UNIDAD ADMINISTRATIVA ESPECIAL DEL SERVICIO PÚBLICO DE EMPLEO

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

BOGOTÁ D.C
2024

Nombre del documento	Política de Seguridad y Privacidad de la Información	
Estado del documento	Versión liberada	
Responsables	**Nombre y Cargo**	**Entidad**
	Elaboró: Jorge Iván Alexis Díaz Bernal - Profesional Especializado **Revisó:** Victor Rolando Jaime Velandia – Profesional Especializado **Aprobó** Fredys Alberto Simanca Herrera – Subdirector de Desarrollo y Tecnología	Unidad Administrativa Especial del Servicio Público de Empleo -SPE

Control de Versiones del Documento

Versión	Creación/ modificación	Liberación	Descripción Cambio
1.0	Diciembre 2018	Enero 2019	Versión inicial
2.0	Junio 2019	Junio 2019	Versión adicionada
3.0	Septiembre 2020	Septiembre 2020	Versión adicionada
4.0	Octubre 2020	Octubre 2020	Versión adicionada
4.1	Junio 2021	Junio 2021	Se reestructura la Política de seguridad y privacidad de la información.
4.2	Diciembre 06 de 2021	Diciembre 2021	Se adicionaron lineamientos sobre Wifi y los provisionales a la política.
4.3	Diciembre 16 de 2021	Diciembre 2021	Presentación y aprobación en el Comité de Gestión y Desempeño
5.0	Diciembre 23 de 2021	Diciembre 2021	Publicación página institucional
6.0	Junio 2024	Junio 2024	Se realizaron ajustes de forma y de fondo a todos los componentes que conforman la Política de Seguridad de la Información, se agregó una introducción, así como, dos capítulos relacionados con Ciberseguridad y Relacionamiento con Terceros.

ÍNDICE

La Unidad ADMINISTRATIVA ESPECIAL del Servicio Público de Empleo (Unidad del SPE)

CONSIDERANDO

En el marco de lo establecido en la Política de Gobierno Digital del Ministerio TIC, regulada a través del Decreto 767 de 2022 (PGD, s.f.), la cual, tiene como objetivo: *"Mejorar la prestación de servicios por parte de las entidades, incrementar la confianza digital, generar valor público e impactar positivamente la calidad de vida de los ciudadanos, soportado por la transformación digital del estado. Lo anterior, de forma responsable, proactiva, confiable, articulada y colaborativa entre los actores del ecosistema digital, considerando siempre los derechos y deberes de los usuarios del ciberespacio"*, se resalta la importancia de implementar sus lineamientos por parte de las entidades de la administración pública. La política comprende inicialmente la gobernanza como elemento clave de relacionamiento, la innovación pública digital que propende por la generación de valor público a través de soluciones novedosas y creativas y los habilitadores que corresponden a las capacidades en materia de arquitectura TI, seguridad y privacidad de la información, servicios ciudadanos digitales, y cultura y apropiación. Adicionalmente, comprende tres líneas de acción constituidas por servicios y procesos inteligentes, decisiones basadas en datos y estado abierto; y dos iniciativas dinamizadoras comprendidas por los proyectos de transformación digital y de ciudades inteligentes que permiten dar cumplimiento al objetivo de la Política.

Particularmente, seguridad de la información se implementa a través del habilitador de arquitectura TI y el habilitador de seguridad, considerando los lineamientos establecidos en el Marco de Referencia de Arquitectura Empresarial y el Modelo de Seguridad y Privacidad de la Información del Ministerio TIC, con el fin de generar beneficios estratégicos, tácticos y operativos para la entidad, que garantizan el cumplimiento normativo, la alineación con la estrategia nacional y territorial, facilitan la gestión y fortalecen las capacidades institucionales de TI.

Por lo anterior, en el presente documento se define la Política de Seguridad y Privacidad de la Información de la entidad, articulando la confidencialidad, disponibilidad e integridad de la información. La Política establece las responsabilidades y objetivos para salvaguardar la información de forma apropiada sobre los activos de información de la Unidad del SPE, adicionalmente, busca mitigar los riesgos asociados a la divulgación, fuga, destrucción o uso indebido de los activos de información. Como consecuencia, la Política de Seguridad y Privacidad de la Información orienta la administración de la protección de la información digital, medios impresos y físicos digitales y no digitales, proporcionando las bases para sensibilizar y salvaguardar los activos de información, así como, los datos contenidos en cada instrumento de almacenamiento.

Por lo anterior, el presente documento inicia con la adopción y el ámbito de aplicación, de igual forma, comprende en el Capítulo I el objetivo, alcance y responsables de implementar la política, en el Capítulo II se exponen los términos y definiciones, en el Capítulo III se relacionan las condiciones de uso de la infraestructura tecnológica, en el Capítulo IV se definen las políticas de uso y administración de la infraestructura tecnológica, en el Capítulo V se relaciona la seguridad física y lógica, en el Capítulo VI Ciberseguridad, en el Capítulo VII el relacionamiento de la entidad con terceros, en el Capítulo VIII la política de uso trabajo en casa y/o teletrabajo y cierra con la bibliografía correspondiente.

En mérito de lo expuesto,

RESUELVE

ARTÍCULO PRIMERO – ADOPCIÓN: adoptar la Política de Seguridad y Privacidad de la Información para la Unidad Administrativa Especial del Servicio Público de Empleo (en adelante Unidad del SPE), para establecer los lineamientos de acuerdo con el Modelo de Seguridad y Privacidad de la Información – MSPI establecidos al interior de los comités, grupos de trabajo y las actividades encaminadas al cumplimiento e implementación de la presente política.

ARTÍCULO SEGUNDO – ÁMBITO DE APLICACIÓN: serán sujetos obligados de acuerdo con la estructura organizacional de la entidad: el director(a), los subdirectores, jefes o coordinadores de oficina, servidores de carrera administrativa, de libre nombramiento y remoción, provisionales, los contratistas que hacen parte de la Unidad del SPE y los terceros que tengan acceso a cualquier tipo de información propia de la Unidad del SPE. Las violaciones a los lineamientos establecidos en la presente política comprometen la responsabilidad del infractor y podrán generar acción disciplinaria interna a los servidores públicos y acciones civiles y penales a los funcionarios, provisionales, contratistas y terceros.

CAPÍTULO I: GENERALIDADES

ARTÍCULO TERCERO - OBJETIVO: velar por el cumplimiento de la reglamentación vigente, la normatividad aplicable de la seguridad y privacidad de la información en torno a quien recibe, produce, procesa y reposa en la infraestructura tecnológica de la Unidad del SPE ya sea en forma digital y/o físico, realizando una adecuada protección, gestión y resguardo por medio de la confidencialidad, integridad y disponibilidad de la información tratada.

ARTÍCULO CUARTO - ALCANCE: los sujetos obligados definidos en el Artículo Segundo. Ámbito de Aplicación, deben acoger las medidas de la presente política de carácter técnico, administrativo y del talento humano para mitigar los riesgos y garantizar la protección y privacidad de la información de la Unidad del SPE. Así se generará el uso confiable de la información en el entorno digital y físico, realizando una adecuada gestión de los riesgos, preservando la confidencialidad, integridad y disponibilidad de la información tratada, y de los servicios que se prestan al ciudadano.

ARTÍCULO QUINTO - RESPONSABILIDAD: la estructura organizacional funcional de la entidad, así como, director(a), subdirectores, jefes o coordinadores de oficina, servidores de carrera administrativa, de libre nombramiento y remoción, provisionales, deberán delegar a quien corresponda las siguientes responsabilidades:

a) Dar a conocer la presente política a los funcionarios, provisionales, contratistas y/o terceros que hagan uso de la información de la Unidad del SPE.
b) El grupo de Talento Humano por medio de la Mesa de Ayuda de Servicios Tecnológicos de la Unidad del SPE, debe solicitar para los funcionarios de la entidad, la activación o inactivación de las credenciales de acceso a los diferentes activos de información o plataformas tecnológicas de uso exclusivo de la Unidad del SPE.

c) Los supervisores de contratos por medio de la Mesa de Ayuda de Servicios Tecnológicos de la Unidad del SPE, deben solicitar para contratistas y terceros, la activación o inactivación de las credenciales de acceso a los diferentes activos de información o plataformas tecnológicas de uso exclusivo de la Unidad del SPE.
d) El jefe de área o supervisor de contrato debe solicitar a cada área funcional los niveles de acceso (permisos), a los diferentes activos de información o plataformas tecnológicas.
e) Fomentar la participación en los entrenamientos, capacitaciones y/o programas de sensibilización y concientización relacionados con la seguridad de la información y las expresadas en la presente política.

CAPÍTULO II: DEFINICIONES Y TÉRMINOS

ARTÍCULO SEXTO: para efectos de la presente política, se adoptan las siguientes definiciones:

- ✓ **Activo de información:** datos o conocimiento que tiene valor para la organización (ISO, 2022).
- ✓ **Amenaza:** causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización (ISO, 2022).
- ✓ **Backup:** duplicado de datos almacenados (ISO, 2022).
- ✓ **Confidencialidad:** propiedad que tiene la información, que no se pone a disposición ni se divulga a personas, entidades o procesos no autorizados (ISO, 2022), es decir, solo las personas autorizadas deben tener acceso a la información.
- ✓ **Control de acceso:** medida adoptada para limitar el acceso a los usuarios de datos que posean la debida autorización (ISO, 2022).
- ✓ **Dato personal:** toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (Unión_Europea, 2016).
- ✓ **Dato privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular (Función Pública, 2021), únicamente se puede acceder a dicha información por autoridades judiciales, por ejemplo, se tiene las historias clínicas y/o pruebas de los procesos judiciales.
- ✓ **Dato público:** es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados (Función Pública, 2021).
- ✓ **Dato semiprivado:** es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a un grupo en particular sino a cierto sector o grupo de personas o a la sociedad en general (Función Pública, 2021). Ejemplo pueden ser el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley.
- ✓ **Dato sensible:** es la información que puede afectar la intimidad del titular, produciendo algún tipo de discriminación, por ejemplo, la religión, afinidad política, raza, etc. (Función Pública, 2021)
- ✓ **Datos personales:** es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos. (Función Pública, 2021)
- ✓ **Datos privados:** es el dato que por su naturaleza íntima o reservada sólo es relevante para la Unidad del Servicio Público de Empleo (Función Pública, 2021).
- ✓ **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera un usuario autorizado (ISO, 2022).

- ✓ **Hardware:** dispositivo que tiene al menos una unidad central de procesamiento, medios para almacenamiento permanente y medios para entrada y salida (ISO, 2022).
- ✓ **Información pública reservada:** es la información que está en poder o custodia de un sujeto obligado, el acceso a ella puede ocasionar un daño a intereses públicos y se encuentra expresamente prohibida para la ciudadanía en la Ley. (Comisión_de_la_Verdad, s.f.)
- ✓ **Información pública:** es toda información que los sujetos obligados (entidades públicas, organismos estatales, entre otros) generen, obtengan, adquieran o controlen, en cualquier formato y en el desarrollo de sus funciones (Función Pública, 2021).
- ✓ **Información:** se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen (Función Pública, 2021).
- ✓ **Infraestructura Tecnológica:** conjunto de hardware, software y servicios informáticos de la entidad.
- ✓ **Ingeniería Inversa:** aplicación de un enfoque sistemático, disciplinado y cuantificable para determinar cómo se fabricó y/o diseñó un producto completo a partir de un proceso o una serie de procesos (ISO, 2022).
- ✓ **Integridad:** Propiedad de la información relativa a su exactitud y completitud (ISO, 2022), es decir la información no debe ser alterada en ningún punto, esto contempla: generación, transmisión, recepción y almacenamiento.
- ✓ **Oficial de Seguridad de la Información:** encargado de planear, coordinar y administrar los procesos de seguridad informática acompañado de los pilares integridad, confidencialidad y disponibilidad de la información.
- ✓ **Propietario de la información:** corresponde al área de la entidad que tiene la responsabilidad de definir quiénes tienen acceso y que pueden hacer con la información (insertar, modificar, eliminar). Autoriza la divulgación de la información.
- ✓ **Red LAN:** cualquier red que conecta dispositivos informáticos para formar un grupo de dispositivos intercomunicados (ISO, 2022).
- ✓ **Red MAN:** una red de dispositivos, que se extiende sobre un área geográfica grande, como un área urbana, y que a menudo proporciona servicios de comunicación integrados, como datos, voz y video (ISO, 2022).
- ✓ **Red WAN:** cualquier red que conecta dispositivos informáticos en el entorno externo a las instalaciones (ISO, 2022).
- ✓ **Riesgo:** probabilidad de que se materialice una amenaza a la seguridad y sus consecuencias (ISO, 2022).
- ✓ **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información (ISO, 2022).
- ✓ **Sistema de Gestión de Seguridad de la Información (SGSI):** sistema de gestión basado en un enfoque de riesgo empresarial, que establece, implementa, opera, monitorea, revisa, mantiene y mejora la seguridad de la información (ISO, 2022).
- ✓ **Software malicioso:** software diseñado con intenciones maliciosas que contiene características o capacidades que potencialmente pueden causar daño directa o indirectamente al usuario y/o al sistema informático del usuario (ISO, 2022).
- ✓ **Software:** corresponde al conjunto de programas, aplicaciones, conjunto de pasos o reglas que hacen posible el funcionamiento de un equipo de cómputo.
- ✓ **Tercero:** hace referencia a proveedores, empresas, organizaciones o entidades del estado con las que se realice algún convenio de acceso o transferencia de información.
- ✓ **Trazabilidad:** requerimiento de Seguridad de la Información, el cual se compone para determinar quién, cuándo, cómo y desde donde se realizan las operaciones sobre los datos.
- ✓ **Usuario:** es el personal de la Unidad del SPE del régimen laboral, modalidad de contratación o nivel jerárquico, personas naturales o jurídicas que prestan servicios, tanto públicas como privadas que utilizan la información para sus actividades cotidianas institucionales, en el desarrollo de sus funciones.

CAPÍTULO III: CONDICIONES DE USO DE LA INFRAESTRUCTURA TECNOLÓGICA

ARTÍCULO SÉPTIMO – CONDICIONES DE USO: al tener acceso a la infraestructura tecnológica de la Unidad del SPE, los sujetos obligados de acuerdo con la estructura organizacional deben acoger las medidas de la presente política de carácter técnico, administrativo y del talento humano para mitigar los riesgos y garantizar la protección y privacidad de la información de la Unidad del SPE deben tener en cuenta las siguientes condiciones:

a) **Uso de los recursos:** la infraestructura tecnológica no puede ser utilizada para actividades comerciales privadas o para propósitos de entretenimiento, acceso y uso a material no autorizado. Los recursos de infraestructura son exclusivamente para el desarrollo de las funciones asignadas y/u obligaciones contractuales. Los usuarios no podrán acceder a los recursos informáticos y/o tecnológicos de la Unidad del SPE si no mediante contrato o nombramiento ordinario a la Entidad, en sus modalidades de vinculación laboral, como lo son los mecanismos de contratación e ingreso a la estructura organizacional funcional vigente.

b) **Derechos de acceso:** la Unidad del SPE podrá utilizar herramientas o instrumentos para monitorear el uso de su Infraestructura Tecnológica y los activos de información almacenados en los equipos de cómputo, en la nube, o cualquier otro medio para salvaguardar los datos, los cuales pueden ser transmitidos, divulgados, recibidos por medio de los recursos tecnológicos. La Unidad del SPE adopta mecanismos de autenticación para el acceso y/o uso de los activos de información como los computadores, aplicativos y demás servicios tecnológicos para el desarrollo de las funciones u obligaciones contractuales, los cuales son personales e intransferibles.

c) **Uso prohibido:** los recursos asignados para el desempeño de las funciones u obligaciones contractuales no deben ser utilizados para el almacenamiento de información personal, documentación, archivos de multimedia o material no autorizado que no sea necesario para el desarrollo de sus funciones u obligaciones contractuales. En el caso de almacenar información personal, la Unidad del SPE no se hará responsable por el daño o pérdida de la información almacenada en la nube y/o computadoras.

d) **Mal uso del recurso tecnológico:** los sujetos obligados definidos en el Artículo Segundo, con acceso a los recursos de información de la Unidad del SPE deben abstenerse de realizar acciones que impliquen una mala utilización de los recursos de la Infraestructura Tecnológica y/o insumos suministrados por la Unidad del SPE, el cual, conlleva a la monopolización, obstaculización, acaparamiento o uso personal de los recursos tecnológicos.

e) **Uso inadecuado del software:** los usuarios no deben efectuar ninguna de las siguientes actividades:

- Copiar software licenciado o adquirido por la Unidad del SPE para uso personal o beneficio de terceros.
- Copiar las claves de los productos adquiridos por la Unidad del SPE y utilizarlas para uso personal o beneficio de terceros.
- Instalar software no licenciado o no autorizado por la Unidad del SPE en los servidores y equipos de cómputo de la Unidad del SPE.
- Intencional o fortuitamente introducir software malicioso en la Infraestructura Tecnológica de la Unidad del SPE.

- Copiar, transformar, revisar, adaptar y/o modificar cualquier software de la Unidad del SPE sin previa autorización.
- Descompilar o realizar actividades de Ingeniería Inversa del software, sobre bases de datos u otros sistemas de información de la Unidad del SPE, de ser necesario el proceso de ingeniería inversa se debe contar con la respectiva autorización del superior inmediato, el cuál debe ser informado en la mesa de ayuda por medio del requerimiento expreso en el desarrollo de sus funciones u obligaciones contractuales.
- Utilizar software, hardware o cualquier tipo de tecnología para capturar o interceptar tráfico de voz o datos. De ser requerido el proceso de captura del tráfico de voz o datos, debe contar con la respectiva autorización del superior inmediato, el cuál debe ser informado mediante oficio dirigido a la Subdirección de Desarrollo y Tecnología explicando el alcance y necesidad de realizar estas actividades.
- Copiar, vender, modificar, alterar o difundir cualquier tipo de información sensible, reservada, privada o confidencial de la Unidad del SPE sin la autorización respectiva.

f) Uso inadecuado del suministro eléctrico: los usuarios de la Unidad del SPE no deben conectar a las fuentes reguladas los dispositivos eléctricos o electrónicos que no se encuentran autorizados.

CAPITULO IV: POLÍTICAS DE USO Y ADMINISTRACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA

ARTÍCULO OCTAVO – USO DE LA INFRAESTRUCTURA TECNOLÓGICA: la infraestructura tecnológica que esté dispuesta para los usuarios de la Unidad del SPE, debe ser utilizada teniendo en cuenta los siguientes parámetros:

a) Los sujetos obligados deben almacenar en la nube la información producida para la Unidad del SPE.
b) Los sujetos obligados no deben dejar abierta la sesión de trabajo en los equipos de cómputo al retirarse del puesto de trabajo, asegurando el bloqueo de la sesión; toda modificación, eliminación, envió de correo electrónico y demás actividades es responsabilidad del usuario al que le fue asignado el equipo de cómputo.
c) Los sujetos obligados deben apagar sus equipos de cómputo al culminar la jornada laboral. Únicamente podrán quedar prendidos aquellos equipos de cómputo que cuentan con la autorización de la Subdirección de Desarrollo y Tecnología.
d) No se permite el cambio de hardware y/o software en los equipos de cómputo por personas no autorizadas por la Unidad del SPE.
e) La Subdirección de Desarrollo y Tecnología a través del Procedimiento de Mantenimiento preventivo y correctivo de hardware y software o como parte de sus funciones, podrá realizar la inspección del software instalado en los equipos de cómputo.
f) No utilizar deliberada o inadecuadamente las herramientas tecnológicas dispuestas para el desarrollo de las funciones y obligaciones contractuales para cometer actos ilícitos.
g) Aquellos contratistas que, en el desarrollo de sus obligaciones contractuales, invitados o funcionarios públicos que traigan sus propios equipos informáticos, deben cumplir con las políticas de seguridad y privacidad de la información a cabalidad, salvaguardando todo el contenido exclusivo y de propiedad de la Unidad del SPE.

ARTÍCULO NOVENO – ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS. USO DE CONTRASEÑAS: la administración de usuarios y contraseñas es responsabilidad del administrador de cada uno de los aplicativos y/o servicios informáticos que hacen parte de la Unidad del SPE, asignando el perfil y rol correspondiente, para lo cual tendrá en cuenta los siguientes parámetros:

a) Definir la periodicidad de caducidad de las contraseñas, en cada uno de los sistemas de información y/o servicios informáticos que hacen parte de la Unidad del SPE.
b) Definir y utilizar los mecanismos de uso de contraseñas seguras para aquellos aplicativos y sistemas que así lo permitan. En caso de no existir mecanismos de contraseña segura en los sistemas de información y/o servicios informáticos, el usuario será el responsable de establecer una contraseña segura.
c) La Unidad del SPE podrá conceder o denegar el acceso a los recursos de la Infraestructura Tecnológica a los usuarios que soliciten acceso a los mismos, conforme al desarrollo de sus funciones u obligaciones contractuales.
d) La Unidad del SPE podrá registrar los eventos que se generen por las cuentas de los usuarios que hacen uso de los recursos de la Infraestructura Tecnológica.

ARTÍCULO DÉCIMO – GESTIÓN DE CONTRASEÑAS: los usuarios tienen la responsabilidad en el uso de las contraseñas para cada uno de los aplicativos y/o servicios informáticos que hacen parte de la Unidad del SPE, y para ello se tendrá en cuenta los siguientes parámetros:

a) La contraseña es de carácter personal e intransferible, esto quiere decir, todo evento registrado y ejecutado es responsabilidad del usuario.
b) Es responsabilidad de cada usuario salvaguardar las contraseñas asignadas,
c) Los usuarios deben establecer en todos los aplicativos y/o servicios informáticos contraseñas seguras, que se caracterizan por: tener mínimo 8 (ocho) caracteres, contar con letras mayúsculas y minúsculas, contener números, poseer caracteres especiales (tales como: @, #, $, ¡ o*) y evitar utilizar información personal o palabras comunes de uso cotidiano.
d) El usuario debe implementar el doble factor de autenticación en la cuenta de correo electrónico institucional y en los aplicativos que así lo permitan.
e) El usuario debe modificar la contraseña inicialmente asignada, así mismo, las contraseñas deben ser cambiadas periódicamente y se debe evitar reutilizar contraseñas antiguas utilizadas anteriormente.
f) No registrar las contraseñas en agendas, cuadernos, bloc de notas, post-it, etc; que sean de fácil acceso o visibles para el público en general.
g) En caso de requerirse el almacenamiento de las contraseñas en un equipo de cómputo, se debe utilizar un mecanismo de cifrado seguro que garantice su confidencialidad.

ARTÍCULO DÉCIMO PRIMERO – RESPALDO DE INFORMACIÓN (BACKUP): es responsabilidad de los usuarios y de los administradores de los aplicativos, preservar la información generando periódicamente copias de respaldo:

a) La Subdirección de Desarrollo y Tecnología implementará una política de generación de copias de seguridad que responda a las necesidades particulares de la generación de respaldos para los diferentes Aplicativos y Bases de Datos de la Unidad del SPE.
b) Los sujetos obligados deben almacenar en la nube los datos, información o conocimiento generados como producto de la realización de las actividades propias de las funciones u objeto contractual, preservando la disponibilidad, integridad y confidencialidad de estos.

c) Los sujetos obligados de la Unidad del SPE no deben utilizar sus equipos de cómputo o espacio en la nube para almacenar archivos personales que no se encuentra del alcance laboral o contractual, la Subdirección de Desarrollo y Tecnología no se hace responsable de la perdida de este tipo de información.

ARTÍCULO DÉCIMO SEGUNDO – USO DEL CORREO ELECTRÓNICO

a) El correo electrónico institucional es el medio de comunicación oficial, a través del cual se podrá enviar o recibir cualquier solicitud oficial interna o externa. Por lo tanto, es responsabilidad de cada usuario revisar y dar trámite a las solicitudes recibidas de forma interna o externa, dando solución a la petición. Cuando el correo electrónico recibido no corresponde a la competencia de la solicitud, se debe reenviar o direccionar al área respectiva para su oportuna gestión.
b) El correo electrónico institucional debe ser usado únicamente para el desarrollo de las funciones u obligaciones contractuales relacionados con las actividades de la Unidad del SPE, de ninguna manera debe ser utilizado para fines personales, entretenimiento, diversión, ofensa, intimidación, acoso, agresión, cadenas de envío masivo no relacionadas con temas de la Unidad del SPE, tendencias políticas, tendencias religiosas, discriminación racial, de género o tendencia sexual o para el envío o recepción de material no autorizado.
c) Todo correo electrónico que sea enviado desde el correo institucional debe llevar la nota de confidencialidad, cuyo contenido trata acerca de la exclusividad de la información enviada, de la integridad y confidencialidad de este. Este mensaje debe ser incorporado junto con la firma institucional la cual se genera automáticamente y se debe visualizar al final del correo.
d) Todo correo electrónico donde el usuario evidencie que es un Spam, Malware o se sospeche sobre la afectación y vulnerabilidad de la seguridad, se debe reportar por medio del aplicativo de mesa de ayuda o enviar el correo electrónico al oficial de seguridad de la Unidad del SPE o a quien haga sus veces, para ejecutar las medidas correctivas adecuadas.
e) Deberá procurarse la disponibilidad de la información laboral o contractual proveniente del servicio de correo electrónico institucional, a través de la transferencia de la propiedad de todos los documentos a una cuenta de correo electrónico establecida para el respaldo de la información; será responsabilidad del funcionario y contratista saliente, así como del jefe y supervisor de contrato respectivamente, propender por la efectiva realización de esta actividad.

ARTÍCULO DÉCIMO TERCERO – USO DE DISPOSITIVOS MÓVILES

a) En los dispositivos móviles de propiedad de la Unidad del SPE no se debe almacenar información de carácter personal sensible en los términos especificados por la Ley 1581 de 2012 de protección de datos personales.
b) Los funcionarios, provisionales y/o contratistas que le sea asignado dispositivos móviles de la Unidad del SPE deben proteger física y lógicamente los dispositivos móviles asignados y que son propiedad de la Unidad del SPE, para evitar el hurto, acceso o la divulgación no autorizada de la información institucional.
c) En caso de extravío o hurto de un dispositivo móvil asignado de la Unidad del SPE, el funcionario, provisional, contratista o tercero será el responsable de informar de manera inmediata a la Unidad del SPE en la mesa de ayuda de servicios tecnológicos, el extravío o hurto del dispositivo móvil para realizar el proceso de borrado de datos de la cuenta en los casos que técnicamente sea posible.

ARTÍCULO DÉCIMO CUARTO – USO DE DISPOSITIVOS EXTERNOS Y/O EXTRAÍBLES

a) Aquellos equipos de cómputo que permiten conexiones de dispositivos externos y/o extraíbles como discos duros externos, memorias flash (USB, SD, microSD) CD, DVD, entre otros, deben ser usados únicamente con fines laborales en el desarrollo de sus funciones u obligaciones contractuales.
b) Está prohibido copiar y extraer información institucional por medio de dispositivos de almacenamiento externo como discos duros externos, memorias flash (USB, SD, microSD) CD, DVD, sin autorización. El uso de la información será para propósitos de la unidad del SPE, aún después de finalizada la vinculación o relación contractual.
c) Los sujetos obligados deben velar por la confidencialidad, integridad y seguridad de los datos sobre la información clasificada, reservada o datos personales, privados y/o sensibles; el uso de dispositivos externos y/o extraíbles deben estar justificados previa autorización y solicitud a la Subdirección de Desarrollo y Tecnología.
d) Cuando el medio removible ya no es requerido por el funcionario, contratista o tercero autorizado, se debe realizar una copia de seguridad de la información almacenada en los discos duros externos, memorias flash (USB, SD, microSD) CD, DVD, entre otros y posteriormente borrada de manera segura.

ARTÍCULO DÉCIMO QUINTO – ESCRITORIOS ORGANIZADOS – PANTALLA LIMPIA

a) Mantener la documentación generada en medios impresos, almacenada o dispuesta en los escritorios que se encuentran en las instalaciones de la Unidad del SPE evitando pérdida, daño o fuga de información, manteniendo las medidas de protección adecuadas para salvaguardar la información clasificada, pública, reservada, o que contenga datos personales, semiprivados, privados o sensibles.
b) Todo activo de información en estado físico, propiedad de la Unidad del SPE que se encuentren en los escritorios de los sujetos obligados, es responsabilidad del usuario asignado mantener la confidencialidad, seguridad, disponibilidad e integridad de los datos contenidos en el documento y/o pantallas.
c) Cuando se imprima información clasificada, reservada, dato sensible, personal o privado los documentos deberán ser retirados de forma inmediata de las impresoras para evitar divulgación no autorizada de la información.
d) El papel usado para reciclaje no puede contener información clasificada, reservada, dato sensible, personal o privado, estos documentos que contengan dicha información deben ser destruidos en su totalidad para evitar fuga de información.
e) Los sujetos obligados deben reportar al área administrativa si no cuentan con los mobiliarios suficientes o insumos adecuados para el almacenamiento de la información, así como solicitar la llave del gabinete y verificación del cerrado con la llave. En caso de que este fallando el cierre o la llave el área administrativa realizará el proceso para mantener el mobiliario funcional.
f) Los sujetos obligados que tengan dentro de sus funciones la atención al público, deberán almacenar los documentos y dispositivos de almacenamiento bajo llave y ubicar el equipo de cómputo de tal forma que se evite el acceso o revisión de la información por parte de los visitantes.

ARTÍCULO DÉCIMO SEXTO – INVENTARIO DE INFRAESTRUCTURA TECNOLÓGICA

a) El Grupo Administrativo en cumplimiento de sus funciones realiza la asignación de los elementos para el desarrollo de las funciones u obligaciones contractuales del personal con vínculo laboral vigente en la Unidad del SPE, manteniendo su debida administración y control sobre los usuarios a quienes se les proporcionó los elementos propiedad de la Unidad del SPE.
b) El Grupo Administrativo de la Unidad del SPE realizará el registro de todo elemento tecnológico que sea adquirido para asegurar el cuidado de los elementos mientras se realiza el proceso de asignación, velando por el cuidado ante cualquier pérdida o daño.

c) El Grupo Administrativo de la Unidad del SPE deberá mantener un inventario actualizado, identificando los elementos de cómputo, junto con sus periféricos por medio de una identificación única de activo, sin tener numeración y/o códigos repetidos.
d) El Grupo Administrativo de la Unidad del SPE realizará la asignación de los elementos por medio del formato establecido por la Unidad del SPE, manteniendo la relación del equipo de cómputo asignado con sus periféricos, indicando la numeración o código único asignado. El documento debe ser firmado por el usuario y la persona encargada de realizar la gestión correspondiente.
e) Todo equipo de cómputo o elementos propiedad de la Unidad del SPE, que no se encuentren en uso por los usuarios, que sean cambiados por algún motivo de daño o mal funcionamiento, o cuando se termine la vinculación laboral, deben ser devueltos al Grupo Administrativo por el usuario que sea asignado por medio del formato establecido por la Unidad del SPE, el cual debe contener las firmas correspondientes.
f) La información almacenada en los equipos de cómputo es responsabilidad de los usuarios, ni el Grupo Administrativo, ni la Subdirección de Desarrollo y Tecnología se hace responsable por pérdida o daño. Toda la información propia de la Unidad del SPE debe quedar almacenada en la nube para los respaldos correspondientes.
g) Al terminar la vinculación laboral de los usuarios, el Grupo Administrativo por medio de la mesa de servicios tecnológicos, generará la solicitud para realizar el proceso de copias de seguridad de los equipos de cómputo, en la nube y correo electrónico del usuario.

ARTÍCULO DÉCIMO SÉPTIMO – USO SERVICIOS DE RED Y VOZ

a) El administrador de la infraestructura tecnológica y personas autorizadas, realizarán el monitoreo, control y detección de forma periódica de los servicios de red, con el fin de salvaguardar la confidencialidad de la información que se transmite por la red, utilizando herramientas tecnológicas de hardware y/o software generando el respectivo reporte a la Subdirección de Desarrollo y Tecnología.
b) El uso de los canales de red y servicios de voz propiedad de la Unidad del SPE, son de uso exclusivo del personal con vinculación vigente de la Unidad del SPE, para aquellos terceros que requieran obtener este recurso debe ser debidamente autorizado por la Subdirección de Desarrollo y Tecnología mediante solicitud a la mesa de servicios tecnológicos.
c) El acceso por escritorio remoto a los servidores, equipos de cómputo y servicios de red, se deben realizar por medio de canales seguros de comunicación, el Subdirector de Desarrollo y Tecnología debe otorgar la autorización a personas que en el desarrollo de sus funciones u obligaciones contractuales deba tener acceso.
d) Los usuarios no deben destruir, manipular, monitorear o capturar la información que circula por los servicios de red de datos o voz.

ARTÍCULO DÉCIMO OCTAVO – USO INTRANET, INTERNET Y WIFI

a) El administrador de la intranet podrá limitar el acceso a las páginas, de acuerdo con el tipo de información, material multimedia, documentos de naturaleza privada, reservada y/o confidencial, para obtener el acceso debe estar debidamente autorizado y sustentado para el desarrollo de las funciones u obligaciones contractuales.
b) Los sujetos obligados deben tener un uso responsable sobre el ingreso a las páginas web, se prohíbe el ingreso a páginas clasificadas con contenido sexual, deportes, novelas, diversión, redes sociales y todas aquellas páginas web prohibidas y no autorizadas.
c) La Subdirección de Desarrollo y Tecnología podrá utilizar software licenciado y autorizado que permita realizar el monitoreo, control y bloqueo de manera automática, de las páginas web que contengan las

categorías de entretenimiento, páginas no autorizadas y redes sociales. Toda excepción debe ser justificada y autorizada por el superior inmediato.

d) Se prohíbe el acceso, carga, descarga, copia, reproducción, almacenamiento o circulación de cualquier tipo de material relacionado con pornografía. En caso de pornografía infantil debe ser informado inmediatamente a las autoridades correspondientes y al jefe de área inmediatamente.
e) El uso del Servicio de Internet debe ser exclusivamente para la realización de las funciones u Obligaciones Contractuales, no puede ser utilizada para actividades comerciales privadas o para propósitos de entretenimiento, acceso y uso a material no autorizado.
f) Al conectarse a través de la opción de red Inalámbrica WiFi, está prohibido recopilar información, datos almacenados sobre terceros, descargar contenido propiedad de la Unidad del SPE sin autorización. Tampoco podrá transmitir y guardar material amenazante, insultante o acosador que degrade la imagen institucional, así como enviar mensajes que contengan spam que puedan ser utilizados en ataques informáticos externos.
g) La red WiFi es de uso exclusivo para los colaboradores de la Unidad del SPE y sus invitados. Aquellos usuarios que no pertenezcan a estos grupos no tienen permitido el uso de este servicio.

CAPÍTULO V: SEGURIDAD FÍSICA Y LÓGICA

ARTÍCULO DÉCIMO NOVENO – SEGURIDAD FÍSICA: establecer las buenas prácticas para el manejo de la información entre los usuarios y la infraestructura tecnológica.

a) Protección de hardware

- El uso de los equipos de cómputo es para los usuarios con vinculación vigente en la Unidad del SPE, los cuales no pueden ser manipulados por usuarios no autorizados.
- Únicamente las personas autorizadas de la Subdirección de Desarrollo y Tecnología y Grupo Administrativo podrán revisar, instalar, trasladar, mover, configurar y proporcionar el soporte a los equipos de cómputo y demás elementos de infraestructura propiedad de la Unidad del SPE.

b) Protección de datos

- Los sujetos obligados son responsables de mantener la confidencialidad, integridad y disponibilidad de la información que se encuentre a su disposición en el desarrollo de sus funciones u obligaciones contractuales.
- Los sujetos obligados deben identificar si la información impresa es clasificada, reservada o si contiene firmas, la cual no se podrá usar como papel reciclable y debe ser destruida inmediatamente cuando ya no sea utilizada para el desarrollo de sus funciones u obligaciones contractuales.
- Los sujetos obligados no deben dejar en sus escritorios documentos o material con información clasificada o reservada, cuya divulgación tenga afectación en la seguridad de la información, hurto o pérdida de datos de la Unidad del SPE.
- La Unidad del SPE como propietario y custodio de la información (física o electrónica) generada como resultado del cumplimiento de su misión, y acogiéndose a la normatividad que le sea aplicable para efectos de la gestión documental institucional, se reserva el derecho de su conservación o destrucción, dependiendo del nivel de criticidad definida para la información con base en los lineamientos del Comité Institucional de Gestión y Desempeño en lo referente a la Gestión Documental.

c) Protección copias de seguridad

- La Subdirección de Desarrollo y Tecnología o quien sea designado debe mantener los repositorios donde se salvaguarda la información bajo los niveles de integridad, confidencialidad y disponibilidad de las copias de seguridad, así como la restauración para consultas y/o usos posteriores.
- La Subdirección de Desarrollo y Tecnología o quien sea designado, debe mantener el mecanismo de autentificación con usuario y contraseña para acceder a los repositorios donde se encuentran almacenadas las copias de seguridad, con el fin de administrar los backups.

d) Protección lógica

- El acceso a los sistemas de información se debe establecer conforme a los roles asignados de acuerdo con las funciones u obligaciones contractuales, generando el respectivo usuario y contraseña para otorgar el acceso a las plataformas tecnológicas de uso exclusivo de la Unidad del SPE.
- El acceso a las plataformas tecnológicas de uso exclusivo de la Unidad del SPE es proporcionado por el administrador del activo de información.

ARTÍCULO VIGÉSIMO – NUBE DE PROCESAMIENTO DE DATOS: es el lugar donde se aloja y realiza el procesamiento de la información de toda la Unidad del SPE, donde se encuentran los servidores, elementos de configuración para el funcionamiento de las aplicaciones, el cuál es catalogada como área restringida.

a) Su acceso es autorizado únicamente por los jefes de dependencia, previo análisis de factibilidad por parte de la Subdirección de Desarrollo y Tecnología.
b) La Subdirección de Desarrollo y Tecnología realizará monitoreo para proteger el flujo de información que entra y sale en la nube de procesamiento de datos.

ARTÍCULO VIGÉSIMO PRIMERO – ACCESO A LOS CENTROS DE CABLEADO: los centros de cableado de las instalaciones físicas de la Unidad del SPE son áreas restringidas, las cuales deben seguir los siguientes lineamientos:

a) El ingreso a los centros de cableado debe ser controlado a través del acompañamiento de la persona de la Subdirección de Desarrollo y Tecnología o el Grupo Administrativo.
b) Al acceso a los centros de cableado debe acatar normas mínimas de seguridad como:
   - No ingresar alimentos
   - No accionar alarmas, únicamente en caso de no ser necesario.
   - No manipular los elementos sin autorización
   - No realizar labores de limpieza con productos dañinos para los dispositivos que se encuentren dentro del área.
   - No desconectar ningún cable o elemento que se encuentre dentro de las instalaciones de los centros de cableado.

CAPÍTULO VI: CIBERSEGURIDAD

ARTÍCULO VIGÉSIMO SEGUNDO – PROTECCIÓN CONTRA CÓDIGO MALICIOSO: los usuarios deben realizar las siguientes actividades relacionadas con la ciberseguridad:

a) Proteger todos los equipos de cómputo de la Unidad del SPE contra códigos maliciosos mediante Antivirus licenciado.
b) Los usuarios deben evitar el envío de archivos o enlaces que sean sospechosos de contener código malicioso.
c) Permitir que los equipos de cómputo realicen las actualizaciones automáticas en sus Sistemas Operativos.
d) Evitar descargar archivos y acceder a enlaces provenientes de páginas de dudosa reputación; en el caso que se requiera una descarga o acceder a un enlace, analizarlos previamente mediante el software antivirus establecido en la entidad.
e) Los usuarios deben evitar realizar transacciones bancarias personales en los equipos de cómputo de la entidad.

ARTÍCULO VIGÉSIMO TERCERO – GESTIÓN DE INCIDENTES DE SEGURIDAD: los usuarios deben reportar o generar oportunamente alertas de la ocurrencia de posibles incidentes de seguridad:

a) Para la gestión de incidentes de seguridad se estructura un equipo de trabajo de la Subdirección de Desarrollo y Tecnología, quienes evaluaran el incidente y gestionaran lo requerido para procurar la continuidad de la operación.
b) Los incidentes de seguridad que afecte la continuidad de la operación de la entidad serán reportados al centro especializado CSIRT Gobierno, y se ejecutarán las recomendaciones indicadas en cuanto al manejo de la seguridad de la información.
c) La Subdirección de Desarrollo y Tecnología documentará los incidentes de seguridad y realizará la debida gestión de las lecciones aprendidas con el fin de responder a futuros ataques.
d) La Subdirección de Desarrollo y Tecnología desarrollará campañas periódicas de concientización en seguridad de la Información, mediante charlas de sensibilización y boletines de seguridad de la información.

CAPÍTULO VII: RELACIONAMIENTO CON TERCEROS Y CONTRATISTAS

ARTÍCULO VIGÉSIMO CUARTO – USO DE DISPOSITIVOS NO INSTITUCIONALES: el tercero o contratista que utilice equipos de cómputo de su propiedad para el cumplimiento de los objetivos del contrato debe cumplir los siguientes requisitos:

a) Debe contar con software legal instalado en su equipo
b) Debe poseer un antivirus activo.
c) La subdirección de Desarrollo y Tecnología verifica las condiciones tecnológicas del equipo en aras de garantizar la integridad de la información.
d) Los terceros que manejen información institucional en sus equipos son responsables de la seguridad de la información tratada.
e) Las aplicaciones de los equipos de cómputo deben ser descargadas en sitios oficiales.

ARTÍCULO VIGÉSIMO QUINTO – ACCESO A INFORMACIÓN CONFIDENCIAL: todos los terceros, contratistas, supervisores, directivos deben propender por la seguridad de la información mediante las siguientes actividades:

a) Los terceros y contratistas deben proteger la confidencialidad de la información antes, durante y después de la ejecución de las actividades objeto del contrato.
b) Los terceros y contratistas deben conocer la Política de Seguridad de la Información y la Política de Tratamiento de Datos.
c) Se debe concientizar a los terceros y contratistas de la relevancia de la seguridad de la Información e invitar a las charlas de sensibilización realizadas por la Subdirección de Desarrollo y Tecnología.
d) Los terceros deben informar inmediatamente al supervisor del contrato cualquier incidente de seguridad que pueda comprometer la seguridad de la información de la entidad.

ARTÍCULO VIGÉSIMO SEXTO – TERCEROS CON ACTIVIDADES DE DESARROLLO DE SOFTWARE: todos aquellos terceros cuya actividad principal requiere la implementación de software deben tener en cuenta los siguientes aspectos:

a) La Subdirección de Desarrollo y tecnología define la arquitectura de seguridad que será tenida en cuenta en el diseño e implementación del software.
b) Se debe garantizar el cumplimiento de los niveles de servicios requeridos y deben ser entregados los manuales técnicos de los sistemas.
c) Las aplicaciones implementadas por terceros deben garantizar el cifrado de contraseñas.
d) Los terceros deben entregar evidencia de que se realizaron pruebas de seguridad al software.
e) Las aplicaciones que tienen interfaz para el ciudadano deben poseer certificados de Seguridad Digital SSL.
f) Los componentes de software implementados por terceros deben contemplar el desarrollo seguro.
g) Se deben realizar pruebas de aceptación del software que verifiquen los requisitos de seguridad pactados.

CAPÍTULO VIII: POLÍTICAS DE USO TRABAJO EN CASA Y/O TELETRABAJO

ARTÍCULO VIGÉSIMO SÉPTIMO – SOLICITUD TRABAJO EN CASA Y/O TELETRABAJO

a) Para los sujetos obligados, el superior inmediato debe enviar la solicitud de acceso externo a los recursos de la Unidad del SPE a través de servicio de VPN, indicando los aplicativos y sistemas de información a los que accede el usuario.
b) El acceso externo a los recursos de la entidad a través del servicio de VPN será concedido por la Subdirección de Desarrollo y Tecnología únicamente bajo circunstancias excepcionales.
c) Los sujetos obligados deben cumplir con las responsabilidades y Políticas de Seguridad de la Información de la Unidad del SPE.
d) En caso de pérdida, hurto o que se presuma que se ha vulnerado la seguridad del equipo en el cual se desarrollan las funciones u obligaciones contractuales trabajo en caso o teletrabajo, será responsabilidad del usuario informar de forma inmediata a la Subdirección de desarrollo y tecnología el evento, con el fin de establecer las medidas de seguridad adecuadas para la protección de la información contenida.

ARTÍCULO VIGÉSIMO OCTAVO – DERECHOS DE AUTOR: La Unidad del SPE no permite bajo ningún motivo la violación de derechos de autor ni de propiedad intelectual, cumpliendo los requisitos legislativos de

reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

a) Todos los productos de software que sean utilizados en la Unidad del SPE bajo los entornos corporativos deberán encontrarse debidamente autorizados y se deberá disponer de la licencia para su funcionamiento.
b) Los sujetos obligados no deben copiar total ni parcialmente libros, artículos, reportajes u otros documentos diferentes de los permitidos por la ley de derechos de autor.

ARTÍCULO VIGÉSIMO NOVENO – SANCIONES: el incumplimiento de las disposiciones anteriores de la presente Política de Seguridad y Privacidad de la Información podrá dar lugar a las sanciones disciplinarias, civiles, penales o investigaciones correspondientes de conformidad con lo dispuesto por la legislación legal vigentes.

ARTÍCULO TRIGÉSIMO – VIGENCIA Y DEROGATORIA: la presente política rige a partir de la fecha de su publicación y deroga todas las disposiciones que le sean contrarias.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D.C. a los 28 de días del mes de junio de 2024.

BIBLIOGRAFÍA

Comisión_de_la_Verdad. (s.f.). *Información Pública Reservada*. Obtenido de https://comisiondelaverdad.co/transparencia/informacion-de-interes/glosario/informacion-publica-reservada#:~:text=Aquella%20que%20re%C3%BAne%20las%20siguientes,la%20ciudadan%C3%ADa%20en%20la%20Ley

Función Pública. (2021). *Ley 1266 de 2008*. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Función Pública. (2021). *Ley 1712 de 2014*. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

ISO. (2022). *Online Browsing Platform*. Obtenido de https://www.iso.org/obp/ui#search

Unión_Europea. (2016). *Diario Oficial de la Unión Europea.* Obtenido de https://www.boe.es/doue/2016/119/L00001-00088.pdf