PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

JULIO DE 2018

"Control Fiscal, con Efectividad y Transparencia"
Calle 48 No. 17-25. Tels: 6025001 – 6020859 Fax 6022175
Email: info@contraloriabarrancabermeja.gov.co
Página Web: www.contraloriabarrancabermeja.gov.co

INTRODUCCIÓN

En la actualidad los sistema 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.

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.

1. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1.1Objetivos

- 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 y pasantes 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.

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 del 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 profesional de 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.

TIC: 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 ultra-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, valora 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 o la información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo, los funcionarios públicos que detecten el mal uso de la información está 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 interna a través del SPARK, 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 area 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 Municipal de 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 y 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, llevar 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 en los computadores, siguiendo las indicaciones técnicas dictadas.

1.7.11 Contingencia

La administración de la Entidad debe preparar, actualizar periódicamente y probar en forma regular 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 etc.

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 por el Director Financiero o 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 equipos 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, s, Memorias Flash (USB), disquetes, 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 derramadas 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, divulgará, 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 o DVD no esté con rayones, 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 debe 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. 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.

2.1 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 controlar 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 sólo 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 GEL 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.

2.2 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.

2.3 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.

2.4 Recursos

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

2.5 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.

2.6 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.

2.7 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.

3. CONTROL DE CAMBIOS

FECHA	*VERSIÓN*	*DESCRIPCIÓN DEL CAMBIO*
17/07/2018	01	Emisión original

OLIVA OLIVELLA GUARÍN
CONTRALORA MUNICIPAL DE BARRANCABERMEJA

LUIS ALFONSO LOZANO CAMACHO
REVISÓ

FERNAN DARIO PÉREZ ACOSTA
PROYECTÓ