POLITICA DE SEGURIDAD DE LA INFORMACIÓN

GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

Bogotá, julio de 2019

MANUEL DOMINGO ABELLO ALVAREZ

Secretario General

JAVIER ALEJANDRO CASTRO GUTIÉRREZ

Subdirector de TI

LINA MARCELA GALLEGO RUIZ

Jefe Oficina de Planeación

Grupo de trabajo del Proceso Gestión de Tecnologías de la Información

Ana Marcela Peña Nieto
Claudia Monica Peña Rubiano
Cristian David Home Acosta
Diego Andrés Fonseca Soto
Juan Sebastián Carreño Peñaloza
Luis Felipe Noreña Lopez

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**
1	Julio de 2008	Elaboración inicial del documento
2	Noviembre de 2008	Ajustes en la estructura del documento y codificación
3	Agosto 2009	Cambio de código
4	Septiembre de 2010	Se agregaron las especificaciones y operatividad del servidor de backup para la información de los servidores de la Dirección Nacional, el cual se encuentra ubicado en el CIEN
5	Agosto de 2011	Se indicó el nuevo tamaño máximo de buzón asignado al correo electrónico Se actualizaron las políticas sobre el Backup de servidores Se eliminaron las consideraciones referentes al CIEN
6	Octubre de 2013	Se actualizan las políticas de backup y las responsabilidades de los usuarios en el manejo de la información.
7	Agosto de 2016	Se realizó una revisión de la política, teniendo en cuenta la nueva modernización de la planta y la nueva infraestructura contratada.
8	Julio de 2019	Se actualiza la política general de seguridad y privacidad de la información, se adicionan políticas específicas: Política de uso Adecuado de recursos tecnológicos, de control de acceso y gestión de comunicaciones y política Privacidad y Confidencialidad.

DISPONIBILIDAD DE LOS DOCUMENTOS

Este documento se encuentra localizado en http://www.computadoresparaeducar.gov.co/intranetcpe, donde se pone a disposición para la consulta de los funcionarios de la entidad en formato PDF, permitiendo conservar su contenido original y controlar su reproducción por el responsable de Sistema Integrado de Gestión, conforme a las políticas definidas por el proceso de Gestión de Tecnologías de la Información.

TABLA DE CONTENIDO

Definiciones 5
Objetivo 6
Sanciones 6
Política General de Seguridad de la Información 7
Alcance / Aplicabilidad 7
Conocimiento y cumplimiento de las Políticas de Seguridad de la Información. 8
Comité de Seguridad de la Información 8
Políticas específicas para la implementación de controles de seguridad de la información 9
Política de Uso Adecuado de recursos tecnológicos 9
Política de Control De Acceso y gestión de comunicaciones 9
Políticas de Privacidad y Confidencialidad 11
Gestión de la plataforma tecnológica 13

1. DEFINICIONES

Acuerdo de Niveles de Servicio: Compromiso que permite establecer tiempos y compromisos sobre procesos y/o tareas y/o acciones correctivas. Su definición y cumplimiento son importantes en toda una cadena de otorgamiento de producto o servicio.

Almacenamiento de la Información: Procedimiento mediante el cual se utiliza cualquier dispositivo físico o tecnológico con el fin de guardar archivos y/o datos en forma ordenada. Para el caso de los dispositivos electrónicos se tienen desde unidades pequeñas de almacenamiento (ej: USB), hasta grandes equipos en centros de datos que almacenan millones de registros de información.

Confidencialidad: Es la propiedad de la información, en la que se garantiza que es accesible únicamente al personal autorizado para consultar dicha información.

Control: Conjunto de medidas para el manejo del riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

Derechos de Autor: Conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: Consiste en garantizar que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Evento de Seguridad de la Información: Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.

Habeas Data: Es un derecho que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada.

Incidente de Seguridad de la Información: Se considera un Incidente de Seguridad de la Información a cualquier evento que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad: es la protección de la exactitud y estado completo de los activos.

Plataforma Tecnológica: Conjunto de elementos tecnológicos (hardware y software), que operan e interactúan para entregar servicios informáticos. Una plataforma está conformada por equipos de comunicación, equipos de almacenamiento de información, equipos servidores de aplicaciones, computadores de escritorio, programas de computador, programas de ofimática y centros de datos entre otros.

Respaldo: Es la garantía sobre un bien tangible o intangible. En tecnología el respaldo hace referencia a las copias de seguridad de la información, su almacenamiento en sitios seguros para poder disponer de los datos en eventos críticos donde se requiera restaurar la información.

Riesgo: Es la posibilidad de sufrir daños o pérdidas

2. OBJETIVO

Las políticas de seguridad de la información tienen por objeto establecer por un lado las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes de voz y datos) y personas que interactúan haciendo uso de los servicios asociados a ellas y velar por la integridad, confidencialidad y disponibilidad de la información; así mismo, controlar si es generada, manipulada, modificada, almacenada, conservada, transportada, accedida, divulgada y/o destruida, de acuerdo con la normatividad vigente.

3. SANCIONES:

El no cumplimiento de las políticas, normas y procedimientos, se calificará como una falta y será sancionada de acuerdo con lo establecido en el reglamento interno de trabajo de COMPUTADORES PARA EDUCAR.

En tal evento, se realizará una reunión donde intervengan las áreas de talento humano, jurídica y la persona involucrada con su respectivo jefe inmediato, con el fin de tipificar la falta y aplicarla tomando como referencia el reglamento interno de trabajo o en su defecto, lo que los participantes de la reunión consideren pertinente, en consecuencia con la normatividad vigente.

4. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la Dirección de COMPUTADORES PARA EDUCAR con respecto a la protección de los activos de información en cuanto a su integridad, acceso, uso y respaldo. Esta política que aplica para trabajadores de todos los niveles, incluye a contratistas y terceros que tengan acceso a la información de CPE.

Esta política ha sido establecida con el ánimo de:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el modelo de seguridad y privacidad de la información.
- Proteger los activos de información.
- 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 usuarios de COMPUTADORES PARA EDUCAR.
- Garantizar la continuidad del negocio frente a incidentes.

4.1 ALCANCE / APLICABILIDAD

Esta política aplica a toda la entidad y debe ser cumplida por los directivos, funcionarios, administrativos, contratistas y terceros que tengan algún tipo de relación con COMPUTADORES PARA EDUCAR en el desarrollo de los procesos en los que se involucren activos de Información.

4.2 CONOCIMIENTO Y CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMACIÓN.

La Dirección de COMPUTADORES PARA EDUCAR – CPE:

- Apoyará la definición, implementación, divulgación, seguimiento y cumplimiento de las políticas de seguridad de la Información al interior de la Entidad. Debe promover activamente una cultura de seguridad de la información, definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en todos los niveles jerárquicos.
- Definirá los aspectos legales para ayudar a dirimir los posibles conflictos que se presenten en la aplicación de las políticas, normas y procedimientos.
- Definirá los aspectos concernientes al acceso físico a las instalaciones de COMPUTADORES PARA EDUCAR - CPE y la seguridad perimetral.

4.3 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Las funciones del comité de seguridad de la Información son asumidas por el Comité Institucional de Gestión y Desempeño de Computadores para Educar, teniendo en cuenta lo establecido en la GUÍA DE CONFORMACIÓN Y FUNCIONES DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO, en el numeral 6, en el que se definen como funciones principales: *"…Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información y aprobar y hacer seguimiento a la implementación de la Estrategia de Gobierno Digital y Seguridad de la Información en la Entidad".*

El comité está conformado por los siguientes miembros:

• Secretario General: con voz y voto
• Oficina asesora de planeación: Secretaría técnica de comité (con voz y voto)
• Asesor de la dirección ejecutiva: con voz y voto
• Subdirector de formación: con voz y voto
• Subdirector TI: con voz y voto
• Subdirector operativo: con voz y voto
• Coordinador de contratación: Secretaría técnica de comité para los casos de seguimiento a la ejecución del PAA y supervisión de contratos (con voz y voto)
• Coordinador administrativo y financiero: con voz y voto
• Invitados: Son todos los que sean requeridos para temas específicos del comité (con voz y sin voto)

5. POLITICAS ESPECÍFICAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

5.1. Política de Uso Adecuado de recursos tecnológicos

El uso adecuado de los recursos tecnológicos asignados por COMPUTADORES PARA EDUCAR a sus funcionarios y/o terceros se reglamenta bajo los siguientes lineamientos:

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo de COMPUTADORES PARA EDUCAR es potestativa de la Subdirección de TI, y por tanto, son los integrantes de esta dependencia los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser aprobados por la subdirección de TI.

- Los usuarios no deben utilizar software diferente al establecido por Computadores para Educar para el desarrollo de sus actividades laborales. En caso de requerirse la instalación de un software adicional, se deberá solicitar autorización por escrito a la subdirección de TI al correo soporteti@cpe.gov.co, La subdirección procederá a validar las condiciones de licenciamiento, seguridad y pertinencia para la instalación y uso del software solicitado.

- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, protector de pantalla corporativo, entre otros.

5.2. Política de Control De Acceso y gestión de comunicaciones

Esta política hace referencia a las directrices para el acceso a la información de COMPUTADORES PARA EDUCAR. Determina los límites y mecanismos de protección relacionados con el acceso a la información de la entidad.

- La subdirección de TI es responsable del control de acceso a redes, aplicaciones, y/o sistemas de información de la entidad. Los integrantes de esta dependencia son los únicos autorizados a realizar las labores de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas.

- Todos los usuarios de la plataforma tecnológica de COMPUTADORES PARA EDUCAR deben tener una identificación y una contraseña única e intransferible, para hacer uso de la información y de los recursos tecnológicos en cada una de las plataformas. Cada usuario es responsable de sus credenciales de acceso y del uso que se haga de las mismas. Los trabajadores y contratistas que laboran para COMPUTADORES PARA EDUCAR deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. Los particulares que requieran acceso a la red de CPE, deben ser autorizados por la subdirección de TI, previa justificación. Proveedores o terceras personas, solamente deben

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

- La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red, será realizada por la subdirección de TI que se encargará de adoptar las medidas necesarias para garantizar la seguridad de los activos de información. Con este fin, los trabajadores de CPE y terceros autorizados, deberán tener en cuenta las siguientes medidas:

  a. Las redes de comunicaciones institucionales deben ser utilizadas exclusivamente con fines laborales.

  b. Se debe evitar conectar dispositivos de comunicaciones no autorizados por la Subdirección de TI, que puedan alterar el funcionamiento normal de la red o comprometer la seguridad, tales como switches, routers, unidades de almacenamiento externas, equipos portátiles o teléfonos celulares.

- La cuenta de correo electrónico institucional debe ser usada para el desempeño de las funciones asignadas dentro del COMPUTADORES PARA EDUCAR y será responsabilidad de cada uno de los usuarios su utilización de manera ética, razonable, no abusiva, productiva y propendiendo por el cumplimiento misional de la entidad.

- Los mensajes y la información contenida en los buzones de correo son propiedad de COMPUTADORES PARA EDUCAR, por lo tanto, cada usuario como responsable de su buzón, deberá conservar únicamente los mensajes relacionados con el desarrollo de sus funciones.
- No se permite el uso de la dirección de correo electrónico institucional de COMPUTADORES PARA EDUCAR como medio de acceso a comunidades interactivas de contacto social, tales como Facebook, Instagram etc, entre otras, para fines diferentes a las funciones propias asignadas laboralmente.

- Se prohíbe el envío de archivos con cualquier tipo de contenido malicioso, potencialmente peligroso y/o ajeno a las funciones propias del rol asignado como trabajador de CPE.

- El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que COMPUTADORES PARA EDUCAR proporciona a cada uno de los usuarios. De igual manera, las cuentas de correo institucionales genéricas no se deben emplear para uso personal.

5.3. Políticas de Privacidad y Confidencialidad

COMPUTADORES PARA EDUCAR firmará acuerdos de confidencialidad con los funcionarios, clientes y terceros que por diferentes razones requieran conocer, publicar o intercambiar información de la Institución, diferente a la que ha sido previamente expuesta de manera oficial, en el sitio web o redes sociales institucionales. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información. Todos los funcionarios y contratistas deberán firmar estos acuerdos que quedarán definidos al momento de suscribir los respectivos contratos TH-051-F Acta de confidencialidad.

Toda la información generada, adquirida o administrada por las personas que laboran para COMPUTADORES PARA EDUCAR - CPE, es propiedad de CPE, y como tal no debe ser empleada para usos diferentes a los del cumplimiento de sus funciones, que no le generen beneficios a la misma.

Toda la información generada, adquirida o administrada por terceros en virtud de la ejecución de procesos de COMPUTADORES PARA EDUCAR - CPE y de la prestación de servicios, se considera propiedad de CPE, y como tal no debe ser empleada para usos diferentes a los que se acordaron contractualmente.

Dentro del uso de la información, todos los empleados y profesionales contratados en la modalidad de prestación de servicios para COMPUTADORES PARA EDUCAR – CPE, no podrán utilizar programas diferentes a los proporcionados por la Entidad, y se comprometen a cumplir la legislación colombiana sobre derechos de autor, **Ley 23 de 1982 Sobre los Derechos de Autor.**

La información de COMPUTADORES PARA EDUCAR podrá ser clasificada según el grado de privacidad y confidencialidad requerido. Los usuarios de la información tendrán restricciones para el acceso a la misma, según las clasificaciones establecidas y las regulaciones a las que haya lugar.

Al interior de COMPUTADORES PARA EDUCAR, los usuarios no podrán: imprimir, copiar, transferir, modificar y/o destruir los activos de información, sin la debida autorización de los jefes de área, encargados del uso y custodia de la información.

Al interior de COMPUTADORES PARA EDUCAR, los usuarios de los activos de información están obligados a preservar su integridad y cuidar su confidencialidad.

Los trabajadores de COMPUTADORES PARA EDUCAR están obligados a dar cumplimiento de la Ley 1581 de 2012 por la cual se dictan disposiciones para la protección

de datos personales y el Decreto 1377 de 2013 por el cual se reglamenta parcialmente la ley 1581 de 2012. Los lineamientos generales en esta materia se pueden consultar en el documento **GTI-001-Po POLÍTICA DE TRATAMIENTO INFORMACIÓN PERSONAL.**

Principios del tratamiento de datos personales:

- Principio de la Legalidad: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
- Principio de finalidad: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
- Principio de libertad: El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.
- Principio de veracidad o calidad: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- Principio de transparencia: Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.
- Principio de acceso y circulación restringida: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.
- Principio de seguridad: La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento
- Principio de confidencialidad: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.

6. GESTIÓN DE LA PLATAFORMA TECNOLÓGICA

La plataforma tecnológica del COMPUTADORES PARA EDUCAR - CPE, debe ser diseñada, adquirida, modificada, operada, controlada y respaldada siguiendo prácticas que garanticen las siguientes características de seguridad: confidencialidad, control de acceso, integridad, disponibilidad y la no repudiación de la información y las operaciones que se realicen sobre la plataforma. La Subdirección de TI definirá los mecanismos y lineamientos que se empleen para proveer dichas características; podrá estar en uno solo de los componentes de la plataforma o en varios de ellos, según el nivel de seguridad que se requiera.

La Plataforma Tecnológica de COMPUTADORES PARA EDUCAR - CPE, está compuesta por:

- Los equipos activos (routers, APs, teléfonos, modems).
- Los canales de comunicación.
- Equipos de computación o procesamiento de datos o de información.
- Las aplicaciones, programas de software.
- Las bases de datos.
- Las licencias de uso de los programas de ofimática y licencias de desarrollo