|  |  |  |
| --- | --- | --- |
| **INFORMACIÓN DEL USUARIO** | | |
| **Nombre Diligenciador:** |  | |
| **Nombre Sistema de información/Proyecto:** |  | |  |  |  | | --- | --- | --- | | **Análisis Base** | **x** | **Fecha** | | **Retroalimentación Base** |  | **Fecha** | | **Verificación de Requerimientos** |  | **Fecha** | |
| **Descripción del Proyecto:** |  | |
| **Área solicitante:** |  | |
| **INTRODUCCIÓN** | | |
| La siguiente lista de chequeo tiene como finalidad implementar una privacidad por diseño, durante la estructuración de los requisitos funcionales de nuestros desarrollos o proyectos informáticos, especialmente de aquellos softwares o aplicativos que realicen tratamiento, almacenen o necesiten datos personales de los ciudadanos para poder funcionar y cumplir su objetivo, con el fin de que éstos cumplan con los requisitos mínimos establecidos en la Ley 1581 de 2012. | | |
| **INSTRUCCIÓN DEL DILIGENCIAMIENTO** | | |
| De la siguiente lista, **marque con una X** de acuerdo con la siguiente instrucción:   1. Al finalizar las actividades de análisis y definición de requisitos funcionales en materia de protección de datos personales, seleccione:  * **Aplica**: En caso de que el requisito se vaya a implementar en el desarrollo del sistema de información. * **No aplica**: En caso de que le jefe de la OTI haya autorizado la exclusión del requisito.  1. Al finalizar la actividad de implementación de requisitos de seguridad de la información, la oficial protección de datos personales diligenciará las dos (2) últimas casillas:  * **Cumple: E**n caso de evidenciar que el requisito funcional de protección de datos fue correctamente implementado en el sistema de información. * **No cumple:** En caso de evidenciar que el requisito de funcional de protección de datos no fue implementado satisfactoriamente.   Igualmente, registre las observaciones que considere necesarias al final del formato. | | |

| **No.** | **Requisito de Protección de datos personales** | **Etapa de Aplicación del Principio** | **Controles del Principio** | **Análisis línea base** | | **Retroalimentación Base/Observaciones** | **Verificación de cumplimiento** | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Aplica** | **No aplica** |  | **Cumple** | **No cumple** |
| 1 | Principio de libertad | Durante la recolección de los datos personales. | **A.** ¿Qué Clase de Datos se recolectarán?  **Datos Públicos:** Nombres, apellidos, número de cédula y Correo corporativo. **Datos Semiprivados:** Correo personal, número de celular personal, dirección física. **Datos Privados:** Contraseñas, datos de credenciales de acceso. IP. **B.** Aviso o disclaimer sobre la autorización de tratamiento de datos en donde se evidencien las finalidades. Esta información va antes del check. **C.** Check de Autorización de tratamiento de datos personales. Este check debe implicar un movimiento del ciudadano. Dicho de otro modo, el ciudadano debe mover el mouse, hacer click, en un botón o en un check.  **C1.** Se le debe dar la oportunidad al ciudadano de negarse a la autorización. Por ser una entidad pública, el check negativo no existe, solo existe el positivo. Sin embargo, la opción del anonimato debe existir. **C2.** Este check debe estar al menos durante la recolección de los datos (Puede ser antes), pues el consentimiento debe ser informado, previo y expreso. **C3.** La entidad debe guardar trazabilidad sobre la autorización, o la forma en que el ciudadano escogió presentar un trámite (Anonimato), como una prueba que debe almacenarse y que pueda ser objeto de consulta en otra ocasión. |  |  |  |  |  |
| 2 | Principio de finalidad | Durante la recolección de los datos personales. | **A.** Aviso o disclaimer sobre la autorización de tratamiento de datos en donde se evidencien las finalidades (Objetivos por los cuales se utilizarán los datos). Esta información va antes del check. |  |  |  |  |  |
| 3 | Principio de veracidad o calidad | Durante la recolección y el tratamiento de los datos personales. | **Durante la recolección:** Herramientas que permitan identificar que, en efecto, la persona que está diligenciando sus datos personales es quien dice ser. Ej: Doble Factor de Autenticación. En caso de utilizarse la creación de credenciales, la oportunidad de que los ciudadanos recuperen sus cuentas por medio de sus correos. **Durante el Tratamiento:** A los ciudadanos se les debe garantizar la oportunidad de actualizar sus datos ¿La misma aplicación lo podría permitir? De no hacerlo, los ciudadanos podrán actualizar o modificar sus datos por el correo [contactenos@sic.gov.co](mailto:contactenos@sic.gov.co). El aplicativo no debe permitir que los ciudadanos se den de baja por su cuenta, debido a que somos una entidad pública y nos corresponde analizar si la eliminación de datos es procedente o no. Tener presente que el historial de datos condensados: Ejemplo: Dejar el rastro de la información del ciudadano. Ejemplo: Quedar trazabilidad de lo que existía y lo que el ciudadano edita y actualiza, a manera de prueba. |  |  |  |  |  |
| 4 | Principio de transparencia | Durante la recolección y el tratamiento de los datos personales. | **Durante la recolección:** Que el ciudadano pueda ver qué datos son los que se encuentran registrados. **Durante el tratamiento:** Que el ciudadano pueda solicitar en cualquier momento prueba de qué autorizó el tratamiento. |  |  |  |  |  |
| 5 | Principio de acceso y circulación restringida | Durante el tratamiento de los datos personales. | **A**. Los datos personales no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva. **B.** Control técnico para brindarle un conocimiento restringido sólo a los Titulares o terceros autorizados (Abogados, testigos) conforme a la ley. |  |  |  |  |  |
| 6 | Principio de seguridad | Durante la recolección tratamiento y depuración de los datos personales. | **A.** Medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. |  |  |  |  |  |
| 7 | Principio de confidencialidad | Durante la recolección tratamiento y depuración de los datos personales. | **A.** Garantizar la reserva de la información suministrada por el ciudadano. No solo de su información sino también de lo que éste escala a través del software o aplicativo. **B.** Solo personas autorizadas legítimamente por la ley podrán acceder a la información del ciudadano. |  |  |  |  |  |
| 8 | Tratamiento de Datos Sensibles | datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas,  la afiliación sindical,  datos genéticos, datos biométricos tratados únicamente para identificar un ser humano,  datos relativos a la salud,  datos relativos a la vida u orientación sexuales de una persona. | **A.** Garantizar métodos de anonimización o desidentificación de información personal cuando se traten datos de carácter sensible. **B.** Todo registro de caracterización de población debe ser solo de uso interno y no debe quedar expuesto en el aplicativo ni quedar condensado en ningún documento que emita la entidad. Ejemplo: Certificado de radicación. No pueden quedar visibles. |  |  |  |  |  |
| 10 | Transmisión /Transferencia de Datos Personales | Durante la recolección | A. Verificar si la base de datos que se desprende del aplicativo será objeto de trasmisión/transferencia nacional o internacional. ¿Se compartirá las bases de datos con un tercero (proveedor, empresa y/o entidad del estado)? |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Los siguientes requisitos son de carácter documental y técnico. | | | | | | | |
| **No**. | **Requisitos adicionales de Protección De Datos Personales** | **Tipo de requisito** | | **Análisis del requisito o del Control** | | **Verificación de cumplimiento** | |
| **Aplica** | **No aplica** | **Cumple** | **No cumple** |
| 1 | Controles de seguridad en la tercerización de servicios para el tratamiento de la información personal. | Técnico | |  |  |  |  |
| 2 | Política implementada de copia de respaldo de la información personal. | Documental | |  |  |  |  |
| 3 | Política de protección para el acceso remoto a la información persona. | Documental | |  |  |  |  |
| 4 | Procedimiento que contemple la definición de especificaciones y requisitos de seguridad de los sistemas de información personal. | Documental | |  |  |  |  |
| 5 | Controles de seguridad de la información durante el mantenimiento (Control de cambios) de los sistemas de información personal. | Técnico | |  |  |  |  |
| 6 | Procedimiento implementado para la validación de datos de entrada y procesamiento de la información personal, para garantizar que los datos recolectados y procesados sean correctos y apropiados, como confirmación de tipos, formatos, longitudes, pertinencia, cantidad, uso, etc. | Documental | |  |  |  |  |
| 7 | Control de seguridad de información para la validación de datos de salida. | Técnico | |  |  |  |  |
| 8 | Política y procedimientos implementados de gestión de incidentes de seguridad de la información personal. | Documental | |  |  |  |  |
| 9 | Política para mejorar la seguridad de la información personal a partir de los incidentes o vulnerabilidades detectados. | Documental | |  |  |  |  |
| **OBSERVACIONES** | | | | | | | |
|  | | | | | | | |
| **FIRMAS** | | | | | | | |
| **Nombre:**  **Firma:**  **Cargo:** Ingeniero desarrollador. | | | **Nombre:**  **Firma:**  **Cargo:** Supervisor o Coordinador del grupo de trabajo responsable del desarrollo. | | | | |
| **Nombre:**  **Firma:**  **Cargo: *Oficial Protección de Datos Personales*** | | | | | | | |