FONDOLÍMPICA
NIT. 890.115.231-9

INFORME TÉCNICO

Fecha: Miercoles, 13 de Julio de 2016

FONDOLÍMPICA
NIT. 890.115.231-9

Con objeto de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la Ley Estatutaria 1581 de 2.012, de Protección de Datos, FONDO DE EMPLEADOS OLÍMPICA, el responsable del tratamiento de datos personales, así como sus encargados del tratamiento, deben implementar medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

No se permite el registro de bases de datos personales que no reúnan las condiciones mínimas de seguridad expuestas en el presente informe.

Las medidas de seguridad se clasifican en tres niveles de seguridad según el tipo de datos: público-semiprivado, privado y sensible. Los niveles de seguridad son acumulativos, de forma que las medidas de seguridad para datos sensibles incluyen también las medidas de seguridad para los niveles, privado y público-semiprivado; y las medidas de seguridad para datos privados incluyen, a su vez, las del nivel público-semiprivado. La clasificación de los niveles de seguridad se realiza atendiendo a la tipología de los datos, la finalidad del tratamiento y la actividad del responsable del tratamiento (Tabla I).

Tabla I. Tipos de datos y el nivel de seguridad

Tipos de datos	Descripción	Nivel de seguridad
Público	Datos contenidos en documentos públicos, en sentencias judiciales debidamente ejecutoriadas no sometidas a reserva y los relativos al estado civil de las personas.	Público-semiprivado
Semiprivado	Bases de datos que contengan Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países (reportes positivos y negativos)	Público-semiprivado
Privado	Números telefónicos y correos electrónicos personales; datos laborales, sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de datos de los responsables de operadores que presten servicios de comunicación electrónica	Privado
Sensible	Datos de salud, ideología, afiliación sindical, creencias, religión, origen racial o étnico, vida sexual, datos recabados sin consentimiento para fines policiales, datos biométricos (huellas, iris, etc.), datos derivados de la violencia de género	Sensible

Las medidas de seguridad también varían según el sistema de tratamiento de la base de datos, que puede ser automatizada, no automatizada o parcialmente automatizada.

La siguiente tabla (Tabla II) indica el nivel de seguridad y el sistema de tratamiento de las bases de datos almacenadas y tratadas por FONDO DE EMPLEADOS OLÍMPICA.

Tabla II. Bases de datos y nivel de seguridad

Base de datos	Nivel de seguridad	Sistema de tratamiento
LINIX	Privado	Mixto
EMPLEADOS	Sensible	Mixto
1.ASOCIADOS	Público-semiprivado	Mixto
2.ASOCIADOS	Sensible	Mixto
3.ASOCIADOS	Privado	Mixto
4.ASOCIADOS	Privado	Mixto
5.ASOCIADOS	Privado	Mixto
6.ASOCIADOS	Privado	Mixto
7.ASOCIADOS	Privado	Mixto
ASOCIADOS/RET	Sensible	Mixto
RETIRADOS	Público-semiprivado	Mixto

A continuación se exponen y describen las medidas de seguridad mínimas implantadas por FONDO DE EMPLEADOS OLÍMPICA, que están recogidas y desarrolladas en su Manual Interno de Seguridad (Tablas III, IV, V y VI).

Tabla III. Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) y bases de datos (automatizadas, no automatizadas)

Gestión de documentos y soportes	Control de acceso	Incidencias	Personal	Manual Interno de Seguridad
1. Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos. 2. Acceso restringido al lugar donde se almacenan los datos.	1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones. 2. Lista	1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la	1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos 2. Definición de las funciones de control y	1. Elaboración e implementación del Manual de obligado cumplimiento para el personal. 2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las

3. Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico. 4. Sistema de etiquetado o identificación del tipo de información. 5. Inventario de soportes.	actualizada de usuarios y accesos autorizados. 3. Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. 4. Concesión, alteración o anulación de permisos por el personal autorizado	notificación, efectos y medidas correctoras. 2. Procedimiento de notificación y gestión de incidencias.	autorizaciones delegadas por el responsable del tratamiento. 3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas	bases de datos, procedimiento ante incidencias, procedimiento de copias y recuperación de datos, medidas de seguridad para el transporte, destrucción y reutilización de documentos, identificación de los encargados del tratamiento.

Tabla IV. Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) según el tipo de bases de datos

Bases de datos no automatizadas			Bases de datos automatizadas	
Archivo	**Almacenamiento de documentos**	**Custodia de documentos**	**Identificación y autenticación**	**Telecomunicaciones**
1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y permitan el ejercicio de los derechos de los Titulares.	1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.	1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos.	1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización. 2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.	1. Acceso a datos mediante redes seguras.

FONDOLÍMPICA NIT. 890.115.231-9

FONDOLÍMPICA
NIT. 890.115.231-9

Tabla V. Medidas de seguridad para datos privados según el tipo de bases de datos

Bases de datos automatizadas y no automatizadas			Bases de datos automatizadas			
Auditoría	**Responsable de seguridad**	**Manual Interno de Seguridad**	**Gestión de documentos y soportes**	**Control de acceso**	**Identificación y autenticación**	**Incidencias**
1. Auditoría ordinaria (interna o externa) cada dos meses. 2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información. 3. Informe de detección de deficiencias y propuesta de correcciones. 4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento. 5. Conservación del Informe a disposición de la autoridad.	1. Designación de uno o varios responsable de seguridad. 2. Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno de Seguridad. 3. Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.	1. Controles periódicos de cumplimiento	1. Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega	1. Control de acceso al lugar o lugares donde se ubican los sistemas de información.	1. Mecanismo que limite el número de intentos reiterados de acceso no autorizados.	1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. 2. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

FONDOLÍMPICA
NIT. 890.115.231-9

FONDOLÍMPICA
NIT. 890.115.231-9

Tabla VI. Medidas de seguridad para datos sensibles según el tipo de bases de datos

Bases de datos no automatizadas				Bases de datos automatizadas		
Control de acceso	**Almacenamiento de documentos**	**Copia o reproducción**	**Traslado de documentación**	**Gestión de documentos y soportes**	**Control de acceso**	**Telecomunicaciones**
1. Acceso solo para personal autorizado. 2. Mecanismo de identificación de acceso. 3. Registro de accesos de usuarios no autorizados.	1. Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.	1. Solo por usuarios autorizados. 2. Destrucción que impida el acceso o recuperación de los datos.	1. Medidas que impidan el acceso o manipulación de documentos.	1. Sistema de etiquetado confidencial. 2. Cifrado de datos. 3. Cifrado de dispositivos portátiles cuando salgan fuera.	1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede. 2. Control del registro de accesos por el responsable de seguridad. Informe mensual. 3. Conservación de los datos: 2 años.	1. Transmisión de datos mediante redes electrónicas cifradas.

FONDOLÍMPICA
NIT. 890.115.231-9