PRIVACIDAD DEL PROGRAMA DE FUERZA LABORAL

El personal del Departamento de Trabajo y Regulación (DLR) puede recibir o manejar información confidencial para realizar las funciones de su trabajo. Esta póliza cubre el manejo de información confidencial, que incluye, entre otros, información privada que un cliente comparte con el personal de DLR sobre su situación e información de identificación personal (PII) recopilada del personal de DLR o del sistema SDWORKS durante el uso de los servicios de DLR. Los empleados del DLR deben participar en una adiestramiento anual sobre el manejo de información confidencial y seguridad de datos. DLR podrá modificar esta póliza según sea necesario.

INFORMACIÓN DE IDENTIFICACIÓN PERSONAL

Las diferencias entre la información PII protegida y la PII no confidencial se basan principalmente en un análisis del "riesgo de daño" que podría resultar de la divulgación de la PII.

1. PII protegida: información que, de divulgarse, podría causar daño a la persona cuyo nombre o identidad está vinculada a la información. Los ejemplos de PII protegida incluyen, entre otros, números de seguro social (SSN), información financiera como números de tarjetas de crédito y números de cuentas bancarias, información personal, números de teléfono residencial, edades, fechas de nacimiento, estado civil, nombres de cónyuges, identificadores biométricos (huellas dactilares, escaneos de iris, etc.), registros de salud, historial médico, registros educativos incluidos los registros GED y contraseñas de computadora.
2. PII no confidencial: información que, de divulgarse, por sí sola no podría esperarse razonablemente que provoque daño personal. Básicamente, se trata de información independiente que no está vinculada ni estrechamente asociada con ninguna información personal identificable (PII) protegida o no protegida. Los ejemplos incluyen nombre y apellido, direcciones de correo electrónico, direcciones comerciales, números de teléfono comerciales, credenciales de educación general, género o raza. Sin embargo, dependiendo de las circunstancias, una combinación de estos elementos podría potencialmente categorizarse como información personal identificable (PII) protegida o sensible.

La información recopilada por DLR incluye, entre otros, nombres, direcciones, números de teléfono, ciudadanía, género, raza, número de seguro social, número de identificación de empleador federal, número de identificación de empleador estatal, edad, historial laboral, resultados educativos, elegibilidad del programa y servicio del individuo, información necesaria para la inscripción al programa y la presentación de informes a los efectos de los informes y el desempeño del programa requeridos.

Manejo de información de identificación personal (PII)

La Administración de Empleo y Capacitación del Departamento de Trabajo de los EE. UU. (ETA) ha establecido los siguientes requisitos para el manejo de PII:

1. Los empleados deberán mantener límites profesionales con los clientes y evitar discutir información del cliente con personas fuera de la organización.
2. La información del cliente sólo podrá compartirse por los siguientes motivos:
    - Auditorías de programas estatales o federales;
    - de programas obligatorios;
    - divulgación involuntarias requeridas durante litigios, investigaciones criminales u otros procesos legales; o acuerdos de intercambio de datos con otras agencias estatales o federales;
    - Con la aprobación escrita del cliente mediante una autorización firmada de información,

- Con la aprobación por escrito del cliente, a través de un acuerdo de intercambio de datos o para fines de programas estatales o federales, como informes o auditorías de programas.
- Las solicitudes legales de información de un cliente deben proporcionarse al oficial de solicitud de registro del DLR y al Director de División.
- Los clientes que soliciten registros educativos GED® pueden ser remitidos al Administrador de GED® del Departamento de Educación de SD.

3. Se utilizarán contraseñas fuertes y únicas para todos los sistemas electrónicos. Las contraseñas y credenciales de seguridad no se compartirán. Las computadoras deben bloquearse cuando un empleado(a) se aleja y se deben tomar precauciones para garantizar que otros no puedan ver las pantallas de las computadoras.
4. Los datos deben procesarse de manera que se proteja la confidencialidad de los registros/documentos y están diseñados para evitar que personas no autorizadas recuperen dichos registros. Los datos PII deben almacenarse en un área físicamente segura contra el acceso de personas no autorizadas en todo momento.
5. Toda la información de identificación personal (PII) y otros datos confidenciales transmitidos por correo electrónico o almacenados en CD, DVD, memorias USB, etc., deben cifrarse mediante un módulo criptográfico que cumpla con los Estándares Federales de Procesamiento de Información (FIPS) 140-2 y esté validado por el Instituto Nacional de Estándares y Tecnología (NIST). Tanto la versión clásica como la nueva de Outlook ofrecen una opción para cifrar un correo electrónico a una entidad externa, es decir, fuera del dominio state.sd.us, utilizando el botón de opción de correo electrónico y eligiendo "Cifrar" para enviar información personal identificable fuera del sistema estatal. La información PII también puede transmitirse a través de métodos seguros como Microsoft Form y Adobe Sign.
6. Solo se pueden utilizar sistemas designados para el almacenamiento autorizado de PII, como carpetas designadas de SharePoint, SDWORKS o LACES, para almacenar PII. Se prohíbe el acceso, procesamiento y almacenamiento de datos PII de la beca ETA en equipos de propiedad personal. No se recomiendan los documentos en papel, pero, cuando sea necesario, deben almacenarse en un armario cerrado con llave y se requieren métodos apropiados para su destrucción, como la trituración.
7. Los datos no podrán obtenerse ni utilizarse para ningún otro fin que el requerido por los programas. El acceso a los datos está restringido únicamente a aquellas personas que los necesitan en su carácter oficial para desempeñar funciones relacionadas con el ámbito de trabajo.
8. Los documentos físicos deben desecharse mediante un método seguro que proteja la confidencialidad, como la trituración.
9. Cualquier sospecha de violación de seguridad o acceso no autorizado debe compartirse inmediatamente con un supervisor directo y el Director de División.
10. La información confidencial no debe enviarse a servicios de traducción, motores de búsqueda de Internet o sitios de inteligencia artificial no aprobados.

Volver al índice

SDWORKS

El sitio web SDWORKS permite a los solicitantes de empleo, empleadores y el público en general utilizar las funciones de intercambio laboral y encontrar información sobre el mercado laboral de Dakota del Sur. SDWORKS recopila información personal identificable durante el registro de la cuenta, durante el uso de SDWORKS y cada vez que se solicita información personal durante el uso del sitio web. Esta información se recopila para cumplir con los requisitos de informes de la fuerza laboral y desempeño del programa para garantizar la integridad del programa y futuras mejoras. Además, la información se utiliza para crear un perfil personal o una lista de trabajos para publicar en los servidores de bases de datos de búsqueda de SDWORKS.

Los usuarios de SDWORKS pueden crear un currículum electrónico o una lista de trabajos para almacenar en línea. En la configuración de la cuenta, los usuarios registrados de SDWORKS tienen la opción de hacer que un currículum esté abierto a la vista pública por parte de los empleadores, esto incluye cualquier información en el currículum, como dirección, teléfono, correo electrónico, etc. Cuando se envía información a un empleador(a) o reclutador, DLR no es

responsable de la retención, el uso o las prácticas de privacidad del empleador(a) o reclutador. La divulgación voluntaria de información personal identificable, nombres de usuario, direcciones de correo electrónico o mensajes de SDWORKS puede generar mensajes no solicitados de otras personas o terceros. Estas actividades están fuera del control del sistema SDWORKS y del DLR.

Las direcciones IP y la información de uso del sitio web se recopilan automáticamente cuando un usuario visita el sitio web de SDWORKS. Esta información ayuda a evaluar el comportamiento de los visitantes de forma agregada, incluido el número y la frecuencia de los visitantes de cada página y el tiempo que se ve cada página.

Las cookies pueden pasar al ordenador de un usuario. Las cookies son archivos de información que un navegador web coloca en el disco duro de una computadora o temporalmente en la memoria de una computadora durante la navegación en Internet. Las cookies no pueden dañar los archivos del usuario ni leer información de un disco duro. Las cookies de SDWORKS se utilizan para mantener la sesión de un usuario a medida que navega por las páginas del sitio web. SDWORKS instalará una cookie de identificación para personalizar el sitio web y satisfacer mejor las necesidades del usuario.

Las direcciones de correo electrónico de los usuarios de SDWORKS, específicamente de los residentes fuera del estado, pueden usarse con fines de investigación de mercado y alcanzamiento. Esta información respalda los esfuerzos de los programas de reclutamiento de trabajadores, como Dakota Roots. Esto podría dar lugar a correo directo no solicitado, correo electrónico masivos, etc.

Se recopilan las visitas a páginas web, el tiempo invertido en una página web, las visitas a una orden de trabajo y las búsquedas de trabajo para conocer más sobre el uso del cliente y el rendimiento de la página web.

Los datos agregados pueden proporcionarse a terceros para ayudar al DLR a mejorar los esfuerzos de desarrollo de la fuerza laboral. El sistema de registro de errores de SDWORKS recopilará nombres de usuario relacionados con cualquier error del sitio web como un medio para ayudar a nuestro personal técnico a comprender el error.

El sitio web de SDWORKS proporciona enlaces para que el usuario navegue a otros sitios web que pueden tener sus propias prácticas de recopilación de información, políticas de privacidad y medidas de seguridad. Los visitantes de otros sitios web de SDWORKS deben revisión las políticas de privacidad y las prácticas de recopilación de información de esos sitios web.

Los sistemas de información de gestión, como SDWORKS, contienen información confidencial que sólo puede ser utilizada por personal asignado con permiso y únicamente para fines autorizados. Las pantallas disponibles con información de identificación personal no deben imprimirse, duplicarse ni difundirse de ninguna manera no autorizada.

Acceso a SDWORKS

Para garantizar la seguridad e integridad del sistema SDWORKS, se han implementado las siguientes medidas:

- **Seguridad física:** El acceso a los servidores de bases de datos está restringido únicamente al personal autorizado.
- **Seguridad Electrónica:** Los datos están protegidos mediante encriptación SSL para evitar la interceptación no autorizada y garantizar una comunicación segura.
- **Protección de cuenta individual:** cada usuario debe usar su propia contraseña para acceder a su cuenta SDWORKS . Las contraseñas nunca deben compartirse.
- **Seguridad de la sesión:** los usuarios deben cerrar la sesión y cerrar su navegador web después de cada sesión para evitar el acceso no autorizado.
- **Restricciones de uso de datos:** La información a la que se accede a través del sistema sólo puede utilizarse para fines directamente relacionados con los programas autorizados. El uso o distribución no autorizados de datos está estrictamente prohibido. Las pantallas de SDWORKS con información personal identificable no deben imprimirse, duplicarse ni difundirse.

Volver al índice

NÚMEROS DE SEGURO SOCIAL

Todo el personal del DLR tiene la responsabilidad de mantener seguros los números de Seguro Social (SSN) de quienes buscan empleo y otras personas.

El DLR prohíbe la divulgación de números de Seguro Social a personas o entidades no autorizadas. El personal del DLR no exhibirá, divulgará, transferirá ni utilizará ilegalmente a sabiendas el SSN de ningún empleado(a), estudiante u otra persona de ninguna manera que viole la Ley de Protección del Seguro Social de 2004 o la Ley de Privacidad de 1974.

Los números de Seguro Social solo deben recopilarse cuando lo exija la ley estatal. Si se necesita un identificador personal único, se utilizará en su lugar un sustituto del Número de Seguro Social.

Los documentos, materiales o pantallas de computadora que muestren números de seguro social deberán mantenerse fuera de la vista del público en todo momento.

Los documentos que contengan números de Seguro Social solo se enviarán cuando lo permitan las ley estatales y federales. Se puede incluir un SSN en un documento enviado por correo cuando:

- Se envía como parte de un proceso de solicitud o inscripción iniciado por el individuo.
- Se envía para establecer, confirmar el estado, dar servicio, modificar o despedir una cuenta, contrato, beneficio de empleado(a) o seguro de salud, o para confirmar la exactitud de un Número de Seguro Social de una persona que tiene una cuenta, contrato, póliza o beneficio de empleado(a) o seguro de salud.
- Se envía con el propósito de cumplimiento con la correcta administración del programa de Asistencia de Reempleo (RA).
- Se encuentra en un registro público y se envía por correo de cumplimiento con la Ley de Libertad de Información. De lo contrario, se omitirá el número de Seguro Social.
- Se envía por correo, o a solicitud de, una persona cuyo Número de Seguro Social aparece en el documento o información de su padre o tutor legal.
- El número no deberá ser revelado a través de la ventana del sobre ni ser visible desde el exterior del sobre.

Se debe evitar enviar números de Seguro Social completos por correo electrónico. En su lugar, el nombre y apellido del individuo y los últimos cuatro dígitos de su número de Seguro Social deben enviarse por correo electrónico, si es necesario. Sin embargo, cuando sea necesario proporcionar un SSN completo a una entidad fuera del dominio estatal, state.sd.us, se utilizará el cifrado de correo electrónico.

El personal del DLR no revelará ningún SSN por teléfono ni dejará un mensaje de correo de voz que revele ningún SSN. Si se debe enviar por fax un SSN, el mensaje de fax deberá ir acompañado de una hoja de transmisión que incluya un "Aviso confidencial" que indique que la información incluida tiene la intención de ser privilegiada y confidencial y que solo está destinada al uso de la persona o entidad nombrada en la hoja de transmisión.

Todos los documentos o archivos que contengan números de Seguro Social deberán almacenarse de forma físicamente segura. Los números de Seguro Social no se almacenarán en computadoras ni en otros dispositivos electrónicos que no estén protegidos contra el acceso no autorizado. Al borrar números de Seguro Social de una computadora portátil o de escritorio, el personal deberá asegurarse de que el número se haya borrado por completo, incluso de la papelera de reciclaje.

Uso de números de la Seguridad Social

El SSN SÓLO se utilizará por los siguientes motivos:

1. Determinación de la elegibilidad del programa o en tales casos del pago de sueldos y subsidios, aunque al momento de la admisión no sea posible determinar la forma de pago, si la hubiera, que recibirá el solicitante; y

Las personas que buscan beneficios de Asistencia de Reempleo, Asistencia Temporal para Familias Necesitadas (TANF), Programa de Asistencia Nutricional (SNAP) y Crédito Tributario por Oportunidad de Trabajo (WOTC) deben proporcionar su SSN para elegibilidad. El Título XI de la Ley del Seguro Social, Sección 1137(a)(1), establece:

> *"el Estado requerirá como condición de elegibilidad para [los programas enumerados en la primera oración de este párrafo] que el reclamante proporcione al Estado el Número de Cuenta de Seguro Social del individuo y el Estado utilizará dicho número en la administración de los programas especificados".*

Las personas que participen en una experiencia laboral pagada deben proporcionar un SSN para que el Departamento pueda informar con precisión
sueldos y emitir un W-2.

2. Seguimiento de los registros salariales de RA para el cálculo de los resultados de las medidas de desempeño del programa.

P seudo SSN
De acuerdo con 20 CFR §666.150, se debe solicitar un SSN en el momento de la admisión o durante el registro en línea en SDWORKS. Sin embargo, no es necesario que el cliente proporcione su SSN. Si un cliente no desea compartir su SSN, se puede generar un pseudo-SSN. Al solicitar el SSN de un cliente, se debe explicar el uso y la privacidad y seguridad del sistema SDWORKS.

De acuerdo con la Sección 7 de la Ley de Privacidad de 1974 (5 USC Sección 552a Nota (Divulgación del Número de Seguro Social), a menos que la divulgación sea requerida por un estatuto federal, a los solicitantes no se les puede denegado ningún derecho, beneficio o privilegio provisto por la ley debido a la negativa del individuo a divulgar su Número de Seguro Social (SSN). Con excepción de los elementos identificados en el punto 1 anterior, no se denegado un servicio por no revelar un SSN.

Volver al índice

DIVULGACIÓN DE INFORMACIÓN

El personal del DLR no debe divulgar información sobre la situación o información personal identificable de un individuo sin autorización escrita en el Formulario de divulgación de información 1.

Las solicitudes de información realizadas por las cumplimiento de la ley o las solicitudes realizadas mediante citaciones deben dirigirse al Director de División y al equipo legal del DLR. La información compartida debe proteger la confidencialidad.

Cuando las agencias federales realizan inspecciones o auditorías in situ, el DLR debe poner la información a disposición; comuníquese con el Director de División para obtener ayuda. Las personas que obtengan acceso a información confidencial deben primero firmar un acuerdo de confidencialidad.

20 CFR § 666.150
TEGL 5-08, 39-11, 10-24
Sección 7 de la Ley de Privacidad de 1974 (5 USC Sección 552a Nota (Divulgación del Número de Seguro Social))
Título XI de la Ley del Seguro Social, Sección 1137(a)(1)
Normas Federales de Procesamiento de Información 140-2 c
Ley de Protección de la Seguridad Social de 2004 o Ley de Privacidad de 1974
Ley de Libertad de Información

Volver al índice