

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN

Intervienen en la celebración del presente “Acuerdo De Confidencialidad y No Divulgación de la Información entregada por la _____ ÁREA CUSTODIA DE LA INFORMACIÓN _____” del Ministerio de Inclusión Económica Social, por una parte, el/la _____ (NOMBRES Y APELLIDOS) con cédula de ciudadanía Nro. _____, en calidad de COORDINADOR/A GENERAL DE ESTUDIOS Y DATOS DE INCLUSIÓN, en representación de la Coordinación General de Estudios y Datos de Inclusión, que en adelante se le denominará como “PROVEEDOR DE LA INFORMACIÓN”; y por otro lado, el/la señor/a _____ (NOMBRES Y APELLIDOS), con cédula de ciudadanía Nro. _____, en su calidad de investigadora, de _____ (INSTITUCIÓN), que en adelante y para efectos del presente instrumento se le denominará como ‘RECEPTOR/A DE LA INFORMACIÓN’, quienes libre y voluntariamente celebran el presente instrumento.

Ambas partes reconocen recíprocamente su capacidad para obligarse, por lo que suscriben el presente Acuerdo de Confidencialidad y de No Divulgación de Información con base en las siguientes cláusulas;

CLÁUSULA PRIMERA. - ANTECEDENTES

1.1. El numeral 19 del artículo 66 de la Constitución de la República del Ecuador, determina que se reconoce y garantiza a las personas el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

1.2. El artículo 226 de la Constitución de la República del Ecuador prevé que: "Las Instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la Ley".

1.3. El artículo 178 del Código Orgánico Integral Penal establece: “La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años...”.

1.4. El artículo 190 del Código Orgánico Integral Penal señala: “La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años...”.

1.5. Artículo 230 del Código Orgánico Integral Penal determina: “Será sancionada con pena privativa de libertad de tres a cinco años: (...) La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible...”.

1.6. El literal b) del artículo 17 de la Ley Orgánica de Transparencia y Acceso a la Información Pública determina que no procede el derecho a acceder a la información pública, con respecto de la información expresamente establecida como reservada en leyes vigentes.

1.7. La Ley del Sistema Nacional de Registro de Datos Públicos en su artículo 4, establece: “Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información...”.

1.8. Mediante Acuerdo Ministerial No. MIES-2021-024, de 29 de abril de 2021, en su Artículo 1 define “Aprobar y expedir la Política de Seguridad de la Información del Ministerio de Inclusión Económica y Social acorde al Esquema Gubernamental de Seguridad de la Información EGSI vigente, y sus anexos, documentos que son parte integrante del presente instrumento”.

La política de Seguridad de la Información define:

- **Objetivo**
 - Definir el acceso y uso a los servicios Tecnológicos provisto por la Coordinación General de Tecnologías de Información y Comunicación - CGTIC mediante controles y normas generales

procurando que la confidencialidad y la integridad de la información se mantenga ante posibles eventos adversos.

- **Alcance**
 - La política de control de acceso aplica tanto a las y los servidores públicos que laboran en el Ministerio de Inclusión Económica y Social, así como a usuarios externos que utilizan servicios tecnológicos provistos por la misma.

- **Glosario**
 - **ACUERDO DE CONFIDENCIALIDAD:** Es un documento en los que los funcionarios del MIES o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la institución, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

- **Responsabilidades – Custodios de la Información**

Son custodios de la información cada uno de los servidores públicos que la genera, procesa, recibe y almacena en cualquier medio, esto incluye:

- Valorar y clasificar la información que está bajo su administración y/o generación, siguiendo los lineamientos establecidos por el área competente.
- Autorizar, restringir y delimitar a los demás usuarios de la Institución el acceso a la información de acuerdo a sus roles y responsabilidades, y a los diferentes funcionarios, contratistas o practicantes que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información, así como la aceptación de acuerdos de confidencialidad establecidos.
- Determinar los tiempos de retención de la información en conjunto con las áreas que se encarguen de su protección y almacenamiento de acuerdo a las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes.

1.9. Mediante Acuerdo Ministerial MINTEL No. 025-2019, de 20 de septiembre de 2019, publicado en el Registro Oficial Edición Especial No. 228, de 10 de enero de 2020, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, expidió el “Esquema Gubernamental de Seguridad de la Información -EGSI-”, el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, en cuyo numeral 9.2.4, se contempla el acuerdo de confidencialidad y

las recomendaciones para su implementación, considerando la no divulgación de la información de acuerdo a la necesidad de la institución.

1.10. Mediante Acuerdo Ministerial No. 030, de 16 de junio de 2020, se emitió la Reforma Integral al Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Inclusión Económica y Social, expedido mediante Acuerdo Ministerial Nro. 000080 de 09 de abril de 2015, publicado en el Registro Oficial Edición Especial Nro. 329, de 19 de junio de 2015, en cuyo numeral 1.3.4.1, se establece como una de las atribuciones y responsabilidades de la Gestión de Estudios y análisis: “j. Realizar informes técnicos para entrega de información institucional a solicitudes externas en el ámbito de acción de la institución.

CLÁUSULA SEGUNDA. - OBJETO

En virtud de los antecedentes expuestos, por medio del presente instrumento **EL/LA RECEPTOR/A DE LA INFORMACIÓN** se obliga expresamente a guardar sigilo, confidencialidad y reserva sobre el contenido de toda la información institucional recibida, generada y/o consultada a través de los sistemas de información institucional del MIES y se compromete a hacer uso de la información, únicamente para las actividades relacionadas con las funciones que desempeña, conforme a las obligaciones y prohibiciones legales pertinentes.

CLÁUSULA TERCERA. - OBLIGACIONES DE EL/LA RECEPTOR/A DE LA INFORMACIÓN

3.1. Guardar reserva y confidencialidad de cualquier tipo de información institucional que se le suministre o a la cual llegare a tener acceso o conocimiento;

3.2. Mantener en forma estrictamente reservada y confidencial toda la información institucional que por razón de su competencia tenga acceso, por lo tanto, se obliga a abstenerse de usar, disponer, divulgar y/o publicar dicha información, por cualquier medio, oral, escrito y/o tecnológico, y en general, de aprovecharse de ella en cualquier otra forma, para efectos ajenos a los intereses de la Institución a la cual pertenece.

3.3. No realizar copia o duplicado alguno de la información institucional que se presenta en los sistemas de información del MIES; y tampoco podrá divulgar dicha información a terceras personas sin que medie igualmente la respectiva autorización previa y escrita de la otra parte. Se excluye de esta obligación la información que sea de dominio público y cuya revelación no cause agravio o perjuicio alguno a su titular.

3.4. Guardar estricta confidencialidad de los datos que le identifican para acceder a los sistemas y equipos informáticos institucionales, así como sobre los

documentos e informaciones relacionados con los sistemas y aplicaciones informáticos del MIES que llegare a conocer.

3.5. No divulgar, revelar ni alterar la información confidencial, procedimientos, formatos y demás aspectos técnicos y administrativos derivados de la misma, aún después de que haya concluido su relación laboral con la Institución.

3.6. Cumplir con el cambio de clave del correo institucional cada 60 días.

3.7. Cumplir con las demás obligaciones previstas en la Política de la Seguridad de la Información del Ministerio de Inclusión Económica y Social, aprobada y expedida con Acuerdo Ministerial No. MIES-2021-024, de 29 de abril de 2021; en el “Esquema Gubernamental de Seguridad de la Información -EGSI-”, el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, expedido con Acuerdo Ministerial MINTEL No. 025-2019, de 20 de septiembre de 2019, y en la demás normativa que resulte aplicable para el efecto.

CLÁUSULA CUARTA. - EXCLUSIVIDAD DE USO

4.1. Una vez que tenga acceso a la información confidencial, **EL/LA RECEPTOR/A DE LA INFORMACIÓN** procederá a utilizarla exclusivamente para los fines y en la forma determinados en el presente acuerdo, y no podrá archivarla en medios de almacenamiento personal, sean estos, físicos o digitales.

4.2. En el caso de existir difusión no autorizada o fugas de información confidencial, se debe proceder en base a lo estipulado en el “Instructivo para Gestión de Incidentes derivados del Incumplimiento de la Política de Seguridad de la Información”.

CLÁUSULA QUINTA. - ENTREGA DE INFORMACIÓN CONFIDENCIAL

EL/LA RECEPTOR/A DE LA INFORMACIÓN tendrá acceso a la información a través de sus credenciales de acceso a los sistemas de información y servicios tecnológicos, la cual es de uso personal e intransferible, y su utilización es de exclusiva responsabilidad frente al MIES, de conformidad con los procedimientos institucionales previstos para el efecto.

CLÁUSULA SEXTA. - CONFIDENCIALIDAD

6.1. **EL/LA RECEPTOR/A DE LA INFORMACIÓN** deberá tratar de manera estrictamente confidencial la información que no haya sido difundida de manera oficial por parte del MIES y no podrá transferirla, difundirla, publicitarla o cederla por ningún medio físico o electrónico, conforme a lo especificado en la Política de Seguridad de la Información de la Institución.

6.2. Toda información procesada en la Institución es de propiedad exclusiva del MIES, por tanto, ningún **RECEPTOR/A DE LA INFORMACIÓN** podrá hacer uso de la misma para su beneficio personal e independiente o para el beneficio de terceros. Bajo ningún concepto, dicha información podrá ser empleada para causar daño a terceros ni usada con fines perjudiciales a los intereses de la Institución y su personal.

CLÁUSULA SÉPTIMA. - SUPERVISIÓN, RESPONSABILIDADES Y SANCIONES

7.1. EL MIES supervisará las actividades de **EL/LA RECEPTOR/A DE LA INFORMACIÓN** relacionadas con la gestión de información en los mecanismos de traspaso de la institución; y, de ser el caso, solicitará la realización de las auditorías correspondientes.

7.2. En caso de que **EL/LA RECEPTOR/A DE LA INFORMACIÓN** incumpliere con una o varias de las obligaciones y/o transgrediere una o varias de las prohibiciones estipuladas en el presente instrumento, será sujeto de la aplicación de las sanciones a que hubiere lugar, sin perjuicio de las acciones civiles y penales que procedan en cada caso, conforme lo establecido en el ordenamiento jurídico vigente.

CLÁUSULA OCTAVA. - VIGENCIA

Los compromisos y obligaciones establecidos en el presente Acuerdo, tendrán vigencia a partir de la suscripción de este instrumento hasta que se cumpla con el objeto de este instrumento y **EL/LA RECEPTOR/A DE LA INFORMACIÓN** se compromete a guardar la confidencialidad de la información institucional inclusive después de dicha finalización, conforme lo señalado en el numeral 3.5 de la cláusula tercera de este Acuerdo.

En aceptación a lo estipulado en el presente Acuerdo las partes expresamente se ratifican en el contenido, para fe y constancia se firman (2) dos ejemplares de igual tenor y valor

En la ciudad de _____, los _____ días de _____ de 202__

NOMBRE DEL COORDINADOR/A

Coordinador/a General de Estudios y Datos de Inclusión

Ministerio de Inclusión Económica y Social

CI: _____

NOMBRES DEL/LA RECEPTOR/A DE INFORMACIÓN

Investigador/a

_____ (INSTITUCIÓN)

CI: _____

NOMBRE DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN - OSI