

# Boletín

EDICIÓN  
**INSTITUCIONAL 012**

Mantente informado ¡Novedades y noticias!

## 03 **POLÍTICAS**

Cambios en teletrabajo.

## 04 **SEGURIDAD**

Lecciones aprendidas, accidentes de trabajo.

## 06 10 12 16 **TECNOLOGÍA**

¿Cómo recuperarse de un ciberataque?

Seguridad en Redes informáticas.

Tips para mantener la seguridad informática y evitar el robo de información.

Alcance. Finalidades del tratamiento de datos personales.

## 14 **ENCUENTROS**

Encuentro Regional Región Cafetera

## 08 **DIRECCIONAMIENTO ESTRATÉGICO**



---

## EDITORIAL

EQUIPO EDITORIAL  
Equipo de Comunicaciones

TEXTOS Y EDICIÓN  
• Subdirección de Desarrollo y Tecnología  
• Planeación  
• Grupo de Estudio  
del Mercado Laboral  
• Equipo de Comunicaciones

COORDINACIÓN DE CONTENIDOS  
María Alejandra Torres Romero  
Wilmar Lozano Rico

---

## DISEÑO

DISEÑO Y DIAGRAMACIÓN  
María Alejandra Villafranca Pineda

FOTOGRAFÍA E ILUSTRACIONES  
<https://freepik.com>

PUBLICACIÓN  
<https://issuu.com/SPE>





# CAMBIOS EN Teletrabajo

Los días de teletrabajo definidos en el Acuerdo de Teletrabajo solamente **se podrán modificar a través de la suscripción de un nuevo acuerdo**, el cual una vez firmado por las partes debe remitirse mediante GESDOC a la Coordinación de Talento Humano para el trámite correspondiente ante la ARL.



Para el caso en que haya cambio de empleo o dependencia el servidor público (teletrabajador) deberá realizar una nueva solicitud para aplicar a esta modalidad, cumpliendo con lo determinado en el procedimiento para tal fin.

Cuando el jefe inmediato o el teletrabajador, requieran modificar las condiciones pactadas, tales como la distribución de la prestación del servicio entre teletrabajo y presencial y/o el horario de trabajo, se debe radicar a través del sistema de gestión documental, el acuerdo de teletrabajo actualizado y debidamente firmado, cuyas condiciones empezarán a regir una vez se reporten a la ARL. Hasta tanto ello ocurra, las condiciones se deben mantener para efectos de la cobertura en riesgos laborales. El nuevo acuerdo se remite a la Coordinación del Grupo de Talento Humano.

Cuando el teletrabajador cambie de lugar de teletrabajo y desee continuar con la modalidad, deberá informar al Grupo de Talento Humano las nuevas condiciones y características de su puesto de teletrabajo, para que el responsable del SG-SST y/o el profesional de la Subdirección de Desarrollo y Tecnología realicen las verificaciones que consideren pertinentes para confirmar que el puesto es apto.

Si ocurre cambio del jefe inmediato, se debe radicar a través del sistema de gestión documental, el acuerdo de teletrabajo actualizado y debidamente firmado, dirigido a la Coordinación del Grupo de Talento Humano. 📍

# Lecciones

## APRENDIDAS, ACCIDENTE DE TRABAJO

En ocasiones se pueden presentar **lesiones músculo esqueléticas**, relacionados con la inadecuada manipulación de cargas o de objetos, por tal razón les sugerimos que, al levantar cargas o determinados objetos, tengan en cuenta estos 7 pasos:



1

Tener en mente que el autocuidado mejora la calidad de vida.



2

Separar las piernas de modo que queden paralelas a la distancia de los hombros. »



3

Flexionar las piernas y mantener la espalda recta.



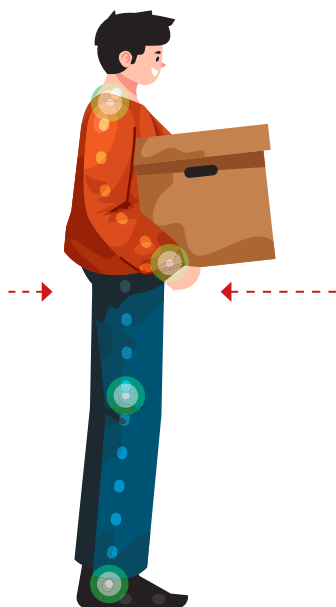
5

Hacer la sujeción del objeto firmemente.



4

Mantener la carga cerca al cuerpo a la altura de la cintura.



6

Realizar la fuerza con las piernas y los brazos.



7

Realizar pausas activas durante la jornada de trabajo.



Adicionalmente, evitar:

- Levantar objetos por encima de la cabeza
- Girar el cuerpo bruscamente de un lado a otro
- Inclinarse a tomar el objeto haciendo la fuerza con la columna. 📍



# ¿CÓMO RECUPERARSE DE UN ciberataque?

Por: Alexander Guzmán García

Los ciberataques se han convertido en los mecanismos en que los delincuentes por medio de sus conocimientos logran acceder a equipos de cómputo a través del acceso no autorizado.

Estos mecanismos es donde los delincuentes **logran robar, destruir, capturar, alterar, inhabilitar y exponer información de la organización afectada**, donde toda la infraestructura queda bloqueada por un tiempo determinado, donde los sistemas de información no pueden operar a fin de paralizar el proceso de producción, por tal motivo se pierde confianza en la empresa que paso por el incidente, donde algunas veces deben responder de forma legal, penal ante la situación presentada.

Las organizaciones a través de sus planes de adquisiciones deben contemplar rubros en infraestructura de seguridad, donde puedan proteger la información que se almacena y se recolecta de los clientes, con el fin de mantener un servicio optimo y en buen funcionamiento para cualquier consulta, por tal motivo para recuperarse de un ataque cibernético es indispensable contar: »





- Plan de respuesta ante incidentes
- Realizar ejercicio de ciberataques internos - Practicar eventos de ciberseguridad
- Mantenerse actualizado sobre las regulaciones en ciberseguridad.
- Realizar convenios con expertos en seguridad
- Adquirir escaneos contantes de la red.
- Mantener actualizados los software y antivirus
- Segmentar la red
- Bloquear la comunicación con el exterior
- Dar acceso a las páginas que se requieren para el desarrollo de las funciones
- Cyber Kill Chain.

## COMO SE EJECUTA UN CIBERATAQUE:

Se realiza en 3 etapas:



### RECONOCIMIENTO:

Analizan la victima.



### PREPARACIÓN:

Recopilan la información de cómo funcionan sus sistemas.



### DISTRIBUCIÓN:

Envían el virus con el que van a controlar los equipos de cómputo y restringir el acceso a los propietarios de la infraestructura. 📍

# Estratégico

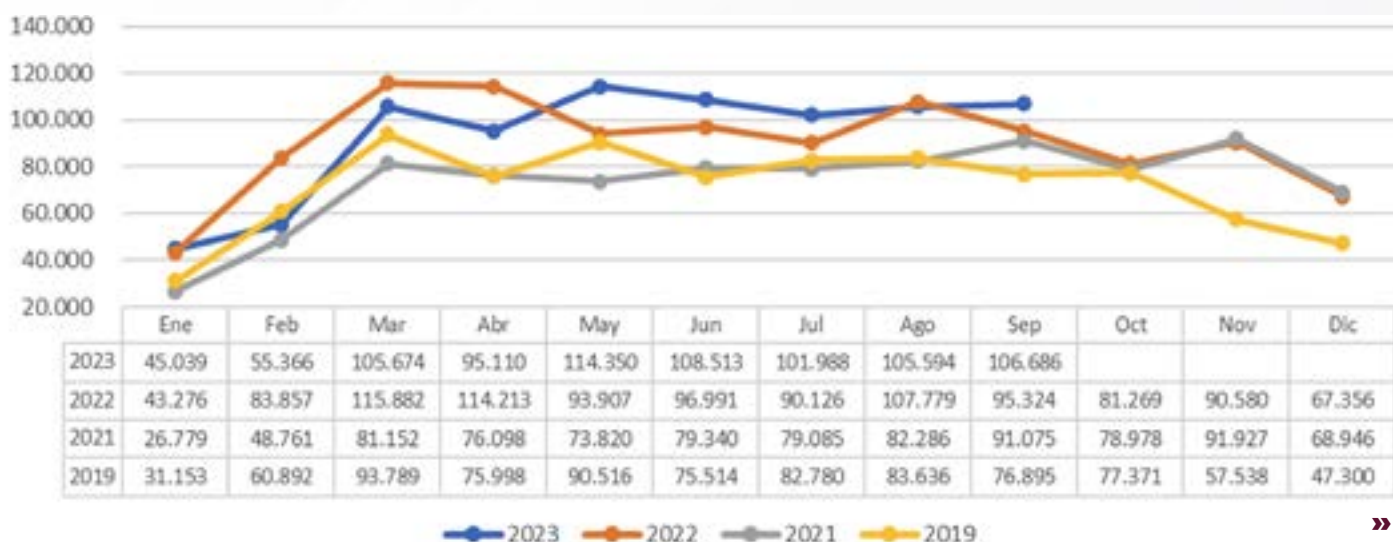
## DIRECCIONAMIENTO

### 1. Dato de colocaciones a corte Septiembre

Se ha visto un avance en las colocaciones a través del servicio público de empleo frente a los años anteriores, te invitamos a conocer la información en cifras que traemos para ti:



| 2023                         | 2022 - 2023                       | 2021 - 2023                       | 2019 - 2023                       |
|------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|
| Variación agosto- septiembre | Variación septiembre - septiembre | Variación septiembre - septiembre | Variación septiembre - septiembre |
| <b>1,0%</b>                  | <b>10,6%</b>                      | <b>14,6%</b>                      | <b>27,9%</b>                      |



## NUESTRA GESTIÓN PERMITE RESALTAR LAS SIGUIENTES CIFRAS:



Colocaciones  
a través del Servicio  
Público de Empleo:  
**838.320**



Colocaciones  
de **víctimas:**  
**108.095**



Colocaciones  
de **jóvenes:**  
**356.983**



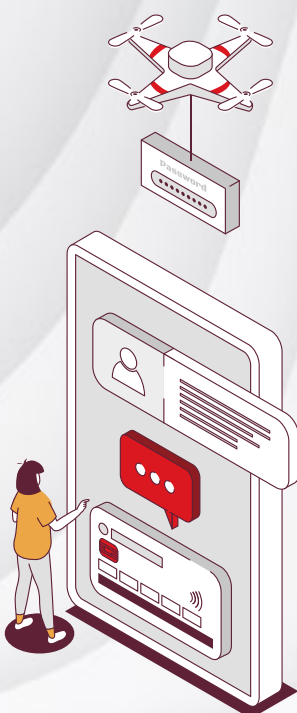
Colocaciones  
de **mujeres:**  
**384.440**



Colocaciones de  
personas en **condición**  
de **discapacidad:**  
**3.216**

## 2. Jornada de planeación estratégica:

El 13 de octubre toda la Unidad se comprometió en el alistamiento y concertación de los retos a asumir en el marco de la gestión institucional. Se logró la identificación de nuevas oportunidades para mejorar la gestión, así como el fortalecimiento del relacionamiento de los diferentes equipos de trabajo, que contribuyó de manera interdisciplinaria en la construcción de los acuerdos para llevar a cabo el cumplimiento de los objetivos institucionales.



## 3. Capacitación transparencia:

Desde la dirección general, el equipo de planeación llevó a cabo la capacitación sobre transparencia y acceso a la información, como mecanismo para fomentar la transparencia activa y pasiva entre los diferentes equipos de trabajo. De igual manera, se presentaron aquellos instrumentos diseñados para promover la transparencia y el relacionamiento de con los diferentes grupos de valor de la entidad.

## 4. ¿Sabes qué es la gestión del conocimiento?

Es la sexta dimensión del Modelo Integrado de Planeación y Gestión – MIPG- es transversal a todas y busca que las entidades públicas analicen la forma en la que generan, capturan, evalúan y distribuyen el conocimiento con el fin de aprender de sí mismas y de su entorno, con el objetivo de mejorar su gestión.

Es por esto que la Unidad del SPE se encuentra realizando la actualización del inventario del capital intelectual y de las necesidades de investigación, en los próximos días recibirás el link para el diligenciamiento de las matrices.

## 5. Rendición de cuentas 2023

Actualmente todos los equipos de trabajo de la Unidad están adelantando el proceso de rendición de cuentas a la ciudadanía, como un compromiso con la transparencia activa y el fortalecimiento de la relación entidad – grupos de valor. El proceso de rendición de cuentas se está desarrollado en las siguientes fases:

- Identificación de los logros alcanzados en la vigencia 2023 por parte de los diferentes equipos de trabajo (para socialización en página web y redes).
- Preparación del informe de rendición de cuentas 2023 con los datos detallados de cada equipo de trabajo y que dan cuenta de la gestión que adelantó la Unidad durante todo el año.
- Audiencia pública de rendición de cuentas a través de la cual se mostrarán los hitos alcanzados en este 2023 a todos los grupos de valor. 📍



# Seguridad

## EN REDES INFORMÁTICAS

Por: Alexander Guzmán García

La seguridad de las redes comprende las actividades y mecanismos orientados a proteger las aplicaciones, dispositivos, sistemas, accesos no autorizados, uso e integridad de la red corporativa, con el fin de **resguardar la infraestructura, al igual que los datos que se transmiten por el canal de comunicación**, frente a las amenazas internas y externas.

### ¿Cómo funciona la seguridad de la red?

La seguridad se centra en dos componentes:



#### **Autenticación:**

verifica que eres quien dice ser.



#### **Autorización:**

válida si tienes los privilegios para acceder a los recursos del sistema de información. »



## La seguridad de la red implica

- Cumplir políticas y procedimientos
- Administrar el acceso a la red
- Incluye la instalación de software y hardware que pueda detectar y bloquear amenazas de forma automática
- Implementar los controles que se ajustan a las necesidades

## ¿En qué me beneficia la seguridad de red?

Ayuda a proteger la reputación de la empresa, porque los datos e información confidencial se encuentran debidamente protegidos, sin que se exponga al público.



## Tipos de seguridad de red



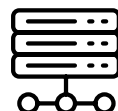
### Firewalls:

incorporan una barrera entre la red interna y la externa, por medio de reglas para permitir el ingreso o bloqueo de información.



### Seguridad del correo electrónico:

verificación de los correos entrantes y salientes que no contengan códigos maliciosos o sean *phishing* para prevenir la pérdida de datos sensibles.



### Segmentación de la red:

clasificación de la información que se trasporta por la red en distintas categorías, las cuales facilitan la aplicación de las políticas de seguridad, no solo en las direcciones IP, sino también en la identidad de los EndPoints (Dispositivo informático comunicado a través de una red. Como, por ejemplo: Equipos de cómputo, portátiles, teléfonos inteligentes, Tablet) [3]. Asignando los derechos de acceso por perfiles, roles y ubicación, otorgando el permiso de forma puntual a cada usuario. 🔗



### Control de acceso a la red (NAC):

permite mantener identificado a los usuarios y dispositivos que ingresan a la red.



### Software antivirus y antimalware:

herramientas que realizan escaneo y seguimiento constante de los archivos para detectar anomalías, eliminar malware y reparar daños.



IBM. (2023). ¿Qué es la seguridad de red? | IBM Recuperado de la URL: <https://www.ibm.com/co-es/topics/network-security>

CISCO. (2023). ¿Qué es la seguridad de red? Recuperado de la URL: [https://www.cisco.com/c/es\\_mx/products/security/what-is-network-security.html#~tipos](https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html#~tipos)



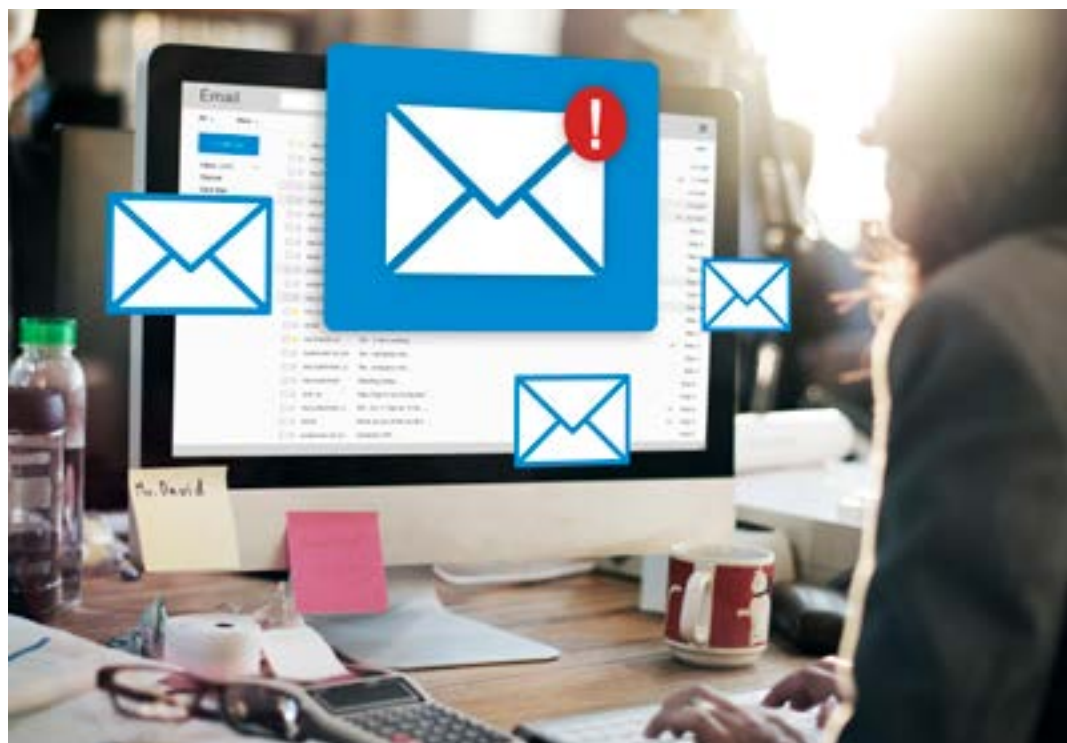
# Tips para mantener la seguridad informática

## Y EVITAR EL ROBO DE información

Por: Alexander Guzmán García

La ciberseguridad es un aspecto omnipresente en nuestras actividades diarias.

Por lo tanto, es crucial mantener una vigilancia constante ante cada correo electrónico, mensaje, llamada o texto que recibimos, a fin de prevenir caer en posibles trampas y evitar convertirnos en víctimas de incidentes de seguridad. Es esencial estar siempre alerta y adoptar prácticas seguras en línea: »



## Recomendaciones de Seguridad al Navegar en Internet

- Cuidado al publicar en redes sociales.
- Activar las configuraciones de privacidad en las plataformas digitales utilizadas.
- Adoptar prácticas seguras durante la navegación en línea.
- Asegurarse de que la conexión a la red esté protegida, especialmente en entornos públicos.
- Descargar contenido de fuentes confiables.
- Crear contraseñas seguras y actualizarlas de manera periódica.
- Mantener actualizado el antivirus.
- Evitar el intercambio de información a través de dispositivos USB que puedan contener virus o ejecutables dañinos.
- No abrir enlaces sospechosos en correos electrónicos y verificar la autenticidad de los remitentes.
- Ser cuidadoso al utilizar servicios wifi públicos o proxy, que actúan como puentes entre el origen (un ordenador) y el destino de una solicitud (internet).
- Encriptar los archivos personales, es decir, codificar el contenido y colocarles claves de seguridad.
- Cambiar regularmente las contraseñas para mantener la seguridad de las cuentas.
- Verificar las páginas donde se descarga información, documentos, música, videos, textos, etc. Verificar que sean sitios conocidos o seguros, cuyos archivos descargados sean analizados inmediatamente cuando están en los equipos de cómputo o dispositivos.
- Mantener actualizado el antivirus y los sistemas operativos.

En un entorno digital constantemente amenazado, la vigilancia continua es esencial para mitigar riesgos y proteger la seguridad en línea. 🔒



Siete tips para mantener la seguridad informática y evitar el robo de información. URL del artículo: <https://www.uncuyo.edu.ar/development/siete-tips-para-mantener-la-seguridad-informatica-y-evitar-el-robo-de-informacion>



## Prestadores de la Zona Cafetera unidos por la

# la inclusión EN EL EMPLEO

Alrededor de 100 representantes del sector empresarial de Antioquia, Caldas, Quindío y Risaralda se congregaron en **Medellín** para promover la igualdad de oportunidades laborales en la zona cafetera del país.



Esta reunión fue parte de la denominada gira de “Encuentros Regionales, Inclusión y Equidad en el Empleo”, que se viene realizando en el país.

El evento reunió a los principales actores del mercado laboral de la región Antioqueña y Eje Cafetero, con el propósito de brindar herramientas técnicas a los prestadores para optimizar sus procesos de gestión y colocación de empleo, desde un enfoque de género y poblacional.

En el marco del Encuentro Regional se realizó un panel de discusión con líderes y expertos del ecosistema laboral para trazar un camino hacia un mercado laboral más

incluyente y lleno de oportunidades para todos y todas en la zona cafetera.

En este ejercicio, los participantes coincidieron en la necesidad de construir puentes hacia un mercado laboral más justo y equitativo que rompa con las brechas que limitan el acceso a trabajos dignos y decentes en toda la extensión de los departamentos de Antioquia, Quindío, Risaralda y Caldas.

Durante la jornada, se llevaron a cabo dos talleres, liderados por la Unidad de Servicio Público de Empleo -SPE- y el Banco Iberoamericano de Desarrollo -BID-, invitando a los participantes a hacer uso del nuevo Sistema de Información del Servicio Público de Empleo, pues esta es una herramienta de innovación TIC que facilitaría los procesos empresariales relacionados con la generación y promoción de vacantes. En estos ejercicios lúdicos surgieron ideas impactantes para dinamizar el mercado laboral y transformar los territorios con oportunidades laborales incluyentes y equitativa, teniendo como base la oferta y la demanda.



En el marco del Encuentro Regional se realizó un panel de discusión con líderes y expertos del ecosistema laboral para trazar un camino hacia un mercado laboral más incluyente.



El Encuentro Regional de Inclusión y Equidad también resaltó las buenas prácticas empresariales desarrolladas por algunos Prestadores autorizados de la zona. Estas prácticas incluyen proyectos, procesos, experiencias, metodologías o técnicas innovadoras que han brindado soluciones novedosas en la prestación de servicios de gestión y colocación de empleo.

Este Encuentro reafirmó el compromiso de los prestadores y actores empresariales de la zona cafetera por construir un mercado laboral incluyente y equitativo, abriendo las oportunidades para todas las personas. 📍

## Alcance

# Finalidades

## DEL TRATAMIENTO DE DATOS PERSONALES

Por: Alexander Guzmán García

### Alcance

La presente política aplica para cualquier registro de datos personales realizado en forma presencial, no presencial y/o virtual para la vinculación a cualquier servicio o beneficio que ofrezca la Unidad del Servicio Público de Empleo o su Red de Prestadores.

La Unidad se encargará directamente del tratamiento de los datos personales, sin embargo, se reserva el derecho a asignar en terceros tal tratamiento exigiendo así mismo al encargado, la atención e implementación de los lineamientos y procedimientos idóneos para la protección de los datos personales y la estricta confidencialidad de estos.

### Finalidades del tratamiento de datos personales

La Unidad Administrativa Especial de Servicio Público de Empleo, identificado con el NIT 900.678.508-4, con domicilio en la Carrera 7, No. 31-10, Pisos 13 y 14, Bogotá - Colombia, informa que los datos personales que usted suministrará al sistema, serán tratados mediante el uso y mantenimiento de medidas de seguridad técnicas, físicas y administrativas y su confidencialidad estará garantizada de conformidad con lo definido en la Ley 1581 de 2012, el Decreto Reglamentario 1377 de 2013, la Resolución 1867 del 13 de mayo de 2014, con las siguientes finalidades. »



## FINALIDADES DEL TRATAMIENTO DE DATOS PERSONALES



**a) Registrar la información** de datos personales en las bases de datos de la Unidad Administrativa Especial de Servicio Público de Empleo, con la finalidad de analizar, evaluar y generar datos estadísticos, así como indicadores para la formulación de políticas en el sector del trabajo.



**b) Ejercer las funciones establecidas** en el Decreto 4108 de 2011, Ley 1562 de 2012, Ley 1610 de 2013 y las establecidas en las demás disposiciones legales vigentes.



**c) Facilitar** la implementación de programas en cumplimiento de mandatos legales.



**d) Enviar la información** a entidades gubernamentales o judiciales por solicitud expresa de las mismas.

Igualmente, es preciso informar que cualquier modificación al presente aviso le será notificado a través de los canales que disponga la Unidad Administrativa Especial de Servicio Público de Empleo para tal fin.

La política completa se puede consultar en la página web institucional o ingresando a la URL: <https://www.serviciodeempleo.gov.co/getattachment/Transparencia-e-Informacion/Planeacion/Políticas-lineamientos-y-manuales/Políticas-lineamientos-y-manuales/Politica-de-proteccion-de-datos-personales/DE-P-02-Politica-Proteccion-de-Datos-2022-Final.pdf.aspx?lang=es-CO>.





Unidad del  
**Servicio  
de Empleo**

**UNIDAD ADMINISTRATIVA ESPECIAL  
DEL SERVICIO PÚBLICO DE EMPLEO**  
Carrera 7, No. 31-10, Pisos 13 y 14, Bogotá D.C.

