

G. PRINCIPIOS DE CALP Y ESTÁNDARES OPERACIONALES PARA EL USO SEGURO DE DATOS PERSONALES EN LOS PROGRAMAS DE TRANSFERENCIA ELECTRÓNICA Y EFECTIVO

1 Respeto La organización debe respetar la privacidad de los beneficiarios y reconocer que la obtención y procesamiento de sus datos personales representan una amenaza potencial para esa privacidad.

2 Proteger por diseño La organización debe "proteger por diseño" los datos personales que obtienen de los beneficiarios para su propio uso o para el uso de terceros para cada programa de efectivo o de transferencia electrónica que inicien o implementen.

3 Comprender los flujos de datos y los riesgos La organización debe analizar, documentar y comprender el flujo de los datos del beneficiario para cada programa de efectivo o de transferencia electrónica que inician o implementan dentro de su organización y entre su organización y otros y desarrollar estrategias de mitigación de riesgos que pueden ser necesarias para abordar cualquier riesgo que surja de estos flujos.

4 Calidad y precisión Las organizaciones deben garantizar la precisión de los datos personales que recopilan, almacenan y utilizan, incluyendo mantener la información actualizada, relevante y no excesiva en relación con el propósito para el cual se la procesa y no guardando los datos por más tiempo de lo necesario.

5 Obtener consentimiento o informar a los beneficiarios sobre el uso de sus datos Al momento de capturar los datos, se debe informar a los beneficiarios en cuanto a la naturaleza de los datos recopilados, con quiénes serán compartidos, quién es responsable del uso seguro de sus datos y a quién se los proporcionará dando la oportunidad de cuestionar el uso hecho de los datos y retirarse del programa si no desean que sus datos personales se utilicen para los propósitos descritos.

6 Seguridad Las organizaciones deben implementar estándares técnicos y operativos adecuados de seguridad para cada etapa de recolección, uso y transferencia de los datos del beneficiario para prevenir el acceso no autorizado, divulgación o pérdida y se debe identificar cualquier amenaza exterior, y acciones tomadas para atenuar cualquier riesgo que surja.

7 Eliminación Las organizaciones no deben mantener los datos de los beneficiarios por más tiempo de lo requerido a menos que tengan razones claras, justificables y documentadas para hacerlo, caso contrario los datos mantenidos por la organización y cualquier tercero relevante deben ser destruidos.

8 Responsabilidad Las organizaciones deben establecer un mecanismo por el cual un beneficiario pueda solicitar información sobre qué datos personales mantiene una organización sobre ellos, y mecanismos para recibir y responder.