE CORREO ELECTRÓNICO Cerrar sesión cada vez que deje de usar su correo electrónico Es recomendable cerrar sesión cada vez que haya terminado su trabajo en su aplicación de correo electrónico. Cualquier persona podría cambiar los accesos a su cuenta o utilizar su correo con fines malintencionados. Use contraseñas seguras Lo recomendable es que tener una contraseña segura, que no sea fácilmente asociada a usted y que combine en lo posible números, letras y símbolos. En correos masivos utilice Con Copia Oculta (CCO) A la hora de enviar un mensaje a muchos contactos utilice el envío en copia oculta (CCO), de esta manera se protegen las direcciones de los destinatarios.

El sitio web de la Caja de Previsión Social Municipal de Bucaramanga, se reserva el derecho de modificar las la presente política de seguridad de la información, con lo cual podrá ser adaptarla a nuevos requerimientos legislativos o técnicos que le permitan brindar mejores y oportunos servicios y contenidos informáticos, por lo cual se aconseja revisar estas normas periódicamente. La información proporcionada por los usuarios en el sitio web de la Caja de Previsión Social Municipal de Bucaramanga, estará encriptada en su proceso de transferencia mediante el uso del certificado SSL y protegida en su buen uso y administración por los acuerdos de confidencialidad de la entidad. En cuanto a la información de las PQRSD, La entidad recopila únicamente aquella información personal que sea necesaria, y de esta manera poder responder las mismas de forma oportuna y acertada. Confidencialidad de la Información El sitio de la Caja de Previsión Social Municipal de Bucaramanga no compartirá, ni revelará la información confidencial con terceros, excepto que tenga expresa autorización de quienes se suscribieron, o cuando ha sido requerido por orden judicial o legal, o para proteger los derechos de propiedad intelectual u otros derechos de la entidad. Aceptación de los Términos Esta declaración de Confidencialidad y Protección de Datos está sujeta a los términos y condiciones del sitio web, con lo cual constituye un acuerdo legal entre el usuario y la entidad. El usuario que utiliza los servicios del sitio

web, ha leído, entendido y aceptado los términos antes expuestos. Si no está de acuerdo con ellos, tiene la opción de no proporcionar ninguna información personal, o de no utilizar los servicios de nuestra página web. La caja de Previsión social Municipal de Bucaramanga también cuenta con un plan de seguridad y privacidad de la información, el cual puede ser consultado en: https://www.portalgov.cpsmbga.gov.co/politicas/

CONTROL DE DOCUMENTOS

FECHA	RESPONSABLE	CAMBIO	VERSIÓN	ARCHIVO
2023/06/30	Sistemas	Emisión Inicial	1.0	Red Interna