PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2025

CONTRALORÍA MUNICIPAL
BARRANCABERMEJA

DANNY MARCELA GOMEZ PUERTA
Contralora Municipal de Barrancabermeja

Barrancabermeja, enero 2025

INTRODUCCIÓN

En la actualidad los sistemas informáticos no son totalmente seguros es por este motivo que se hace necesario la implementación de procedimientos, estrategias y políticas para mitigar los posibles riesgos.

La Contraloría Municipal de Barrancabermeja, a través de la definición de su PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025, tendrá la oportunidad al interior de la Entidad de adoptar los lineamientos de la Gestión de TI del Estado Colombiano, desarrollar su rol estratégico al interior de la CMB, apoyar las áreas misionales mientras se piensa en tecnología, liderar las iniciativas de TI que deriven en soluciones reales y tener la capacidad de generar transformaciones en el sector, como parte de los beneficios que un plan estratégico de TI debe producir una vez se inicie su ejecución.

En este sentido, las políticas de seguridad informática, definidas en este documento para la Contraloría Municipal de Barrancabermeja, surgen como una herramienta organizacional para concientizar a cada uno de los funcionarios de la entidad, sobre la importancia y sensibilidad de la información y servicios críticos.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1.1 Objetivo

Establecer los lineamientos básicos que permitan mantener en óptimas condiciones de funcionamiento los recursos de TI (tecnología informática: equipos de cómputo, software, información, entre otros) asegurando el control y seguridad de la información.

- Controlar y soportar los recursos de datos de cómputo, software y hardware en la entidad, buscando una adecuada administración ante las amenazas técnicas, físicas, tecnológicas y de inoperancia que las afecta

1.2 Propósito

Establecer los lineamientos que en materia de seguridad informática requiera la Contraloría Municipal de Barrancabermeja y formular políticas, estrategias y parámetros necesarios para evitar vulnerabilidades que afecten los Sistemas de Información.

1.3 Alcance

Las políticas definidas el presente documento aplican a todos los funcionarios públicos, contratistas, personal temporal y otras personas relacionadas con terceras partes que utilicen recursos informáticos de la Contraloría Municipal de Barrancabermeja. Estos lineamientos están dados para proteger la información y los recursos tecnológicos, así como su recuperación con el fin de responder a los requerimientos de los procesos de la entidad.

1.4 Normatividad

- Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 de2013: Por la cual se dictan disposiciones generales para la protección de datos personales.

- Decreto 2578 de 2012: Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye "El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles" entre otras disposiciones.

- Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.

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

- Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

- Decreto 2573 de 2014: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea.

- Decreto 767 de 2022, Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2

del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, 16/05/2022

- Resolución 1519 de 2020, Por la cual se definen los estándares y directrices para publicar la información señalada por la ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos, 24/08/2020

- Resolución 500 de 2021, Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital, 10/03/2021

1.5 Definiciones

Activo: Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Aplicaciones críticas: Son las aplicaciones o sistemas de información que reciben este término porque previamente se encuentran clasificados como vital o necesarias para el buen funcionamiento de los procesos y procedimientos misionales.

Brecha: Término que se utiliza para denominar la diferencia que se observa entre el mecanismo de seguridad que existe y la situación ideal para evitar que germinen vulnerabilidades que impacten en la Entidad.

Buenas prácticas: Son lineamientos que contiene los principios básicos y generales para el desarrollo de los productos o servicios de la organización para la satisfacción al cliente.

Ciclo de vida de la información digital: Se refiere a la clasificación y almacenamiento de la información; siendo necesario tener en cuenta los requisitos técnicos y legales; así como tener claro los conceptos de disponibilidad y velocidad que depende de la misma clasificación que varía conforme su valor con el tiempo.

Clasificación de las aplicaciones: Las aplicaciones se clasifican conforme los procesos de la entidad y son: Misional, Estratégico y de Apoyo.

Clasificación de la información: Proceso formal que se utiliza para ubicar el nivel a la información de la Entidad con el fin de protegerla; previa estructura de valoración en atención al riesgo que se presume existe si hay una divulgación no autorizada. Generalmente la información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.

Clientes: Persona natural o usuario que recibe un producto Institucional. El cliente puede ser interno o externo a la organización.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.

Corriente eléctrica regulada: Se utiliza para regular o mantener el voltaje de la red eléctrica para que no afecte el funcionamiento de los recursos TIC de la Entidad.

Dato: Es una letra, número o símbolo que tiende a convertirse en información.

Dependencias: Son los grupos que conforman la estructura organizacional de la Entidad.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

Documento: Es el medio físico que contiene la información que se quiere transmitir.

Dueño de la información: Es cualquier persona que es propietaria de la información y tiene la responsabilidad de custodiarla.

Incidente: Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa o puede causar una interrupción del mismo o reducción de la calidad del servicio.

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 que es guardada en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Información Digital: Cuando la información está almacenada en un medio magnético porque cuando se imprime se convierte en documento físico y en este último caso existe en el SGC la dependencia que define los lineamientos, normas, guías y estándares.

Información sensible: Es la tipificación que recibe la información que no se considerada de acceso público como por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. Aunque lo más común es usar este término para designar datos privados relacionados con Internet o la informática, sobre todo contraseñas, tanto de correo electrónico, conexión a Internet, IP privada, sesiones del PC, etc.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Política TIC: Documento que contiene los lineamientos que define la organización para reglamentar el desarrollo de los proyectos y recursos TIC de la Entidad, como las acciones que deben permanecer en el tiempo para alcanzar los objetivos de su negocio.

Política de seguridad: Es el documento de normas y lineamientos de seguridad de la información que define la Entidad para evitar que surja vulnerabilidades que puede afectar el negocio de la Entidad.

Procesos críticos: Concepto que se utiliza para definir el conjunto de actividades o eventos que se ejecutan bajo ciertas circunstancias que inciden en los productos misionales de la entidad y en la satisfacción de los clientes.

Proveedores: Negocio o empresa que ofrece servicios a otras empresas o particulares. Ejemplos de estos servicios incluyen: acceso a internet, operador de telefonía móvil, alojamiento de aplicaciones web etc.

Propietario de la información: Se utiliza para denominar a la persona autorizada para organizar, clasificar y valorar la información de su dependencia o área conforme al cargo de la estructura organizacional de la Entidad.

Repositorio de documentos: Sitio centralizado donde se almacena y mantiene información digital actualizada para consulta del personal autorizado.

Requerimiento: Necesidad de un servicio TIC que el usuario solicita a través de un mecanismo definido por la organización en los procedimientos normalizados.

Servicio: Incluye los servicios profesionales para la instalación, mantenimiento, desarrollo, integración de software y adquisiciones, enajenaciones, arrendamientos y contratación de Hardware y soporte tanto de software como de hardware; así como de la Plataforma Tecnológica.

- Servicios TIC: El concepto de Servicio TIC consiste en dar soporte, de forma integrada y personalizada, a todas estas herramientas que necesita hoy en día el trabajador de la empresa para realizar su trabajo. Los elementos del Servicio TIC son:

- Los dispositivos: PC, portátiles, agendas electrónicas, impresoras, teléfonos, sistemas de videoconferencia, etc.

- La Red de Área Local corporativa (LAN). Así como las comunicaciones de voz incluyendo el teléfono y ahora llega el momento de proporcionar y gestionar los PC y la electrónica de red necesarios para las comunicaciones de datos.

- Las comunicaciones de voz y datos WAN (Red de Área Extensa), que incluyen tanto las redes privadas corporativas como el acceso a redes públicas como Internet. La integración de las comunicaciones WAN y estas cada vez se requieren con las comunicaciones LAN.

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.

T.C. Conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información, en la actualidad no solo una computadora hace referencia al procesamiento de la información. Internet forma parte de ese procesamiento que, quizás, se realice de manera distribuida y remota.

El procesamiento remoto, además de incorporar el concepto de telecomunicación, hoy día hace referencia a un dispositivo como un teléfono móvil o una computadora portátil, con capacidad de operar en red mediante Comunicación inalámbrica.

Usuario: Persona que utiliza los recursos TIC y que interactúan de forma activa en un proceso, secuencia, código etc.

1.6 Condiciones Generales

Los líderes de cada proceso son los responsables de identificar, valorar y clasificar su información, dado que son estos los propietarios y generadores de los datos, por tal motivo todos los funcionarios deben seguir las políticas, estrategias y parámetros establecidos para la seguridad de la información.

1.6.1 Principios de la Seguridad de la Información

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas que estén autorizadas para tener acceso a ella.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

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.

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

Auditabilidad: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

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.

No Repudio: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

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.

1.7 Políticas de Seguridad

1.7.1 Acceso a la Información

Todos los funcionarios públicos, contratistas y pasantes que laboran para la Contraloría Municipal de Barrancabermeja deben tener acceso sólo a la Información necesaria para el desarrollo de sus actividades.

En el caso de personas ajenas a la CONTRALORÍA MUNICIPAL DE BARRANCABERMEJA, es responsabilidad del cuerpo directivo, autorizar el acceso sólo indispensable a la información y a los equipos de cómputo, de acuerdo con el trabajo realizado por estas personas, previa justificación.

Todas las prerrogativas para el uso de los sistemas de información de la entidad deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la entidad.

Terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

1.7.2 Administración de Cambios

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos. Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

1.7.3 Seguridad de la Información

Los funcionarios públicos, contratistas y pasantes de la Contraloría Municipal de Barrancabermeja son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los funcionarios públicos, contratistas y pasantes no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas.

Todo funcionario que utilice los Recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Después de que el trabajador deja de prestar sus servicios a la Entidad, se compromete entregar toda la información respectiva de su trabajo realizado. Una vez retirado el funcionario, contratistas y pasantes de la Contraloría Municipal de Barrancabermeja deben comprometerse a no utilizar, comercializar o divulgar los productos de información generada o conocida durante la gestión en la entidad, directamente o a través de terceros, así mismo, los funcionarios públicos que detecten el uso de la información están en la obligación de reportar el hecho al grupo de control interno disciplinario.

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según el caso respectivamente.

1.7.4 Seguridad para los Servicios Informáticos

El sistema de correo electrónico debe ser usado únicamente para el ejercicio de las funciones de cada competencia funcionario y de las actividades contratadas en el caso de los contratistas y pasantes.

Queda prohibida la descarga de archivos que no correspondan al trabajo realizado por cada funcionario, contratista o pasante.

En cuanto a los grupos de charla (Chat) y utilidades asociadas, queda prohibido su uso, excepto cuanto el trabajo realizado lo amerite y por ende será autorizado por el jefe de la dependencia, no obstante, la entidad cuenta con el sistema de mensajería a través de un grupo de WhatsApp, sistema que debe ser utilizado adecuadamente dentro de los horarios laborales.

La entidad se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito. Los funcionarios públicos, contratistas y pasantes no deben utilizar versiones

escaneadas de Firmas hechas a mano para dar la impresión de que un mensaje de correo electrónico o cualquier otro tipo de comunicación electrónica haya sido firmado por la persona que la envía.

La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la Entidad. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, programas de computación, códigos fuentes, documentación y otros materiales.

Los funcionarios públicos, contratistas y pasantes que hayan recibido aprobación para tener acceso a Internet a través de las facilidades de la entidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet. Al respecto el profesional universitario a cargo del área de sistemas, es y será la única persona de la entidad autorizada para subir información a la página web de la entidad, relacionada con las notificaciones de los procesos.

En cualquier momento que un trabajador publique un mensaje en un grupo de discusión de Internet, en un boletín electrónico, o cualquier otro sistema de información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la entidad.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente comunicarlo al profesional universitario encargado para atender estos casos, no utilizar el computador y desconectarlo de la red.

1.7.5 Seguridad en Recursos Informáticos

Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los funcionarios públicos, contratistas y pasantes de la Contraloría

municipales Barrancabermeja son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales. Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

Antes de que un nuevo sistema se desarrolle o se adquiera, los subdirectores, jefes de oficina, en conjunto con el funcionario encargado de asesorar la Entidad en temas de informática, deberán definir las especificaciones y requerimientos de seguridad necesarios.

La seguridad debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño de sistemas hasta la conversión a un sistema en producción.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad. En cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

1.7.6 Seguridad en Comunicaciones

Las direcciones internas (IP), topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser considerados y tratados como información confidencial y no pueden ser modificadas sin previa autorización del profesional universitario a cargo de administrar el recurso informático de la Entidad.

Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un acuerdo o documento de formalización.

Los computadores de la Contraloría Municipal de Barrancabermeja se conectarán de manera directa con computadores de entidades externas, conexiones seguras, previa autorización del profesional universitario encargado de los sistemas informáticos y de la seguridad informática.

Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la Entidad e Internet deberá estar cifrada. Este cifrado de información aplica únicamente para la información que es enviada anualmente a la Auditoría General de la República a través del SIREL, utilizando el certificado de firma digital entregado por Certicámaras, el cual consta del token y la contraseña respectiva.

1.7.7 Seguridad para Usuarios Terceros

Los dueños de los Recursos Informáticos que no sean propiedad de la entidad y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente debe definir un documento de acuerdo oficial entre las partes.

Cuando se requiera utilizar recursos informáticos u otros elementos de propiedad de Contraloría Municipal de Barrancabermeja para el funcionamiento de recursos que no sean propios de la entidad y que deban ubicarse en sus instalaciones, los recursos serán administrados por el funcionario delegado por la secretaria general de la Contraloría Municipal de Barrancabermeja.

Los usuarios terceros tendrán acceso a los Recursos Informáticos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben

ser aprobados por quien será el jefe inmediato o coordinador. La conexión entre sistemas internos de la entidad y otros de terceros debe ser aprobada y certificada por la secretaria general con el fin de no comprometer la seguridad de la información interna de la entidad.

1.7.8 Software Utilizado

Todo software que utilice la Contraloría Municipal de Barrancabermeja será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.

Todo el software de manejo de datos que utilice la Contraloría Municipal de Barrancabermeja dentro de su infraestructura informática, deberá contar con las técnicas apropiadas para garantizar la integridad de los datos.

Debe existir una cultura informática al interior de la Entidad que garantice el conocimiento por parte de los funcionarios públicos, contratistas y pasantes de las implicaciones que tiene el instalar software ilegal en los computadores de la Contraloría Municipal de Barrancabermeja.

Está prohibido el uso de software ilegal dentro de la Contraloría Municipal de Barrancabermeja, así mismo la descarga de software a través de Internet y su posterior instalación.

El funcionario encargado de administrar el recurso informático de la entidad, está autorizado para monitorear periódicamente los equipos y en los casos de encontrar software instalado no licenciado por la Entidad, levar a cabo las acciones correctivas e informar a la secretaria general las irregularidades encontradas.

1.7.9 Actualización de Hardware

Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del área responsable. La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.

Los equipos de cómputo (PC, servidores, LAN etc.) No deben moverse o re ubicarse sin la aprobación previa del profesional universitario a cargo del área involucrada.

1.7.10 Almacenamiento y Respaldo

La información que es soportada por la infraestructura de tecnología informática de la Contraloría Municipal de Barrancabermeja deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad. Las copias de seguridad se realizarán de acuerdo con los procedimientos establecidos en el manual.

El jefe del área dueña de la información, con la asesoría de la persona encargada de administrar la infraestructura computacional de la Contraloría Municipal de Barrancabermeja, definirán la estrategia a seguir para el respaldo de la información y siguiendo los lineamientos definidos en el Manual de Procesos y Procedimientos.

Los funcionarios públicos son responsables de los respaldos de su información (la información que no se encuentra en la red sino en el equipo asignado) en los computadores, siguiendo las indicaciones técnicas dictadas.

1.7.11 Contingencia

La Administración de la Entidad debe preparar, actualizar periódicamente y probar formalmente un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación.

1.7.12 Auditoría

Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la Entidad, como son sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar pistas (adición, modificación, borrado) de auditoría.

Todos los archivos de auditorías deben proporcionar suficiente información para apoyar el monitoreo, control y auditorias.

Todos los computadores de la Entidad deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria sea correcto.

1.7.13 Seguridad Física

Siempre que un trabajador se dé cuenta que un visitante no autorizado se encuentra dentro de áreas restringidas de la entidad, el visitante debe ser inmediatamente cuestionado acerca de su propósito de encontrarse en área restringida e informar a las responsables de la seguridad del edificio.

Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso. Todos los computadores, impresoras, portátiles, módems y equipos de comunicación se deben registrar su

ingreso y salida y no debe abandonar la entidad a menos que esté acompañado por la autorización respectiva del Secretaria General.

Los equipos de cómputo (PCS, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa).

Los funcionarios públicos se comprometen a no utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras, ventiladores y en general cualquier equipo que generen caídas de la energía.

Los particulares en general no están autorizados para utilizar los recursos informáticos de la entidad.

Con respecto a los familiares de los funcionarios públicos, está prohibido el uso de los equipos informáticos para uso personal, descargas de música, juegos y software variado que interrumpa el normal desempeño de las actividades de los funcionarios.

1.7.14 Escritorios y Computadores Limpios

Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD, DVD, Memorias (USB), con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

Es responsabilidad de los funcionarios públicos, contratistas y pasantes de la Contraloría Municipal de Barrancabermeja, mantener en buen estado los equipos de cómputo asignados para el desempeño de las labores diarias, igualmente se recomienda no consumir alimentos y bebidas que accidentalmente puedan ser

contaminación sobre los computadores, periféricos, documentos y otros elementos, con el fin de evitar daños irreparables en los mismos.

1.7.15 Administración de la Seguridad

La evaluación de riesgos de seguridad para los Recursos Informáticos en producción se debe ejecutar al menos una vez cada dos años. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.

Cualquier brecha de seguridad o sospecha en la mala utilización en el Internet, la red corporativa o Intranet, los recursos informáticos de cualquier nivel (local o corporativo) deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial a la Secretaria General o profesional universitario encargado de sistemas de la Entidad.

Los funcionarios públicos, contratistas y pasantes de la Contraloría Municipal de Barrancabermeja que realicen las labores de administración del recurso informático son responsables por la implementación, permanencia y administración de los controles sobre los Recursos computacionales. La implementación debe ser consistente con las prácticas establecidas de sus funciones.

Los funcionarios que realicen labores de administración del recurso informático de la Entidad, divulgarán, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará al Contralor, los casos de incumplimiento con copia a la Secretaria General y a la Oficina de Control Interno, para que estos tomen las medidas correctivas correspondientes.

1.7.16 Generales

- Todo lo no expresamente permitido está prohibido al funcionario público (Art. 6 Constitución política de Colombia).

- Toda Información Contenida, Procesada o Generada en los equipos de cómputo es propiedad de la Contraloría Municipal de Barrancabermeja.

- El usuario es el único responsable de la información contenida en el o los PC'S asignados para ello. El usuario deberá determinar el grado de importancia y el tiempo que se debe conservar la información que amerita copias de seguridad, entre esta información tenemos la siguiente: Hojas de Excel, Documentos tipo Word. Carpeta de correo personal, Manejo de contactos para correo, Software de carácter no institucional.

- Antes de realizar un Backup verifique el tamaño de los documentos a copiar y compáralo con el del medio en donde va a almacenar la copia, con el fin de determinar cuántos medios necesitará para que la copia quede completa.

- Verifique que el medio en donde va a copiar esté en buenas condiciones físicas, por ejemplo, que el CD, DVD no esté con rayones, los discos duros externos, memorias USB u otro medio externo de almacenamiento esté en buen estado y se pueda leer. De esta manera, asegura que la información posteriormente pueda ser recuperada.

- No deje visible sus contraseñas de correo, red y archivos, porque pueden ser utilizadas por otras personas alterando o dañando su información.

- No permita que personal externo opere su información, tampoco comparta sus contraseñas.

1.8 Organización de la Información

- La Contraloría Municipal de Barrancabermeja adelanta los lineamientos, guías y procedimientos para organizar, clasificar y valorar la información de la entidad.
- El líder de cada proceso debe determinar cuál es la información de carácter sensible y su disponibilidad.
- Los funcionarios de la entidad deben ubicar la información que debe ser respaldada de acuerdo a los procedimientos previamente establecidos para la realización de las copias de seguridad. En caso contrario la responsabilidad recaerá en el funcionario que omita este procedimiento al igual que la restauración de la información.
- Dentro de las obligaciones contractuales de las personas vinculadas a la entidad existe un apartado donde se establece el compromiso de confidencialidad de la información, así como el cumplimiento de las políticas de seguridad y privacidad de la información.

1.9 Clasificación de la información

- Se deben establecer y documentar los procedimientos de clasificación de la información como activo de la entidad, los cuales se basan en la seguridad, confidencialidad, integridad y disponibilidad de la información.
- Los líderes de cada proceso deben determinar cuál es la información de carácter sensible y su disponibilidad.
- Todos los líderes de los procesos deben supervisar que en su dependencia se aplique el procedimiento previamente definido en la entidad para la clasificación de la información de su competencia.

- La información clasificada por cada proceso debe ser consolidada en un solo inventario de activos de información.

2. Política de Privacidad y Seguridad Página Web de la Contraloría Municipal de Barrancabermeja.

La Contraloría Municipal de Barrancabermeja, a través de su Sitio Web, podrá solicitar información personal (en los casos que se requiera, se le hará saber). Por lo tanto, la utilización de nuestro Sitio Web supone que usted reconoce haber leído y aceptado nuestra Política de Privacidad y Seguridad que aquí se presenta.

El portal Contraloría Municipal de Barrancabermeja se compromete a proteger su privacidad y el desarrollo de tecnología que le dé la más potente y segura experiencia en línea. Esta Declaración de Privacidad se aplica al sitio Web Contraloría Municipal de Barrancabermeja y regula la recolección de datos y su uso. Al usar el sitio web Contraloría Municipal de Barrancabermeja usted da su consentimiento a las prácticas de respecto de los datos descrita en esta declaración.

2.1 PROPÓSITO

El siguiente documento es la base de la política general de seguridad y privacidad de información para la Contraloría Municipal de Barrancabermeja, como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en línea, según lo establecido en el Decreto 1078 de 2015 y la Política de Gobierno Digital es la política del Gobierno Nacional que propende por la transformación digital pública. Con esta política pública se busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública y el Estado en general, a través del uso y aprovechamiento de las TIC. Hace parte del Modelo Integrado de Planeación y Gestión - MIPG y se integra con las políticas de Gestión y Desempeño Institucional.

7.1 GLOSARIO

Política: Declaración de alto nivel que describe la posición de la Contraloría Municipal de Barrancabermeja sobre un tema específico.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la Contraloría Municipal de Barrancabermeja.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la Contraloría Municipal de Barrancabermeja, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

2.3 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección de la CONTRALORIA MUNICIPAL DE BARRANCABERMEJA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad. Para la CONTRALORIA MUNICIPAL DE BARRANCABERMEJA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la CONTRALORIA MUNICIPAL DE BARRANCABERMEJA
- Garantizar la continuidad del negocio frente a incidentes.

La CONTRALORIA MUNICIPAL DE BARRANCABERMEJA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios. Finalmente es de gran ayuda incluir la descripción

general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva. Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc., que la Entidad ha establecido como necesarias y primordiales. De esta forma se presenta el siguiente ejemplo:

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de CONTRALORIA MUNICIPAL DE BARRANCABERMEJA:

• Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

• La CONTRALORIA MUNICIPAL DE BARRANCABERMEJA protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

• La CONTRALORIA MUNICIPAL DE BARRANCABERMEJA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• La CONTRALORIA MUNICIPAL DE BARRANCABERMEJA protegerá su información de las amenazas originadas por parte del personal.

• La CONTRALORIA MUNICIPAL DE BARRANCABERMEJA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• La CONTRALORIA MUNICIPAL DE BARRANCABERMEJA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• La CONTRALORIA MUNICIPAL DE BARRANCABERMEJA implementará control de acceso a la información, sistemas y recursos de red.

• La CONTRALORIA MUNICIPAL DE BARRANCABERMEJA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• La CONTRALORIA MUNICIPAL DE BARRANCABERMEJA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

• La CONTRALORIA MUNICIPAL DE BARRANCABERMEJA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

• La CONTRALORIA MUNICIPAL DE BARRANCABERMEJA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

2.4 IMPORTANCIA DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Para las entidades es importante contar con políticas de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la entidad.

2.5 FASES DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Para realizar una correcta implementación de políticas de seguridad de la información, es necesario cumplir con una serie de fases que se sugieren en este documento, las cuales tienen como objetivo que la entidad desarrolle, apruebe, implemente y socialice e interiorice las políticas para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de la entidad.

1. Desarrollo de las políticas: En esta fase la Entidad debe responsabilizar las áreas para la creación de las políticas, estructurarlas, escribirlas, revisarlas y aprobarlas; por lo cual para llevar a buen término esta fase se requiere que se realicen actividades de verificación e investigación de los siguientes aspectos:

Identificación de la creación de política: Debe identificarse el cor qué la Entidad requiere la [illegible] política de seguridad de información y determinar el control al cual hace [illegible] implementación.

- Alcance: Debe determinarse el alcance, ¿A qué población, áreas, procesos o departamentos aplica la política?, ¿Quién debe cumplir la política?

- Roles y Responsabilidades: Se debe definir los responsables y los roles para la implementación, aplicación, seguimiento y autorizaciones de la política.

- Revisión de la política: Es la actividad mediante la cual la política una vez haya sido redactada pasa a un procedimiento de evaluación por parte de otros individuos o grupo de individuos que evalúen la aplicabilidad, la redacción y se realizan sugerencias sobre el desarrollo y creación de la misma.

- Aprobación de la Política: Se debe determinar al interior de la entidad la persona o rol de la alta dirección que tiene la competencia de formalizar las políticas de seguridad de la información mediante la firma y publicación de las mismas.

- Es importante que la Alta Gerencia de la Entidad muestre interés y apoyo en la implementación de dichas políticas.

2. Cumplimiento: Fase mediante la cual todas aquellas políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas versus los controles de seguridad implementados y documentados.

3. Comunicación: Fase mediante la cual se da a conocer las políticas a los funcionarios, contratistas y/o terceros de la Entidad. Esta fase es muy importante toda vez que del conocimiento del contenido de las políticas depende gran parte del cumplimiento de las mismas; esta fase de la implementación también permitirá obtener retroalimentación de la

efectividad de las políticas, permitiendo así realizar excepciones, correcciones y ajustes pertinentes. Todos los funcionarios contratistas y/o terceros de la entidad debe conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física de tal documento o documentos, para que sean consultados en el momento que se requieran.

4. Monitoreo: Es importante que las políticas sean monitoreadas para determinar la efectividad y cumplimiento de las mismas, deben crearse mecanismos ejemplo indicadores para verificar de forma periódica y con evidencias que la política funciona y si debe o no ajustarse.

5. Mantenimiento: Esta fase es la encargada de asegurar que la política se encuentra actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones.

6. Retiro: Fase mediante la cual se hace eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Entidad. Esta es la última fase para completar el ciclo de vida de las políticas de seguridad y requiere que este retiro sea documentado con el objetivo de tener referencias y antecedentes sobre el tema.

2.6 Recolección de su Información Personal

El portal Contraloría Municipal de Barrancabermeja recoge directamente información de identificación, como su dirección de e-mail, nombre, su dirección de trabajo o domicilio o número de teléfono. El portal web de la Contraloría Municipal de Barrancabermeja podría recoger también información demográfica anónima, que no es exclusiva de usted, como su, edad, sexo, preferencias, intereses y preferencias.

También hay información sobre el hardware y software del equipo que es automáticamente recogida por el portal Contraloría Municipal de Barrancabermeja. Esta información puede incluir: su dirección IP, tipo de navegador, nombres de dominio, tiempos de acceso y direcciones de sitios Web referidos. Esta información es utilizada por el portal Contraloría Municipal de Barrancabermeja para su funcionamiento y para mantener la calidad del servicio, y proporcionar estadísticas generales acerca del uso de sitio web Contraloría Municipal de Barrancabermeja. Por favor, tenga en cuenta que, si usted directamente revela información personal o datos sensibles a través de foros públicos del portal

de Barrancabermeja, esta información puede ser recogida y utilizada

Municipal de Barrancabermeja no lee ninguna de sus comunicaciones

Municipal de Barrancabermeja lo anima a revisar las declaraciones de privacidad de sitios Web a los que elija un vínculo a partir del portal Contraloría Municipal de Barrancabermeja para que pueda comprender cómo los sitios Web recopilan, utilizan y comparten su información. El portal no se responsabiliza de las declaraciones de privacidad u otros contenidos en sitios Web fuera del portal Contraloría Municipal de Barrancabermeja.

2.7 Uso de su Información Personal

El portal Contraloría Municipal de Barrancabermeja recopila y utiliza su información personal para operar el sitio Web Contraloría Municipal de Barrancabermeja y entregar los servicios que usted solicita. El sitio Contraloría Municipal de Barrancabermeja también utiliza su información de identificación personal para informarle de otros productos o servicios disponibles a partir de Contraloría Municipal de Barrancabermeja.

La Contraloría Municipal de Barrancabermeja también puede contactar con usted a través de encuestas para llevar a cabo investigaciones acerca de su opinión de los servicios actuales o potenciales nuevos servicios que puedan ofrecerse.

El sitio Contraloría Municipal de Barrancabermeja no vende, alquila o arrienda sus listas de clientes a terceros. Además, el sitio Contraloría Municipal de Barrancabermeja puede compartir datos con socios de confianza para que nos ayuden a realizar el análisis estadístico, enviarle e-mail, proporcionar soporte al cliente, o acordar entregas. Todos esos terceros tienen prohibido utilizar su información personal, excepto para proporcionar estos servicios a la Contraloría Municipal de Barrancabermeja, y están obligados a mantener la confidencialidad de su información.

El sitio Contraloría Municipal de Barrancabermeja no utiliza o divulga información personal confidencial, como raza, religión o afiliación política, sin su consentimiento explícito.

El sitio Contraloría Municipal de Barrancabermeja realiza un seguimiento de los sitios web y páginas que nuestros clientes visitan dentro de Contraloría Municipal de

Barrancabermeja, a fin de determinar qué servicios son más populares en el portal de la Contraloría Municipal de Barrancabermeja. Estos datos se utilizan para entregar contenido personalizado y publicidad dentro de Contraloría Municipal de Barrancabermeja a los clientes cuyo comportamiento indica que están interesados en un campo particular.

El sitio web Contraloría Municipal de Barrancabermeja no divulgará su información personal, sin previo aviso, sólo si es necesario hacerlo por la ley o de buena fe si dicha acción es necesaria para: (a) ajustarse a los decretos de la ley o cumplir con un proceso legal en el sitio Contraloría Municipal de Barrancabermeja o dentro de nuestros servidores, (b) proteger y defender los derechos o propiedad de Contraloría Municipal de Barrancabermeja, y, (c) actuar bajo circunstancias urgentes para proteger la seguridad personal de los usuarios de Contraloría Municipal de Barrancabermeja, o el público.

2.8 Uso de Cookies

El sitio Web Contraloría Municipal de Barrancabermeja utiliza "cookies" para ayudarle a personalizar su experiencia en línea. Una cookie es un archivo de texto que se coloca en el disco duro por un servidor de páginas Web. Las cookies no pueden ser utilizadas para ejecutar programas o enviar virus a su computador. Las cookies le son asignadas, específicamente y sólo pueden ser leídas por un servidor web en el dominio que emitió la cookie.

Uno de los propósitos principales de las cookies es proporcionar una característica conveniente para ahorrarle tiempo. El propósito de una cookie es decirle al servidor Web que usted ha regresado a una página específica. Por ejemplo, si usted personaliza las páginas Contraloría Municipal de Barrancabermeja, o registra el sitio Contraloría Municipal de Barrancabermeja o sus servicios, una cookie ayuda a Contraloría Municipal de Barrancabermeja a recordar su información específica en visitas posteriores. Esto simplifica el proceso de registrar su información personal, como direcciones de facturación, las direcciones de envío, y así sucesivamente. Cuando regrese al mismo sitio web Contraloría Municipal de Barrancabermeja, la información que usted brindó anteriormente puede ser recuperada, así que usted puede utilizar fácilmente las características de Contraloría Municipal de Barrancabermeja que usted personalizo.

Usted tiene la posibilidad de aceptar o rechazar cookies. La mayoría de navegadores aceptan automáticamente cookies, pero normalmente puede modificar la configuración de su navegador para rechazar las cookies si lo prefiere. Si decide rechazar cookies, es

posible que no pueda experimentar plenamente las características interactivas de los servicios de Contraloría Municipal de Barrancabermeja que personalizo.

2.9 Seguridad de su Información Personal

El sitio Contraloría Municipal de Barrancabermeja asegura su información personal de accesos no autorizados, uso o divulgación. El sitio Contraloría Municipal de Barrancabermeja asegura la información personal identificable que usted proporciona en servidores con un entorno controlado y seguro, protegido del acceso no autorizado, uso o divulgación. Cuando la información personal (como un número de tarjeta de crédito) se transmite a otros sitios Web, es protegida mediante el uso de la encriptación, como el protocolo Secure Socket Layer (SSL).

Dado que ningún sistema puede garantizar seguridad completa, se trata de mantener la información que el Usuario suministra o accede lo más segura posible, incluyendo su seguridad física en la ubicación del servidor donde la información está almacenada.

2.10 Cambios a esta Declaración

El sitio Contraloría Municipal de Barrancabermeja ocasionalmente puede actualizar esta Declaración de Privacidad para reflejar los comentarios de los clientes y la entidad. El sitio le anima a que periódicamente revise esta Declaración para estar informado de cómo protege su información.

2.11 Actualización de políticas

La política de privacidad y seguridad de la página web de la Contraloría Municipal de Barrancabermeja fue revisada en enero de 2025. Podremos modificarla periódicamente, en dicho caso comunicaremos la política modificada en nuestro Sitio Web.

2.12 Información de Contacto

El sitio Contraloría Municipal de Barrancabermeja da la bienvenida a sus comentarios con respecto a esta Declaración de Privacidad. Si usted cree que Contraloría Municipal de Barrancabermeja no se ha adherido a esta declaración, póngase en contacto con Contraloría Municipal de Barrancabermeja a info@contraloriabarrancabermeja.gov.co

3. CONFIGURACIÓN DE USUARIOS Y SEGURIDAD EN EL SERVIDOR BUFFALO DE LA CONTRALORIA MUNICIPAL

3.1 CONFIGURACIÓN DE EQUIPOS DE COMPUTO Y CUENTAS DE USUARIO:

Esta configuración consiste en unir los equipos de cómputo del instituto al dominio principal de la CONTRALORIA MUNICIPAL para regirse a los lineamientos de seguridad y privacidad del servidor de datos. Adicionalmente, entregar usuario y contraseña a los funcionarios y contratistas con equipos asignados.

3.1.1 **INSTALACIÓN DE LA CARPETA COMPARTIDA Y DEMAS CARPETAS ASIGNADAS A SUS FUNCIONES.** Se mantiene la estrategia que garantiza el almacenamiento e intercambio de la información interna en el servidor BUFFALO con acceso restringido y otorgado a cada usuario de la red, por medio del jefe de cada área SOLO a las carpetas asignadas para desempeñar sus funciones.

Se les recuerda que, en la CARPETA COMPARTIDA, no se puede almacenar información personal, sino única y exclusivamente inherente al cumplimiento de las funciones u obligaciones contractuales.

3.1.2 **CONFIGURACIÓN DE LAS UNIDADES DE RED POR AREA.** Hay mecanismos de administración de archivos para los miembros de la Red, en unidades compartidas por área o nombre de auditores que permitan compartir en tiempo real los archivos con todos los usuarios con privilegios asignados.

3.1.3 **CONFIGURACIÓN DE ACCESO AL GAT-ISSAI:** Es el *Sistema guía interno de auditorías*, diseñado para ser utilizado de forma permanente por parte de los auditores,

director técnico de fiscalización y encargado de control interno con inherencia en el desarrollo de las actividades misionales.

6. ACTIVACIÓN DE WINDOWS DEFENDER: Verificar la configuración activa de la herramienta y en mejora de esta herramienta cumpliendo con los lineamientos de seguridad de la CONTRALORÍA MUNICIPAL.

4 CONFIGURACIÓN DE SEGURIDAD PARA EL ACCESO A INTERNET

Configurar el Router de servicio a internet, limitando el acceso SÓLO a los equipos propios del CONTRALORIA MUNICIPAL y se restringe totalmente el uso de dispositivos móviles en la red WiFi de la CONTRALORIA MUNICIPAL. Adicionalmente, se socializa el lineamiento para solicitar acceso al servicio de internet para contratistas o usuarios invitados con dispositivos portátiles.

Todos los funcionarios, contratistas y usuarios con autorización al uso y acceso a estos servicios deben:

- Utilizar este servicio exclusivamente para fines laborales.
- Conservar normas de respeto, confidencialidad y criterio ético.
- Descarga, documentos o archivos tomando las medidas de precaución para evitar el acceso de virus y malware en las redes y equipos informáticos.

Uso indebido del servicio de Internet/Intranet:

- Acceder a sitios de juegos o apuestas en línea.
- Acceder a sitios de divulgación, descarga o distribución de películas, videos, música, webcams, etc.
- Acceder y/o descargar material pornográfico u ofensivo.
- Compartir en sitios web información propia de la CONTRALORIA MUNICIPAL clasificada o reservada por sus usuarios, funcionarios, o contratistas.

- Emplear este servicio de internet para la recepción, envió o distribución de información pública clasificada o reservada de la CONTRALORIA MUNICIPAL a través de servicios y cuentas de correo públicos. (ej. Gmail, Hotmail, Yahoo! etc.)
- Cargar, descargar, enviar, imprimir o copiar archivos, software o contenidos en contra de las leyes de derechos de autor.
- Utilizar el servicio de Internet para propósitos comerciales ajenos a la CONTRALORIA MUNICIPAL.
- Intentar o modificar las opciones de configuración y/o parámetros de seguridad de los navegadores instalados por la CONTRALORIA MUNICIPAL.
- Comprar o vender artículos personales a través de sitios web o de subastas en línea.
- Publicar o enviar opiniones, declaraciones políticas y asuntos no propios del CONTRALORIA MUNICIPAL dirigidos a funcionarios, contratistas o usuarios y público en general, del sector oficial, de otras compañías y organizaciones, a través de este servicio.
- Descargar, instalar y configurar navegadores distintos a los recomendados por el ingeniero encargado.

Por otra parte, se les recuerda que la **CONTRALORIA MUNICIPAL NO ES RESPONSABLE** por la pérdida de información, desfalco o daño que pueda tener un usuario al acceder a sitios de suplantación o al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito al hacer el uso de este servicio.

5. CONFIGURACIÓN Y SOCIALIZACIÓN DE LOS SERVICIOS DEL CORREO INSTITUCIONAL Y GRUPOS DE MENSAJERIA INSTANTANEA.

5.1 CONFIGURACIÓN DE CUENTAS GOOGLE PARA EL CORREO INSTITUCIONAL:

Esta configuración facilitaría el envío y recepción de información entre los funcionarios de la entidad, garantizando una comunicación ágil, veraz y eficaz, a su vez que se efectuen

Cronograma con las actividades o mesas de trabajo a desarrollar, entre otras herramientas que ofrece la suite de Google.

5.2 SOCIALIZACIÓN DE LOS CORREOS ELECTRONICOS Y ACTUALIZACIÓN DE CONTRASEÑAS: El uso del correo electrónico constituye una poderosa herramienta de trabajo, que permite la transferencia de información interna, en forma eficiente, ágil y económica; y cualquier uso indebido del mismo puede afectar severamente la imagen y la reputación de la entidad. Así las cosas, se deberá tener en cuenta los lineamientos y responsabilidades definidos en la Política de Seguridad y Privacidad de la información.

5.3 CONFIGURACIÓN DEL CALENDARIO PARA CUENTAS GOOGLE: Configurar el calendario para compartir las diferentes actividades de la CONTRALORIA MUNICIPAL a través de las cuentas de Google, y capacitar a los funcionarios y contratistas para el manejo de esta agenda y sus recordatorios mediante notificaciones.

5.4 CONFIGURACIÓN DE CUENTAS GOOGLE PARA COPIAS DE SEGURIDAD EN LA NUBE: Capacitar a los funcionarios con cuenta institucional para implementar una herramienta de copias de seguridad en la nube, con frecuencia semanal para todos los archivos de trabajo diario.

5.5 SOCIALIZACIÓN DEL WHATSAPP INSTITUCIONAL. En aras de mantener una comunicación permanente con el personal que se encuentra vinculado a la CONTRALORIA MUNICIPAL, se mantiene los grupos de difusión en el WhatsApp denominados "Contraloria BcaBja y CPS-2025", el cual es administrado por la contralora municipal, el secretario general, director técnico responsabilidad fiscal y jurisdicción coactiva y el director técnico de fiscalización con las siguientes directrices:

a) En el WhatsApp se DEBEN encontrar todos los contratistas vinculados a la contraloría municipal.

b) Los Prestadores de Servicio que se vinculen contractualmente a la contraloría serán agregados al grupo de WhatsApp. Una vez se liquide el Contrato, serán eliminados del grupo.

c) El WhatsApp tiene como objetivo dar a conocer directrices internas emanadas por parte del despacho, programación de reuniones, mesas de trabajo, talleres, actividades misionales, capacitaciones, noticias de actualización, citaciones por parte de los jefes de área, seguimiento o requerimientos, entre otras actividades inherentes a las funciones misionales o administrativas de la contraloría.

5.6 En el WhatsApp queda prohibido realizar las siguientes manifestaciones:

a) Cualquier propaganda o publicidad distinta a las funciones misionales y administrativas de la contraloría.

b) Enviar videos o mensajes de reflexión, religiosos, de amistad, personales, chistes o de cualquier otra índole.

c) Enviar fotografías o videos personales que distan de las funciones de la contraloría.

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

Este plan se establece para la implementación y socialización del componente de gobierno digital en lo correspondiente a la estrategia de tratamiento de riesgos de seguridad y privacidad de la información con el fin de preservar los datos de los usuarios internos y externos, garantizando la seguridad de la información.

6.1 Definiciones

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a

la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización.

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento

Ciber-seguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Datos Personales Públicos: Es el dato que no sea semi-privado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar

contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos juntos con datos privados o sensibles.

Datos Personales 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. (Decreto 1377 de 2013, art 3).

Declaración de Aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación.

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados.

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

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.

Privacidad: En el contexto de este documento, por privacidad se entiende 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 en Linea la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación, de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

6.2 Objetivo General

Establecer controles para minimizar los riesgos generados en los procesos tecnológicos llevados a cabo como parte de la misión de la Contraloría Municipal de Barrancabermeja, con el fin de salvaguardar los activos de información, el manejo de medios digitales, controles de acceso, y gestión de usuarios.

6.3 Objetivos específicos

- Adelantar actividades para el análisis de los recursos con los que cuenta la entidad para establecer el adecuado plan de tratamiento de seguridad y privacidad de la información.

- Aplicar las metodologías, políticas y estrategias respectivas en seguridad y riesgos de la información.

6.4 Recursos

- Humano: funcionarios de planta, contratistas y pasantes.
- Físico: infraestructura tecnológica.
- Financieros: recursos aprobados en el PAA (plan anual de adquisiciones).

6.5 Responsables

- Contralor.
- Líderes de procesos.

- Equipo de trabajo del proceso Gestión de las TIC o Profesional Universitario encargado de la Gestión TIC de la Entidad.

6.6 Implementación

Para el desarrollo del plan de tratamiento de riesgos de seguridad y privacidad de la información se tendrá como base la metodología PHVA (Planear, Hacer, Verificar y Actuar), y los lineamientos y estrategias definidos por el Ministerio de las Tecnologías y las Comunicaciones MinTic a través de la normatividad vigente.

6.7 Actividades

- Realizar análisis de la situación actual de la Entidad.
- Realizar diagnóstico.
- Realizar la identificación de los riesgos por dependencias con los líderes de cada proceso.
- Valoración de los riesgos encontrados.
- Elaborar el plan de tratamiento de riesgos de seguridad y privacidad de la información.
- Comunicar, revisar y/o modificar el plan definido con los líderes de los procesos.
- Seguimiento y evaluación.

7. COPIAS DE SEGURIDAD DE LA INFORMACION BACKUPS

7.1 Objetivo

Asegurar los datos contenidos en los sistemas de información a través de la generación de copias de respaldo de archivos, portal web institucional, programas, sistemas operativos y

bases de datos, garantizando su restauración ante posibles pérdidas o daños en la infraestructura.

7.2 Alcance

Este procedimiento aplica a los servidores del ambiente productivo de la Contraloría Municipal de Barrancabermeja. Servidor BUFFALO, Portal Web Institucional, usuarios con equipo portátil y a usuarios que manejen información sensible de la Contraloría de Barrancabermeja

7.3 Definiciones

a) **Respaldo:** Una copia de seguridad, también llamada Backup (su nombre en inglés), es una copia íntegra y confiable de los datos originales, que se almacena fuera del dispositivo en donde éstos se alojan, con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

b) **Información importante y/o crítica:** Son todos los archivos generados por los aplicativos que tiene la compañía, o aquellos archivos que guarda o genera el usuario final y que son fuente de información primordial para la empresa.

c) **Base de datos:** Una base de datos es una colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que necesite

d) **Restauración de los datos:** (en inglés restore), es la acción de leer y grabar en la ubicación original u otra alternativa los datos requeridos.

e) **Repositorio:** Un repositorio, depósito o almacén, es un sitio centralizado donde se almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos.

7.4 Roles y Responsabilidades

a) **Administrador Sistema de Backup**: Es la persona responsable de llevar a cabo este proceso de copias y restauraciones de los diferentes sistemas de información

b) **Solicitante:** Es la persona autorizada para realizar solicitudes de respaldo o restauración sobre los diferentes Sistemas de Información. Estos solicitantes autorizados son (Lideres de área, jefes inmediatos o Coordinadores)

7.5 Indicadores

METRICAS		
Indicador de Proceso	**Nombre del Indicador**	**Descripción del indicador (Que busca medir)**
Respaldo de Información	Porcentaje de cumplimiento de copias de respaldo de la Información	Medir el nivel de cumplimiento de las copias de respaldo que se realizan a los servidores productivos y equipos de usuario final.
Cómo se mide (Formulación)	**Frecuencia de seguimiento**	**Meta (target)**
N° de copias de respaldo de información exitosas / total copias de respaldo x 100.	Mensual	90%
Responsable: dueño del indicador	Administrador de Respaldo de Información	

METRICAS		
Indicador de Proceso	**Nombre del Indicador**	**Descripción del Indicador (Que busca medir)**
Copias de respaldo con pruebas de restauración	Porcentaje de cumplimiento de copias de respaldo de la Información con pruebas de restauración	Medir el nivel de cumplimiento de las copias de respaldo con prueba de restauración que se realizan a los servidores productivos y equipos de usuario final
Cómo se mide (Formulación)	**Frecuencia de seguimiento**	**Meta (target)**
N° de copias de respaldo con prueba de restauración/ total de copias de respaldo X 100.	Mensual	95%
Responsable: dueño del indicador	Administrador de Respaldo de Información	

7.6 Periodicidad de los respaldos de información

Tipo Equipo	Tipo de Respaldo	Dia de Ejecución	Tiempo de Retención
Servidor NAS (Almacenamiento de Carpetas de trabajo y Procesos)	Físico (Disco Duro Externo)	Viernes	15 días
Portal Web stitucional	Físico (Disco Duro Externo)	Viernes	15 días

7.7 rocemiento respaldo de información

dentifi los sistemas de información: El administrador de Backup revisara con base el alcance definido los sistemas o equipos que deben agregarse al esquema de Backu

2) **Elabo el plan de copias de respaldo:** Teniendo en cuenta el volumen de inform ión y la periodicidad de las copias, el administrador debe generar un plan de copia e respaldo según las políticas de seguridad

3) **Pro mar /lanzar Job de Backup:** De acuerdo con la periodicidad establecida y el tam de la información, el administrador creará los Jobs de las copias o las generará ma lmente.

4) **Ve car resultado del Backup:** El administrador valida el estado de la finalización de lo ackup

¿ ckup Satisfactorio?

, sigue al paso 5

o, Si hay fallas en la copia, se deben analizar las causas, tomar los correctivos y generar nuevamente el Backup.

Diligenciar bitácora: El administrador de Backup diligencia la bitácora con el resultado de la copia de seguridad. Anexo A. Bitácora de Realización de Copias de Seguridad (Backup), restauración y pruebas de restauración

b) **Solicitante:** Es la persona autorizada para realizar solicitudes de respaldo o restauración, sobre los diferentes Sistemas de Información. Estos solicitantes autorizados son (Líderes de área, jefes inmediatos o Coordinadores)

7.5 Indicadores

METRICAS		
Indicador de Proceso	**Nombre del Indicador**	**Descripción del Indicador (Que busca medir)**
Respaldo de Información	Porcentaje de cumplimiento de copias de respaldo de la Información	Medir el nivel de cumplimiento de las copias de respaldo que se realizan a los servidores productivos y equipos de usuario final.
Cómo se mide (Formulación)	**Frecuencia de seguimiento**	**Meta (target)**
N° de copias de respaldo de información exitosas / total copias de respaldo x 100.	Mensual	90%
Responsable: dueño del indicador	Administrador de Respaldo de Información	

METRICAS		
Indicador de Proceso	**Nombre del Indicador**	**Descripción del Indicador (Que busca medir)**
Copias de respaldo con pruebas de restauración	Porcentaje de cumplimiento de copias de respaldo de la Información con pruebas de restauración	Medir el nivel de cumplimiento de las copias de respaldo con prueba de restauración que se realizan a los servidores productivos y equipos de usuario final
Cómo se mide (Formulación)	**Frecuencia de seguimiento**	**Meta (target)**
N° de copias de respaldo con prueba de restauración/ total de copias de respaldo X 100. .	Mensual	95%
Responsable: dueño del indicador	Administrador de Respaldo de Información	

7.6 Periodicidad de los respaldos de información

Tipo Equipo	Tipo de Respaldo	Dia de Ejecución	Tiempo de Retención
Servidor NAS (Almacenamiento de Carpetas de Trabajo y Procesos)	Físico (Disco Duro Externo)	Viernes	15 días
Portal Web stitucional	Físico (Disco Duro Externo)	Viernes	15 días

7.7 Procemiento respaldo de información

1) **Identificar los sistemas de información:** El administrador de Backup revisara con base el alcance definido los sistemas o equipos que deben agregarse al esquema de Backup

2) **Elabo el plan de copias de respaldo:** Teniendo en cuenta el volumen de información y la periodicidad de las copias, el administrador debe generar un plan de copia respaldo según las políticas de seguridad

3) **Programar /lanzar Job de Backup:** De acuerdo con la periodicidad establecida y el tamaño de la información, el administrador creará los Jobs de las copias o las generará manualmente.

4) **Verificar resultado del Backup:** El administrador valida el estado de la finalización de los Backup

¿Backup Satisfactorio?

Si, sigue al paso 5

No, Si hay fallas en la copia, se deben analizar las causas, tomar los correctivos y generar nuevamente el Backup.

Diligenciar bitácora: El administrador de Backup diligencia la bitácora con el resultado de la copia de seguridad. Anexo A. Bitácora de Realización de Copias de Seguridad (Backup), restauración y pruebas de restauración

b) **Solicitante:** Es la persona autorizada para realizar solicitudes de respaldo o restauración, sobre los diferentes Sistemas de Información. Estos solicitantes autorizados son (Lideres de área, jefes inmediatos o Coordinadores)

7.5 Indicadores

METRICAS		
Indicador de Proceso	**Nombre del Indicador**	**Descripción del Indicador (Que busca medir)**
Respaldo de Información	Porcentaje de cumplimiento de copias de respaldo de la Información	Medir el nivel de cumplimiento de las copias de respaldo que se realizan a los servidores productivos y equipos de usuario final.
Cómo se mide (Formulación)	**Frecuencia de seguimiento**	**Meta (target)**
N° de copias de respaldo de información exitosas / total copias de respaldo x 100.	Mensual	90%
Responsable: dueño del indicador	Administrador de Respaldo de Información	

METRICAS		
Indicador de Proceso	**Nombre del Indicador**	**Descripción del Indicador (Que busca medir)**
Copias de respaldo con pruebas de restauración	Porcentaje de cumplimiento de copias de respaldo de la Información con pruebas de restauración	Medir el nivel de cumplimiento de las copias de respaldo con prueba de restauración que se realizan a los servidores productivos y equipos de usuario final
Cómo se mide (Formulación)	**Frecuencia de seguimiento**	**Meta (target)**
N° de copias de respaldo con prueba de restauración/ total de copias de respaldo X 100. .	Mensual	95%
Responsable: dueño del indicador	Administrador de Respaldo de Información	

7.6 Periodicidad de los respaldos de información

Tipo de Equipo	Tipo de Respaldo	Dia de Ejecución	Tiempo de Retención
Servidor NAS (Almacenamiento de Carpetas de Trabajo y Procesos)	Físico (Disco Duro Externo)	Viernes	15 días
Portal Web Institucional	Físico (Disco Duro Externo)	Viernes	15 días

7.7 Procedimiento respaldo de información

1) **Identificar los sistemas de información:** El administrador de Backup revisara con base en el alcance definido los sistemas o equipos que deben agregarse al esquema de Backup.

2) **Elaborar el plan de copias de respaldo:** Teniendo en cuenta el volumen de información y la periodicidad de las copias, el administrador debe generar un plan de copias de respaldo según las políticas de seguridad

3) **Programar /lanzar Job de Backup:** De acuerdo con la periodicidad establecida y el tamaño de la información, el administrador creará los Jobs de las copias o las generará manualmente.

4) **Verificar resultado del Backup:** El administrador valida el estado de la finalización de los Backup

   ¿Backup Satisfactorio?

   Si, sigue al paso 5
   No, Si hay fallas en la copia, se deben analizar las causas, tomar los correctivos y generar nuevamente el Backup.

5) **Diligenciar bitácora:** El administrador de Backup diligencia la bitácora con el resultado de la copia de seguridad. Anexo A. Bitácora de Realización de Copias de Seguridad (Backup), restauración y pruebas de restauración

6) **Almacenamiento de Backup:** Una vez finaliza el Backup se almacena en el repositorio destinado para tal fin, quedando disponible para una restauración en caso de ser necesario.

7) **Copia Externa:** Enviar la copia de los Backup realizados a la Secretaria General

7.8 Procedimiento Pruebas restauración de información

1) **Elaborar plan de pruebas de restauración:** El administrador de Backup armara un plan de pruebas de restauración de bases de datos e información de los diferentes sistemas y/o usuarios.
2) **Restauración Información:** De acuerdo con el plan de pruebas de restauración el administrador generara las restauraciones en las fechas indicadas

¿Restauración Satisfactoria?

Si, continua con el paso 3
No, Si se presentan fallas en la restauración, el administrador notificara a la secretaria general para buscar la causa raíz del problema y remediar inmediatamente.

3) **Diligenciar bitácora:** El administrador de Backup diligenciará el control de pruebas de restauración. Anexo A. Bitácora de Realización de Copias de Seguridad (Backup), restauración y pruebas de restauración
4) **Validación de información:** Con el apoyo del área de TICs o usuario responsable se valida la integridad de la información restaurada

7.9 Procedimiento restauración de información

1) **Solicitud restauración de información:** El solicitante registrará un caso de restauración de información a través de correo electrónico o solicitud al área de TICs o Administrador de Backup.
2) **Validación de la información:** El Administrador de Backup valida que la información este completa y sea clara para poder realzar la restauración de la información.

¿La información está completa?

Sí, continuar con la actividad número 3.
No, devolverse a la actividad número 1, comunicando que se requiere más información para poder gestionar la solicitud realizada

3) **Restauración Información:** De acuerdo a la información suministrada se da inicio a la restauración

¿Restauración Satisfactoria?

Si, Si la restauración es exitosa, se registra en el caso y se da cierre
No, Si se presentan fallas en la restauración, se informa al solicitante y se validan otros posibles puntos de restauración.

4) **Cierre de Caso:** El Administrador de Backup procede a registrar la restauración en la Bitácora de Restauración de Copias de Seguridad y procede con el cierre del mismo. Anexo A. Bitácora de Realización de Copias de Seguridad (Backup), restauración y pruebas de restauración

7.10 Documentación

Anexo A. Bitácora de Realización de Copias de Seguridad (Backup), restauración y pruebas de restauración

CONTROL DE FIRMAS

Aprobado en Comité Institucional de Gestión y Desempeño – Acta No. 01 del 28 de enero de 2025.

CARLOS ARTURO VÁSQUEZ ALDANA
Secretario General

Proyecto: HECTOR FIDEL CASTAÑO SORZA, Profesional Externo – Ingeniero de Sistemas