



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

# UNIDAD ADMINISTRATIVA ESPECIAL DEL SERVICIO PÚBLICO DE EMPLEO

---

## POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN





“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

Nombre del documento	Política de seguridad y privacidad de la información	
Estado del documento:	Versión liberada	
Responsables:	Nombre	Empresa
Elaboró: Alexander Guzmán García - Profesional Universitario Revisó: Víctor Rolando Jaime Velandia - Profesional Especializado María Elena Silva Fandiño- Profesional Especializado Ricardo Abad Chacón Ibarra – Subdirector de Desarrollo y Tecnología	Subdirección 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 de 2019		Versión adicionada
3.0	Sep. de 2020		Versión adicionada
4.0	Octubre de 2020		Versión adicionada
4.1	Junio 2021		Se reestructura la Política de seguridad y privacidad de la información.
4.2	06 diciembre 2021		Adiciono los lineamientos sobre Wifi, adiciono los provisionales a la política.
4.3	16 de diciembre 2021		Presentación y aprobación en el comité de gestión de desempeño
5.0	23 de diciembre 2021		Publicación página institucional



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

## LA UNIDAD ADMINISTRATIVA ESPECIAL DEL SERVICIO PÚBLICO DE EMPLEO (UNIDAD DEL SPE)

### CONSIDERANDO

Mediante el artículo 26 de la Ley 1636 de 2013, se crea la Unidad Administrativa Especial del Servicio Público de Empleo, entidad del orden nacional con personería jurídica, patrimonio propio, autonomía administrativa y financiera, adscrita al Ministerio del Trabajo, para la administración del Servicio Público de Empleo y la Red de Prestadores del Servicio Público de Empleo, la promoción de la prestación del servicio público de empleo, el diseño y operación del Sistema de Información del Servicio Público de Empleo, el desarrollo de instrumentos para la promoción de la gestión y colocación de empleo y la administración de los recursos públicos para la gestión y colocación de empleo entre otras funciones que serán reglamentadas por el Gobierno Nacional.

Por medio del decreto 2521 de 2013, se establece la Estructura de la Unidad del SPE; en el que con el artículo 3, estableció sus funciones, entre las que se encuentran:

1. *“Ejecutar las políticas en materia de la prestación del servicio público de empleo, la gestión del empleo y la intermediación laboral”.*
2. *“Administrar el servicio público de empleo con miras a que se desarrolle con sujeción a los principios de eficiencia, universalidad, igualdad, libre escogencia, integralidad, confiabilidad, transparencia y calidad”.*
3. *“Llevar el registro de las agencias de colocación y bolsas de empleo nacionales y transnacionales”.*
4. *“Monitorear la prestación del servicio público de empleo para constatar la calidad y el resultado obtenido de los servicios prestados por las agencias de colocación y bolsas de empleo autorizadas, y hacer las recomendaciones de reglamentación al Ministerio del Trabajo, cuando a ello haya lugar”.*
5. *“Promover la creación de operadores que presten el servicio público de empleo”.*
6. *“Desarrollar instrumentos para la gestión y colocación de empleo”.*
7. *“Administrar la red de prestadores del servicio público de empleo focalizando sus servicios en los territorios y sectores que requieran las acciones de mitigación del desempleo y organización del servicio público de empleo”.*
8. *“Realizar acciones de articulación y coordinación entre entidades públicas, la red de prestadores y otros actores incidentes para lograr una mejor prestación del servicio público de empleo”.*





“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

9. *“Apoyar la implementación de planes y programas relacionados con el servicio público de empleo para la población vulnerable”.*
10. *“Asesorar y prestar asistencia técnica a las entidades públicas del orden nacional y territorial, la red de prestadores y otros actores incidentes para lograr la mejor organización del servicio público de empleo”.*
11. *“Diseñar, desarrollar y operar el Sistema de Información del Servicio Público de Empleo en condiciones de compatibilidad e interoperabilidad con el sistema de información del Sector Administrativo del Trabajo, el Sistema de Gestión de Empleo para la Productividad y aquellos a los cuales deba integrarse”.*
12. *“Administrar los recursos públicos destinados para la gestión y colocación de empleo que le correspondan, de conformidad con el reglamento que expida el Gobierno Nacional, así como los destinados a la creación de empleos de emergencia y el fomento del empleo en situaciones de emergencia”.*
13. *“Las demás que le señale la Constitución Política y la ley de acuerdo con su misión y naturaleza”.*

De la misma manera el artículo 14 del Decreto 2521 de 2013, estableció las funciones de la Subdirección de Desarrollo y Tecnología, entre las que se encuentran:

1. *“Diseñar y desarrollar en el Sistema de Información del Servicio Público de Empleo las herramientas que permitan incorporar la información para la vinculación de oferta y demanda de empleo, la búsqueda de empleo y la mejora en las condiciones de empleabilidad de los oferentes, bajo los lineamientos de Gobierno en Línea”.*
2. *“Diseñar, mantener y ejecutar acciones de mejora sobre el Sistema de Información del Servicio Público de Empleo en condiciones de compatibilidad e interoperabilidad”.*
3. *“Fijar y divulgar los estándares para la interoperabilidad entre el Sistema de Información del Servicio Público de Empleo y los sistemas de información que tienen los operadores de la red de prestadores de servicio público de empleo, así como los protocolos que permitan incorporar la información recaudada en la red, permitiendo el acceso por parte de los usuarios del Sistema”.*
4. *“Apoyar a los operadores en la construcción y estandarización de sus sistemas de información para la gestión del empleo”.*
5. *“Adelantar las acciones para que el Sistema de Información del Servicio Público de empleo permita divulgar la información proveniente de los procesos de selección, convocatoria y provisión de empleos públicos, en la forma que establezca el gobierno Nacional”.*



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

6. *“Formular y establecer indicadores para el monitoreo y seguimiento del servicio público de empleo en coordinación con las direcciones misionales de la Unidad”.*
7. *“Hacer recomendaciones al Director General sobre la administración e inversión de los recursos públicos para la gestión y colocación de empleo”.*
8. *“Apoyar la implementación y sostenibilidad del Sistema integrado de gestión institucional y sus componentes, en coordinación con las demás dependencias de la entidad”.*
9. *“Atender las peticiones y consultas relacionadas con asuntos de su competencia”.*
10. *“Las demás funciones asignadas que correspondan a la naturaleza de la dependencia”.*

Por lo anterior, y en cumplimiento de estas funciones, se hace necesario implementar la Política de Seguridad y Privacidad de la Información con el propósito de dar cumplimiento a las necesidades a la Unidad del SPE articulando confidencialidad, disponibilidad e integridad de la información.

La Política de Seguridad y Privacidad de la Información establecerá las responsabilidades y objetivos para salvaguardar la información de forma apropiada sobre los activos de información de la Unidad del SPE.

La Política de Seguridad y Privacidad de la Información 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 debe orientar la administración de la seguridad de los activos de información, proporcionando las bases para sensibilizar y salvaguardar los activos de información, así como los datos contenidos en cada instrumento de almacenamiento.

En mérito de lo expuesto,



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

## RESUELVE

**ARTÍCULO PRIMERO – ADOPCIÓN:** Adoptar las Políticas 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 de la Información – MSIP 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 – funcional vigente: Consejo directivo, Dirección General, Subdirección de Administración y Seguimiento, Subdirección de Promoción, Subdirección de Desarrollo y Tecnología, Secretaria General, Órganos de asesoría y coordinación, comisión de personal, comité de coordinación de sistemas de control interno; así también al director(a), 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 comprometerán 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.

## CAPITULO I

**ARTÍCULO TERCERO - OBJETIVO:** Velar por el cumplimiento de la reglamentación vigente, la normatividad aplicable de la seguridad y privacidad de la información entorno 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 de acuerdo con la estructura organizacional – funcional vigente: Consejo directivo, Dirección General, Subdirección de Administración y Seguimiento, Subdirección de Promoción, Subdirección de Desarrollo y Tecnología, Secretaria General, Órganos de asesoría y coordinación, comisión de personal, comité de coordinación de sistemas de control interno; así también al director(a), subdirectores, jefes o



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

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, 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 DE:** De acuerdo con la estructura organizacional – funcional vigente: Consejo directivo, Dirección General, Subdirección de Administración y Seguimiento, Subdirección de Promoción, Subdirección de Desarrollo y Tecnología, Secretaria General, Órganos de asesoría y coordinación, comisión de personal, comité de coordinación de sistemas de control interno; así también al director(a), subdirectores, jefes o coordinadores de oficina, servidores de carrera administrativa, de libre nombramiento y remoción, provisionales, quienes 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) Por medio de la mesa de ayuda de la Unidad del SPE, el grupo administrativo solicita a la Subdirección de Desarrollo y Tecnología la activación de las credenciales de acceso a los diferentes activos de información o plataformas tecnológicas de uso exclusivo de la Unidad del SPE definiendo los niveles de acceso cuando un usuario ha sido vinculado a la Unidad del SPE o trasladado de sus funciones.
- c) Por medio de la mesa de ayuda de la Unidad del SPE, el grupo administrativo solicita inmediatamente a la Subdirección de Desarrollo y Tecnología la inactivación de las credenciales de acceso a los diferentes activos de información o plataformas tecnológicas de uso exclusivo de la Unidad del SPE cuando un usuario ha sido desvinculado de la Unidad del SPE o ha sido retirado de sus funciones de forma temporal, así mismo de los contratistas al vencimiento de sus obligaciones contractuales.
- d) 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.



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

## CAPITULO II

### DEFINICIONES Y TÉRMINOS

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

**Activo de información:** En relación con la seguridad de la información, se refiere a cualquier dato o elemento que está asociado a (sistemas, software, imagen, muebles, enseres, soportes, sedes, personas, etc.) que tenga valor para la organización. (ISO27000)

**Amenaza:** Evento externo que no está bajo el control de la entidad y que aprovecha una debilidad interna para la materialización de un riesgo.

**Análisis de riesgos:** Proceso de comprender la naturaleza del riesgo y determinar su nivel de riesgo.

**Backup:** Son las copias de seguridad de los sistemas de información, bases de datos, equipos de cómputo, que generan un respaldo de la operación para ser conservadas.

**Confidencialidad:** Solo las personas autorizadas deben tener acceso a la información, donde la propiedad de la información no se debe ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

**Contraseña segura:** Mecanismo de protección de acceso a las aplicaciones la cual se compone de letras mayúsculas, letras minúsculas, números y cuya longitud debe ser mínimo de ocho (8) caracteres.

**Control de acceso:** Requerimiento de Seguridad de la Información, lo cual permite denegar o conceder ciertos permisos a los usuarios que manipulan la información de acuerdo con su rol en el desarrollo de sus funciones.

**Dato personal:** El artículo 4 del Reglamento General de Protección de Datos, define que por datos personales se entenderá lo siguiente: *“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”.*







“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

**Dato privado:** Es la información relevante únicamente para el titular<sup>1</sup>, 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, de conformidad con la presente ley<sup>2</sup>.

**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<sup>3</sup>. 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.

**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.<sup>4</sup>

**Datos privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para la Unidad del Servicio Público de Empleo<sup>5</sup>.

**Departamento de procesamiento de datos:** Ubicación física donde se encuentra en operación, concentra, procesa y almacenan los datos e información de una manera sistematizada y automática.

**Disponibilidad:** La información debe estar disponible para los usuarios en el momento en que sea requerida.

**Gestión de riesgos:** Actividades coordinadas para mitigar y controlar al interior de una organización las vulnerabilidades que se pueda presentar.

**Hardware:** Corresponde a todos los componentes físicos y/o partes tangibles de la infraestructura tecnológica y/o computador.

**Información clasificada:** Es la información que se encuentra regulada por las leyes, donde su acceso es por medio de autorización, por contener datos restringidos y sensibles.

<sup>1</sup> WEB. (2019). Industria y Comercio – Superintendencia. – Protección de datos personales. Recuperado URL: <https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales#:~:text=Dato%20Privado%3A,indebido%20puede%20generar%20su%20discriminaci%C3%B3n.>

<sup>2</sup> Ibid

<sup>3</sup> Ibid

<sup>4</sup> WEB. (2021). Función Pública Ley 1266 de 2008. Recuperado URL: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488>

<sup>5</sup> Ibid





“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

**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”*<sup>6</sup>

**Información pública:** Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la Unidad del Servicio Público de Empleo, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.

**Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen Ley 1712/2014

**Infraestructura Tecnológica:** Conjunto de hardware, software y servicios informáticos de la entidad

**Ingeniería Inversa:** Proceso mediante el cual se busca obtener información a partir de un producto con el fin de comprender como está hecho y que lo hace funcionar.

**Integridad:** 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

**Parte interesada (Stakeholder):** Persona u organización que se ven afectados por las acciones de la empresa.

**Propietario de la información:** corresponde al área de la entidad que tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información (insertar, modificar, eliminar). Autoriza divulgación de la información.

**Red LAN:** Es el mecanismo de intercambio de datos e información por medio de la red, la cual es catalogada como Local Área Network, está construida mediante la interconexión de nodos como los son los cables o medios inalámbricos que operan a través de un software de acceso, la conexión se limita ya sea un edificio, planta o habitación.

**Red MAN:** Es el mecanismo de intercambio de datos e información por medio de la red, la cual es catalogada como Metropolitana Área Network, está construida mediante nodos que extienden la cobertura a una geografía y/o extensión de una ciudad, configurados en forma de redes troncales que contienen subredes que se interconectan por medio de un cable par trenzado y cada vez más mediante fibra óptica

<sup>6</sup> <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.>





“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

**Red WAN:** Es el mecanismo de intercambio de datos e información por medio de la red, la cual es catalogada como Wide Área Network, está construida por los medios que proporcionan los operadores de telecomunicaciones en cada uno de los países utilizando el método de conmutación de paquetes para que el enrutamiento de la información se adapte a los estándares de cada país, la cobertura es a nivel mundial.

**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 consideraciones. (ISO Guía 73:2002).

**Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, conforme a los lineamientos establecidos por la alta gerencia.

**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, objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

**Software malicioso:** Conocido como malware, diseñado por medio de códigos al interior de un software con el objetivo de infiltrarse, dañar o controlar el sistema de una computadora sin el consentimiento y conocimiento de su propietario.

**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.



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

### CAPITULO 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 – funcional vigente, 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:

**7.1. 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.

**7.2. Derechos de acceso:** La Unidad del SPE podrá utilizar herramientas tecnológicas o instrumentos para monitorear el uso de su Infraestructura Tecnológica y aquel activo de información almacenado en los equipos de cómputo, DRIVE, o cualquier otro medio para salvaguardar los datos, los cuales pueden ser transmitidos, divulgados, recibido 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.

El acceso a la información es autorizado por el propietario de esta misma.

**7.3. 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, 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 Google DRIVE y/o computadoras.

**7.4. Mal uso del recurso tecnológico:** Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente, con acceso a los recursos de información de la Unidad del SPE deben abstenerse de realizar acciones que impliquen un desperdicio de los recursos de la Infraestructura Tecnológica y/o insumos suministrados por la Unidad del SPE, el cuál conlleven a la monopolización, obstaculización, acaparamiento o uso personal de los recursos tecnológicos.



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

**7.5. Uso inadecuado del software:** Los usuarios no deben efectuar ninguna de las siguientes actividades:

- a) Copiar software licenciado o adquirido por la Unidad del SPE para uso personal o beneficio de terceros.
- b) Copiar las claves de los productos adquiridos por la Unidad del SPE y utilizarlas para uso personal o beneficio de terceros.
- c) Instalar software no licenciado o no autorizado por la Unidad del SPE en los servidores y equipos de cómputo de la Unidad del SPE.
- d) Intencional o fortuitamente introducir software malicioso en la Infraestructura Tecnológica de la Unidad del SPE.
- e) Copiar, transformar, revisar, adaptar y/o modificar cualquier software de la Unidad del SPE sin previa autorización.
- f) 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.
- g) Utilizar software que permita capturar el tráfico de datos generado al interior de la Unidad del SPE. De ser requerido el proceso de capturar el tráfico de datos debe contar con la respectiva autorización del superior inmediato, el cuál debe ser informado en la mesa de ayuda por medio de requerimiento a la Subdirección de Desarrollo y Tecnología expreso en el desarrollo de sus funciones u obligaciones contractuales.
- h) Utilizar software, hardware o cualquier tipo de tecnología para capturar o interceptar tráfico de voz en su origen, destino o al interior de la Unidad del SPE. De ser requerido el proceso de capturar el tráfico de voz debe contar con la respectiva autorización del superior inmediato, el cuál debe ser informado en la mesa de ayuda por medio de requerimiento a la Subdirección de Desarrollo y Tecnología expreso en el desarrollo de sus funciones u obligaciones contractuales.
- i) Copiar, vender, modificar, alterar cualquier tipo de información sensible, reservada, privada, confidencial y personal de la Unidad del SPE sin la autorización respectiva.

**7.6 Uso inadecuado del suministro eléctrico:** Los usuarios de la Unidad del SPE no deben conectar a las fuentes reguladas los dispositivos electrónicos que no se encuentran autorizados.



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

#### **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 de acuerdo con la estructura organizacional – funcional vigente deben almacenar en el DRIVE la información producida para la Unidad del SPE.
- b) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente 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, envío de correo electrónico y demás actividades es responsabilidad de cada usuario, las cuales fueron generadas con la cuenta asignada.
- c) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente deben apagar sus equipos de cómputo al culminar la jornada laboral. Únicamente podrán quedar prendidos aquellos equipos de cómputo que cuenten 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 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) La Subdirección de Desarrollo y Tecnología configurara el bloqueo automático de los computadores después de un tiempo determinado de inactividad del equipo. Es



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

responsabilidad del usuario mantener siempre bloqueado el equipo de cómputo al retirarse del puesto de trabajo.

- h) Aquellos contratistas que en el desarrollo de sus obligaciones contractuales 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 sistemas de información que hacen parte de la Unidad del SPE, asignando el perfil y rol correspondiente, para lo cual tendrá en cuenta los siguientes parámetros:

- a) Realizar la asignación de usuarios de la siguiente forma:
  - 1. Incorporar al usuario en el sistema de información de la Unidad del SPE con primer nombre punto primer apellido.
  - 2. Cuando existan usuarios en el sistema de información con el mismo primer nombre y mismo primer apellido, se debe incorporar el estándar primer nombre punto segundo apellido.
- b) Definir la periodicidad de caducidad de las contraseñas, en cada uno de los sistemas de información que hacen parte de la Unidad del SPE, como por ejemplo el directorio activo, correo electrónico, etc.
- c) 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 se debe recalcar y generar comunicados y/o boletines indicando la importancia de las contraseñas seguras y como debe ser su estructura.
- d) Eliminado un usuario de la cuenta de correo institucional, se deben respaldar los documentos compartidos, así como la información que estén asociados a la cuenta, generando la respectiva copia de seguridad en el repositorio dispuesto por la Unidad del SPE.





“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

- e) 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.
- f) 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 a través de las herramientas y sistemas de información productores de logs de auditoría.
- g) La contraseña es de carácter personal e intransferible, esto quiere decir, todo evento registrado y ejecutado es responsabilidad del usuario asociado.
- h) Es responsabilidad de cada usuario salvaguardar las contraseñas entregadas y modificadas por el mismo usuario, las cuales generan el acceso a cada una de las aplicaciones de la Unidad del SPE, las cuales deben ser cambiadas periódicamente.

**ARTÍCULO DÉCIMO – RESPALDO DE INFORMACIÓN (BACKUP):** Es responsabilidad del administrador de la Infraestructura Tecnológica, Correo Electrónico, Equipos de Cómputo y demás aplicaciones donde se deban generar las copias de seguridad, el salvaguardar los archivos correspondientes a la información propiedad de la Unidad del SPE dando cumplimiento a las siguientes reglas:

- a) El Grupo administrativo por medio de solicitud expresa en la mesa de ayuda a la Subdirección de Desarrollo y Tecnología, indicara el trámite de cancelación y/o suspensión de la cuenta de correo electrónico y de accesos o plataformas tecnológicas de uso exclusivo de la Unidad del SPE, así como la cancelación del registro de huella dactilar en el sistema biométrico.
- b) La realización de las copias de seguridad de los servidores de la Unidad del SPE es responsabilidad de la Subdirección de Desarrollo y Tecnología o quién esté a cargo de la gestión y operación de la Infraestructura Tecnológica, este procedimiento debe estar documentado.
- c) Se debe establecer una periodicidad para realizar las copias de seguridad a los servidores de la Unidad del SPE de acuerdo con los recursos de almacenamiento disponibles. Así





“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

mismo, la Subdirección de Desarrollo y Tecnología o quién esté a cargo de la gestión y operación de la Infraestructura Tecnológica debe elaborar el Plan de Backups de acuerdo con las necesidades expresadas por las áreas y/o Subdirecciones propietarias de la información.

#### **ARTÍCULO DÉCIMO PRIMERO – 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 o de 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 trate 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 visualizarse 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 para ejecutar las medidas correctivas adecuadas.



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

## **ARTÍCULO DÉCIMO SEGUNDO – USO DE DISPOSITIVOS MÓVILES:**

- a) Mantener la seguridad de la información propiedad de la Unidad del SPE, cuando se consulte, transmita, almacene información por medio de los móviles, utilizando redes de datos de la Unidad y de terceros.
- b) 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 protección de datos personales.
- c) 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.
- d) 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 cabeza del Grupo Administrativo 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 TERCERO – 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.



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

- c) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente deben velar por la confidencialidad, integridad y seguridad de los datos sobre la información clasificada, reservada o datos personales, privados y/o sensibles, debida 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.
- e) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente deben proteger física y lógicamente el medio removible.

#### **ARTÍCULO DÉCIMO CUARTO – ESCRITORIOS ORGANIZADOS – PANTALLA LIMPIA**

- a) Mantener la documentación generada, almacenada o dispuesta en los escritorios que se encuentran en las instalaciones de la Unidad del SPE en sus respectivos muebles para evitando pérdida, daño o fuga de información, manteniendo las medidas de protección adecuadas para salvaguardar la información clasificada, publica, 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 de acuerdo con la estructura organizacional – funcional vigente 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.



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

- e) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente 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 realizara el proceso para mantener el mobiliario funcional.
- f) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente que tenga 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 QUINTO – INVENTARIO DE INFRAESTRUCTURA TECNOLOGÍA**

- 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 proporciono 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



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

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 el DRIVE para los respaldos correspondientes.
- g) La Subdirección de Desarrollo y Tecnología mantendrá actualizado el inventario de equipos de cómputo y periféricos instalados en la Unidad.
- h) Al terminar la vinculación laboral de los usuarios, el Grupo Administrativo por medio de la mesa de ayuda generará la solicitud para realizar el proceso de copias de seguridad de los equipos de cómputo, DRIVE y correo electrónico del usuario.
- i) Todo equipo de cómputo nuevo adquirido debe ser reportado a la Subdirección de Desarrollo y Tecnología, al igual que debe ser inventariado en el documento asignado por la Unidad del SPE para llevar el control de estos.

## **ARTÍCULO DÉCIMO SEXTO – USO SERVICIOS DE RED Y VOZ**

- a) El administrador de la infraestructura tecnología 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 en el formato para uso servicios de red.
- 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.



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

- 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 SÉPTIMO – 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 de acuerdo con la estructura organizacional – funcional vigente no deben utilizar la internet para realizar búsquedas de entretenimiento, páginas no autorizadas y redes sociales.
- c) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente 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 y todas aquellas páginas web prohibidas.
- d) 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.
- e) 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.
- f) El uso del Servicio de Internet debe ser exclusivamente para la realización de las funciones u Obligaciones Contractuales, de tal forma, que, al acceder a páginas con contenido multimedia, para la visualización de videos o escuchar música, estará afectando directamente a todos los colaboradores de la Unidad del SPE, asimismo, la visualización de material multimedia (videos) o escucha de audios en redes sociales como Facebook o TikTok, impactará también negativamente a los demás colaboradores.



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

- g) Está restringido la conexión de dispositivos móviles a las redes wifi.
- h) 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 mensajería como spam que pueda ser utilizados en ataques informáticos externos.
- i) Al conectarse a través de la opción de red inalámbrica WIFI, no se podrá acceder a las aplicaciones de uso exclusivo de la Unidad del SPE sin previa autorización
- j) La contraseña para acceder a la red inalámbrica WiFi debe ser cambiada periódicamente con el fin de evitar contraseñas predeterminadas.
- k) Las redes inalámbricas no deben radiar su nombre de red por medio del SSID (identificador de red de servicio).
- l) La controladora de redes WiFi debe tener mecanismos de protección de uso y acceso.
- m) 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.
- n) Al conectarse a través de la opción de red Inalámbrica WiFi, debe ser consiente que trabajará con las siguientes limitaciones:
  - La Unidad del SPE tendrá una conexión variable en calidad de la señal debido a la distancia desde donde se estará conectando, al dispositivo activo de red de comunicaciones (Access Point - AP) que permite la conexión a la red WiFi.
  - Rendimiento variable dependiendo de la cantidad de usuarios conectados y aplicaciones/páginas en uso.



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

- Debido a las características físicas propias del medio compartido de propagación (Aire), existen afectaciones inherentes a este tipo de tecnologías inalámbricas, que no tiene una conexión por red cableada, tales como:
  - i. Interferencias en la señal causadas por materiales como metal, concreto, yeso, vidrio, cemento o madera que generan una degradación de la potencia de la señal o incluso la ausencia de conexión, técnicamente se produce una absorción de la señal.
  - ii. Adicional a la absorción de la señal, una señal inalámbrica debe convivir con afectaciones derivadas con la forma en que se propaga la señal, tales como: refracción (cambio en la dirección y velocidad), difracción (obstrucción en la trayectoria generando un cambio de dirección), reflexión (modificación en la dirección, p.e un espejo) y dispersión (descomposición de la señal original).
  - iii. Señales WiFi-adyacentes que no son de la Unidad del SPE también afectan la señal Inalámbrica, tales como las que son detectadas del mismo piso o pisos superiores o inferiores.

## CAPITULO V

### SEGURIDAD FÍSICA Y LÓGICA

**ARTÍCULO DÉCIMO OCTAVO – SEGURIDAD FÍSICA:** Establecer las buenas prácticas para el manejo de la información entre los usuarios y la infraestructura tecnología.

#### 8.1. Protección de hardware:

- a) 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.
- b) Es obligatorio el uso y porte del carné que lo acredita como usuario con vinculación vigente en la Unidad del SPE en un lugar visible, con el propósito de mantener el control y desplazamiento sobre el acceso de personas a las instalaciones de la Unidad del SPE. Cuando el carné el olvidado para el ingreso a las instalaciones de trabajo, se debe





“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

registrar en la entrada para la respectiva asignación de tarjeta y poder desplazarse al lugar donde se desarrollan las funciones u obligaciones contractuales.

- c) 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, servidores y demás elementos de infraestructura propiedad de la Unidad del SPE.

## 8.2. Protección de datos

- a) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente 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.
- b) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente 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.
- c) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente no deben dejar en sus escritorios documentos o material con información clasificada o reservada, cuya divulgación tenga afectación en la seguridad, hurto o pérdida de datos de la Unidad del SPE.

## 8.3. Protección copias de seguridad

- a) La Subdirección de Desarrollo y Tecnología o el administrador de infraestructura 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.
- b) La Subdirección de Desarrollo y Tecnología o el administrador de infraestructura, debe mantener el mecanismo de autenticación con usuario y contraseña para acceder a los



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

repositorios donde se encuentran almacenadas las copias de seguridad, con el fin de administrar, incorporar los nuevos backup, eliminar backup antiguos conforme al plan de contingencia para para aumentar el espacio en el repositorio.

#### **8.4. Protección lógica**

- a) 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 otorga el acceso a las plataformas tecnológicas de uso exclusivo de la Unidad del SPE.
- b) El acceso a las plataformas tecnológicas de uso exclusivo de la Unidad del SPE es proporcionado por el administrador del activo de información.
- c) La Subdirección de Desarrollo y Tecnología debe sincronizar automáticamente la hora y fecha de los equipos de cómputo, servidores con la establecida con el país y región en la que se encuentran.

**ARTÍCULO DÉCIMO NOVENO – 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.
- 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 – INSTALACIONES ELÉCTRICAS Y DE COMUNICACIONES:** La infraestructura tecnológica debe contar con una fuente alterna de alimentación eléctrica generada de una UPS, con el propósito de mantener la energía cuando se presenten caídas de energía inesperadas.

- a) El ingreso a las instalaciones eléctricas y de comunicaciones debe ser controlado con su respectivo acompañamiento de la persona de la Subdirección de Desarrollo y Tecnología asignada.
- b) Al acceso las instalaciones eléctricas y de comunicaciones debe acatar normas mínimas de seguridad como.
  - a. No ingresar alimentos





“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

- b. No accionar alarmas, únicamente en caso de no ser necesario.
- c. No manipular los equipos de cómputo sin autorización
- d. No realizar labores de limpieza con productos dañinos para los equipos de cómputo, periféricos y demás elementos electrónicos, eléctricos, etc. Que se encuentren dentro del área.
- e. No desconectar ningún cable o elemento que se encuentre dentro de las instalaciones eléctricas y de comunicaciones.

## **CAPITULO VI**

### **POLÍTICAS DE USO TRABAJO EN CASA Y/O TELETRABAJO**

#### **ARTÍCULO VIGÉSIMO PRIMERO – SOLICITUD TRABAJO EN CASA Y/O TELETRABAJO**

- a) Para los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente el superior inmediato debe enviar la solicitud de acceso externo a la red y aplicaciones de la Unidad del SPE, indicando los aplicativos y sistemas de información que accederá el usuario.
- b) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente deben conectarse a través de escritorio remoto a los equipos de cómputo de la Unidad del SPE con su respectivo usuario y contraseña, por medio de la VPN asignada por la Subdirección de Desarrollo y Tecnología.
- c) La Subdirección de Desarrollo y Tecnología establecerá el mecanismo de conexión a escritorio remoto, salvaguardando la seguridad del canal de comunicación, con sus respectivos registros de autoría, estableciendo los accesos a los sistemas de información y datos necesarios para el desarrollo de las funciones u obligaciones.
- d) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente deben cumplir con las responsabilidades y Políticas de Seguridad de la Información de la Unidad del SPE.
- e) 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.



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

**ARTÍCULO VIGÉSIMO SEGUNDO – 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) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente no pueden realizar copia de los productos de software puestos a su disposición para el desempeño de sus funciones u obligaciones contractuales.
- b) Todos los productos software que sean utilizados en la Unidad del SPE bajo los entornos corporativos deberán encontrarse debidamente autorizados y se deberá disponer de la correspondiente licencia para su función correspondiente.
- c) La Subdirección de Desarrollo y Tecnología debe mantener el inventario del software autorizado donde se registrará como mínimo:
  - a. Nombre del Software
  - b. Tipo de licencia
  - c. Cantidad de licencias
  - d. Documentos soporte de la licencia
  - e. Documento de transferencia de derechos de autor para los desarrollos internos o contratados.
- d) Los sujetos obligados de acuerdo con la estructura organizacional – funcional vigente 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 SEGUNDO – 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.



“Por la cual se establecen los lineamientos y estándares para la adopción de las políticas de seguridad y privacidad de la información en la Unidad del Servicio Público de Empleo (Unidad del SPE)”

**ARTÍCULO VIGÉSIMO TERCERO – VIGENCIA Y DEROGATORIA:** La presente resolución 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 23 de días de mes de Diciembre del 2021

