RESOLUCION GERENCIAL N° 071 -2019- GRSM-PEAM-01.00

Moyobamba, 17 MAYO 2019

VISTOS:

El Informe N°047-2019-GRSM-PEAM-01.06, del Especialista en Sistemas e Informática.

El Informe N°007-2019-GRSM-PEAM-06.04, de la Especialista en Planes, Monitoreo y Evaluación.

El Informe N°051-2019-GRSM-PEAM-06.00, del Jefe de la Oficina de Presupuesto, Planificación, Estudios y Ordenamiento Territorial.

CONSIDERANDO:

Que, mediante Resolución Gerencial N°423-2018-GRSM-PEAM.01.00, de fecha 05 de Diciembre del 2018, se aprobó los *"Lineamientos de la Política de Seguridad de la Información del Proyecto Especial Alto Mayo";*

Que, con Informe N°047-2019-GRSM-PEAM-01.06, el Especialista en Sistemas e Informática, refiere que con Resolución Gerencial N°423-2018-GRSM-PEAM.01.00 se aprobó los *"Lineamientos de la Política de Seguridad de la Información del Proyecto Especial Alto Mayo"*. Ante la necesidad de implementar lo establecido en la normatividad referente al gobierno digital, precisamente a la conformación del comité de gobierno digital en la Institución, es de urgencia la modificación de los lineamientos de la política de seguridad de la información del Proyecto Especial Alto Mayo.
Es así, que luego de la revisión de la normatividad de gobierno digital actualizada, se ha modificado el documento aprobado mediante la citada Resolución Gerencial, cuyo documento se remite en anexo, solicitando la aprobación de la Directiva N°001-2019-GRSM-PEAM-01.00 "Políticas de Seguridad de la Información", mediante documento resolutivo;

Que, mediante Informe N°007-2019-GRSM-PEAM-06.04, la Especialista en Planes, Monitoreo y Evaluación, refiere que posterior al trámite de aprobación de los Lineamientos de la Política de Seguridad de la Información de la Entidad; la Presidencia del Consejo de Ministros y la Secretaría de Gobierno Digital aprobaron varias disposiciones referente al Gobierno Digital, motivo por el cual el Especialista en Sistemas e Informática, comunica que se debe modificar los "Lineamientos de la Política de Seguridad de Información del Proyecto Especial Alto Mayo" y remite la Directiva N°001-2019-GRSM-PEAM-01.00 "Políticas de Seguridad de la Información", solicitando su aprobación mediante documento resolutivo.
Teniendo como soporte el historial de revisión y aprobación que forma parte de la Directiva, realizado por el citado profesional en su calidad y la última

RESOLUCION GERENCIAL N° 171 -2019- GRSM-PEAM-01.00

revisión del documento, concluye que las políticas se enmarcan en la normatividad vigente emitida por el Poder Ejecutivo, la Presidencia del Consejo de Ministros, la secretaria del Gobierno Digital y lo dispuesto en las Normas Técnicas Peruanas: "NTP ISO/IEC 27001: 2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da. Edición" y "NTP ISO/IEC 17799: Código de Buenas Prácticas para Gestión de la Seguridad de la Información"; por lo que sugiere otorgar la conformidad y su trámite a la Gerencia General para su aprobación mediante documento resolutivo.
Del mismo modo se debe dejar sin efecto la Resolución Gerencial N°423-2018-GRSM-PEAM.01.00;

Que, mediante Informe N°051-2019-GRSM-PEAM-06.00, el Jefe de la Oficina de Presupuesto, Planificación, Estudios y Ordenamiento Territorial, solicita a esta Gerencia General la aprobación mediante documento resolutivo de la Directiva N°001-2019-GRSM-PEAM-01.00 "Políticas de Seguridad de la Información", la cual cuenta con la conformidad de esta Jefatura al encontrarse enmarcada en la normatividad vigente emitida por el Poder Ejecutivo, la Presidencia del Consejo de Ministros, la Secretaria del Gobierno Digital, lo dispuesto en las Normas Técnicas Peruanas: "NTP ISO/IEC 27001: 2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da. Edición" y "NTP ISO/IEC 17799: Código de Buenas Prácticas para Gestión de la Seguridad de la Información".
Asimismo, refiere que la citada Directiva fue elaborada y revisada por el Especialista en Sistemas e Informática, como responsable y especialista en la materia y también contó con la revisión por parte de la Especialista en Monitoreo y Evaluación. Solicitando se deje sin efecto los "Lineamientos de la Política de Seguridad de la Información del Proyecto Especial Alto Mayo", considerando que a la fecha se encuentra aprobada;

Por las consideraciones que anteceden y estando a las facultades conferidas por la Resolución Ejecutiva Regional N°317-2018-GRSM/GR de fecha 29.05.2018, y a lo señalado por el inciso h) del Artículo 15° y demás pertinentes del Manual de Organización y Funciones del Proyecto Especial Alto Mayo, con las visaciones de la Oficina de Presupuesto, Planificación, Estudios y Ordenamiento Territorial y Oficina de Asesoría Jurídica;

SE RESUELVE:

Artículo Primero.- **APROBAR,** Directiva N°001-2019-GRSM-PEAM-01.00 *"Políticas de Seguridad de la Información"*, por motivos expuestos en la parte considerativa de la presente resolución; la misma que se Anexa y forma parte de ésta.

RESOLUCION GERENCIAL N° 171 -2019- GRSM-PEAM-01.00

Artículo Segundo.-**DEJAR SIN EFECTO** la Resolución Gerencial N°423-2018-GRSM-PEAM.01.00, de fecha 05 de Diciembre del 2018.

Artículo Tercero.-**HACER,** de conocimiento la presente resolución a la Oficina de Presupuesto, Planificación, Estudios y Ordenamiento Territorial, Oficina de Administración, Especialista en Sistemas e Informática y Oficina de Asesoría Jurídica del Proyecto Especial Alto Mayo.

Regístrese, comuníquese y archívese,

Ing. Muller A. Huancas Huamán
GERENTE GENERAL

Directiva N° 001-2019-GRSM-PEAM-01.00

Políticas de Seguridad de la Información

Versión 1.0

Año 2019

Historial de Revisiones

Fecha	Versión	Autor	Detalle	Estado
01/04/2019	1.0	ESRS	Versión preliminar del documento	Elaborado
15/04/2019	1.0	ESRS	Documento revisado	Revisado
23/04/2019	1.0	ESRS	Documento revisado para ser aprobado	Trámite de aprobación

Autor

ESRS : Ing. Ernesto Segundo Ríos Sandoval
Especialista en Sistemas e Informática

Revisión

ESRS : Ernesto Segundo Ríos Sandoval
Especialista en Sistemas e Informática

Aprobación

Tabla de Contenido

Introducción

La información obtenida como producto de los procesos realizados en el Proyecto Especial Alto Mayo es reconocida como activo vital, es por ello que se encuentra comprometido en salvaguardar su integridad y disponibilidad, mediante la aplicación de lo recomendado en las normas técnicas peruanas, estándares internacionales y las mejores prácticas de tecnologías de la información y seguridad de la información, a fin de asegurar la continuidad de sus operaciones y mantener un nivel óptimo de calidad en los servicios tecnológicos que brinda y da soporte.

A través del presente documento, el Proyecto Especial Alto Mayo, exhorta que se reconozca a la información como uno de sus activos principales, así como motor de intercambio y desarrollo en el ámbito de sus funciones; por tanto, se debe adoptar una posición consciente y vigilante respecto al uso y limitaciones de los recursos y servicios informáticos críticos de la institución.

Los usuarios, internos y externos, deben ser conscientes que la importancia de la información es proporcional al valor de sus procesos, lo que hace necesario adoptar mecanismos de gestión de seguridad de la información, entre los que se pueden contar la política, reglamento, procedimientos, estructura organizacional y soluciones tecnológicas sobre la base de estándares, tanto a nivel nacional como internacional.

Es importante tener en cuenta que la seguridad de la información se define como la salvaguarda de la información para su confidencialidad y su disponibilidad, que sólo quienes estén autorizados puedan acceder a la información; además de su integridad, que la información sea exacta y completa; asegurando que los usuarios autorizados tengan acceso a la información cuando la requieran.

POLITICAS DE SEGURIDAD DE LA INFORMACION DEL PROYECTO ESPECIAL ALTO MAYO

1. Objeto

Las ***"Políticas de Seguridad de la Información del Proyecto Especial Alto Mayo"***, en adelante las "políticas", tienen como objeto establecer el marco general de seguridad de la información del Proyecto Especial Alto Mayo, en base a las necesidades y riesgos de sus procesos.

2. Finalidad

La finalidad de las políticas es la de proteger los activos de la información, la confidencialidad, disponibilidad e integridad de la información del Proyecto Especial Alto Mayo, minimizando los riesgos y asegurando la continuidad operativa.

3. Alcance

Las políticas son de cumplimiento obligatorio por el personal del Proyecto Especial Alto Mayo y de sus sedes descentralizadas, independientemente de su vínculo laboral o contractual con la institución, así como de las personas naturales o jurídicas que brindan servicios a la entidad y que tengan acceso a la información.

4. Base Legal

- TUO de la Ley N° 27444: Ley de Procedimiento Administrativo General.
- Ley N° 27927: Modificatoria de la Ley de Transparencia y Acceso a la Información Pública.
- Ley N° 27806: Ley de Transparencia y Acceso a la Información Pública.
- Ley N° 27658: Ley Marco de Modernización de la Gestión del Estado, modificada por el Decreto Legislativo N° 1446.

- Ley N° 27815: Ley del Código de Ética de la Función Pública y sus modificatorias.
- Ley N° 28716: Ley de Control Interno de las Entidades del Estado.
- Decreto Legislativo N° 822: Ley Sobre el Derecho de Autor.
- Decreto Supremo N° 043-2003-PCM: Aprueba el TUO de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
- Decreto Supremo N° 070-2013-PCM: Modifica el Reglamento de la Ley de Transparencia y Acceso a la Información Pública aprobado por Decreto Supremo N° 072-2003-PCM.
- Resolución Ministerial N° 004-2016-PCM: Aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 166-2017-PCM: Modifica el artículo 5 de la Resolución Ministerial N° 004-2016-PCM, referente al Comité de Gestión de la Seguridad de la Información.
- Resolución Ministerial N° 119-2018-PCM: Crea el Comité de Gobierno Digital, sus funciones, alcance, entre otras disposiciones.
- Resolución Ministerial N° 087-2019-PCM: Modifica los artículos 1 y 2 de la Resolución Ministerial N° 119-2018-PCM y deja sin efecto los artículos 2, 5 y 5A de la Resolución Ministerial N° 004-2016-PCM, modificada mediante Resolución Ministerial N° 166-2017-PCM.
- Resolución Ministerial N° 224-2004-PCM: Dispone el uso obligatorio de la NTP-ISO/IEC 17799: Código de Buenas Prácticas para Gestión de la Seguridad de la Información.
- Resolución de Contraloría General N° 320-2006-CG: Normas de Control Interno.

- Resolución N° 001-2007/INDECOPI-CTR: Aprueba Normas Técnicas Peruanas.
- Resolución Gerencial N° 102-2013-GRSM-PEAM-01.00: Aprueba la Directiva N° 002-2013-GRSM-01.06: "Normas y Reglas de Uso de los Recursos de Tecnologías de Información y Comunicaciones" del Proyecto Especial Alto Mayo.
- Resolución Gerencial N° 161-2014-GRSM-PEAM-01.00: Aprueba la Directiva N° 008-2014-GRSM-PEAM-01.00: "Políticas y Procedimientos para el Respaldo de Información" en el Proyecto Especial Alto Mayo.
- Resolución Gerencial N° 099-2014-GRSM-PEAM-01.00: Directiva de organización de documentos de archivo y colecciones documentales del Proyecto Especial Alto Mayo.

5. Disposiciones Generales

Las políticas se enmarcan en lo dispuesto por la Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001: 2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición" y sus modificatorias.

La información y los sistemas de información son activos importantes para el Proyecto Especial Alto Mayo, así como para la toma de decisiones de sus dependencias.

La seguridad de la información, en su concepción moderna y técnica, busca, fundamentalmente, alcanzar los objetivos de confidencialidad, integridad y disponibilidad de la información en general.

5.1. Lineamientos

5.1.1. Responsabilidades

5.1.1.1. Es responsabilidad de la Gerencia General, designar mediante documento resolutivo, al Líder de Gobierno Digital, quien será responsable de coordinar las políticas, objetivos, planes y acciones para desplegar la transformación digital y el desarrollo del gobierno digital de la entidad, teniendo en consideración los lineamientos del líder del gobierno digital.

5.1.1.2. Es responsabilidad de la Gerencia General, designar mediante documento resolutivo, a un Oficial de Seguridad de la Información, quien será responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información de la entidad. Dicha designación deberá ser puesta en conocimiento a la Secretaría de Gobierno Digital para las coordinaciones y acciones correspondientes.

5.1.1.3. Es responsabilidad de la Gerencia General conformar el Comité de Gobierno Digital, mediante documento resolutivo; el cual deberá estar integrado por:

- El/la titular de la entidad o su representante,
- El/la líder de gobierno digital,
- El/la Especialista en Sistemas e Informática,
- El/la responsable de Recursos Humanos o quien haga sus veces,
- El/la responsable de Abastecimiento y Servicios Auxiliares como representante de la atención al ciudadano,
- El/la oficial de seguridad de la información,

- El/la responsable de la Oficina de Asesoría Jurídica y
- El/la responsable de la Oficina de Presupuesto, Planificación, Estudios y Ordenamiento Territorial

5.1.1.4. Es responsabilidad del personal del Proyecto Especial Alto Mayo, detectar cualquier incumplimiento de las obligaciones y prohibiciones señaladas en las políticas y comunicarlas a la Gerencia General - Informática, quien gestionará la investigación del hecho y reportará al Comité de Gobierno Digital del Proyecto Especial Alto Mayo.

5.1.1.5. En caso de comprobarse alguna vulnerabilidad a las políticas, la entidad deberá tomar las medidas administrativas disciplinarias correspondientes.

5.1.1.6. Es responsabilidad de la Oficina de Administración del Proyecto Especial Alto Mayo:

- Que el personal, independientemente de su vínculo laboral o contractual, sea informado por su jefe inmediato superior acerca de las directivas relacionadas a la seguridad de la información.
- Que el personal se comprometa a cumplir con las políticas.
- Que todas las dependencias se responsabilicen para que el personal externo que preste sus servicios en sus ambientes de información, conozcan y cumplan lo normado en las políticas.

5.2. El Proyecto Especial Alto Mayo deberá contar con una estructura que soporta los aspectos de gobierno digital y seguridad de información, considerándose, principalmente, los siguientes:

5.2.1. Comité de Gobierno Digital, con los siguientes roles:

- Formular el Plan de Gobierno Digital, en coordinación con los órganos, unidades orgánicas, programas y/o proyectos de la entidad.
- Liderar y dirigir el proceso de transformación digital de la entidad.
- Evaluar que el uso actual y futuro de las tecnologías digitales sea acorde con los cambios tecnológicos, regulatorios, necesidades de la entidad, objetivos institucionales, entre otros, con miras a implementar el gobierno digital.
- Gestionar la asignación de personal y recursos necesarios para la implementación del Plan de Gobierno Digital, Modelo de Gestión Documental, Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información (SGSI) en los planes operativos institucionales, plan anual de contrataciones y otros.
- Promover y gestionar la implementación de estándares y buenas prácticas en gestión y gobierno de tecnologías digitales, interoperabilidad, seguridad digital, identidad digital y datos de la entidad.
- Elaborar informes anuales que midan el progreso de la implementación del Plan de Gobierno Digital y evalúen el desempeño del Modelo de Gestión Documental, Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información.
- Vigilar el cumplimiento de la normatividad relacionada con la implementación del gobierno digital,

interoperabilidad, seguridad de la información y datos abiertos en las entidades públicas.

- Promover el intercambio de datos, información, software público, así como la colaboración en el desarrollo de proyectos de digitalización entre entidades.
- Gestionar, mantener y documentar el Modelo de Gestión Documental, Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información
- Promover la conformación de equipos multidisciplinarios ágiles para la implementación de proyectos e iniciativas de digitalización de manera coordinada con los responsables de órganos y unidades orgánicas de la entidad.
- Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.

5.2.2. Oficial de seguridad de la información, integrante del Comité de Gobierno Digital, con las siguientes tareas:

- Proponer la política y objetivos de seguridad de la información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y regulación en el ámbito de seguridad de la información.
- Promover y gestionar la implementación del Sistema de Gestión de Seguridad de la Información.
- Promover la gestión de seguridad de la información en los procesos y cultura organizacional.
- Formular, revisar y aprobar la política de seguridad de la información.

- Revisar la efectividad en la implementación de la política de seguridad de la información.
- Asegurar que la implementación de los controles de la seguridad de información sea coordinada a través de la institución.
- Implementar un plan de sensibilización para que el personal interno y usuarios externos del Proyecto Especial Alto Mayo, se alinee a lo definido en las políticas.
- Proponer normas, procedimientos y controles sobre aspectos de seguridad de información.

5.2.3. Propietario de la Información

Los directores y jefes de oficinas del Proyecto Especial Alto Mayo, son responsables de generar y hacer uso de dicha información. El propietario de la información es quien define la clasificación de la data y es responsable del mantenimiento y actualización de dicha clasificación, sin perjuicio de la responsabilidad por las funciones que por delegación le sean asignadas al personal adscrito a sus dependencias.

Esta responsabilidad no puede ser delegada a terceros, con excepción de la custodia de la información que puede darse a un colaborador perteneciente a la dependencia en particular, quien apoya en las tareas operativas de administración y control de seguridad correspondiente a la información.

Es de responsabilidad del director o jefe de oficina de la dependencia designar al custodio de la información del ámbito de su competencia.

5.2.4. Custodio de la Información

Es el personal de cada dependencia que tiene la responsabilidad de mantener y proteger la información que ha sido generada. Cabe señalar que los custodios no necesitan de la información para el desarrollo de su trabajo, simplemente la procesan, la gestionan y la hacen accesible a los demás usuarios.

Las funciones más importantes que debe cumplir son:

- Asegurar el establecimiento y aplicación de los controles establecidos en las políticas.
- Asegurar que la información entregada al usuario sea actualizada e íntegra.

5.2.5. Usuario de la Información

Persona o conjunto de personas internas, autorizadas para consultar, ingresar, modificar o borrar la información almacenada en los sistemas informáticos u otros medios de almacenamiento.

Los usuarios sólo deben tener acceso a la información a la que están autorizados a consultar y procesar. Las autorizaciones que se otorguen limitarán su capacidad en los entornos informáticos de forma que no puedan realizar actividades diferentes a las autorizadas.

Toda vez que se confíe información a un tercero, previamente, deberá suscribir el Acuerdo de Confidencialidad, el mismo que incluirá las instrucciones precisas para el manejo de los datos y la eliminación o borrado de los mismos, cumplido el periodo circunstancial que llevo a confiar en el tercero.

En el caso que se requiera que el Proyecto Especial Alto Mayo firme un Acuerdo de Confidencialidad con terceros, debe hacerse uso del modelo que se muestra en el Apéndice N° 02.

Las principales responsabilidades de los usuarios de información son las siguientes:

- Utilizar la información sólo para el propósito para el que recibió autorización de uso.
- Cumplir los controles establecidos en la normativa interna.
- Adoptar las medidas adecuadas para evitar que la información se divulgue o utilice sin autorización.
- Informar de inmediato al propietario de la información y al Especialista en Sistemas e Informática sobre cualquier exposición de seguridad de los activos de información, sea esta real o potencial.

- **Propiedad de la Información**

  Toda la información generada, almacenada y soportada por el Proyecto Especial Alto Mayo, pertenece a la entidad y no puede ser utilizada en beneficio personal o de terceros.

- **Requisitos de la Documentación**

  La documentación debe incluir registros de las decisiones de las direcciones y oficinas del Proyecto Especial Alto Mayo, que asegure que las acciones realizadas respondan a las decisiones adoptadas y a las normas establecidas.

  La documentación del Sistema de Gestión de Seguridad de Información (SGSI) deberá incluir lo siguiente:

  - Declaraciones documentadas de las normas y procedimientos que correspondan a la Seguridad de la Información.
  - Alcance del SGSI.
  - Descripción de la metodología de evaluación del riesgo.
  - Informe de evaluación del riesgo.
  - Plan de tratamiento del riesgo.
  - Procedimientos documentados necesarios en la organización para garantizar la planificación efectiva, funcionamiento y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles.

6. Disposiciones Específicas

- **Control de Documentos**
  - Los documentos exigidos por el SGSI estarán protegidos y controlados. Se establecerá un procedimiento documentado para definir las acciones administrativas necesarias para:
    - Revisar y actualizar los documentos que sean necesarios.
    - Emitir visto bueno en la documentación para su implementación.
    - Asegurar que los cambios y el estado de la versión actual de los documentos sean identificados.
    - Asegurar que las versiones más recientes de los documentos pertinentes estén disponibles en los puntos de uso.
    - Asegurar que los documentos sean legibles y fácilmente identificables.
    - Asegurar que los documentos se encuentren disponibles para quienes los necesiten y sean transferidos, almacenados y dispuestos en concordancia con los procedimientos aplicables para su clasificación.
    - Asegurar que los documentos de origen externo sean identificados.
    - Asegurar que la distribución de documentos sea controlada.
    - Proponer documentos normativos relacionados al ámbito de su competencia.

- **Control de Registros**

  Se establecerán y mantendrán registros para ofrecer evidencia de la conformidad con los requisitos y el funcionamiento efectivo del SGSI. Estos registros deberán ser controlados. El SGSI tomará en cuenta

procesamiento, almacenamiento y comunicación de información del Proyecto Especial Alto Mayo, la misma que comprende:

- **Controles de Acceso Perimetral**
  - El personal del Proyecto Especial Alto Mayo, bajo cualquier modalidad de contratación, deberá ser plenamente identificado durante su permanencia en la institución.
  - Los visitantes o terceros que presten servicios para la entidad, a su ingreso a las instalaciones del Proyecto Especial Alto Mayo, deberán estar adecuadamente identificados y anunciada su llegada a través del personal de vigilancia, previo a su desplazamiento por las oficinas.
  - Cualquier bien que ingrese o salga de las instalaciones del Proyecto Especial Alto Mayo, debe ser registrado por el personal de vigilancia.
  - Las puertas de acceso a las áreas de manipulación o administración de información confidencial o privada, deberán permanecer cerradas en todo momento.
  - Para el ingreso o salida de cualquier bien, deberá tramitarse el formato de actualización que tiene establecida la entidad con el registro completo de la información que se necesita.
  - Las personas que ingresen a las áreas restringidas del Proyecto Especial Alto Mayo, deberán cumplir los controles establecidos para los accesos específicos a dichas áreas.

- **Controles Ambientales**

  Los ambientes donde se procese, almacene y comunique la información del Proyecto Especial Alto Mayo deben ser implementados teniendo en cuenta los estándares y

recomendaciones de seguridad física y ambiental de organizaciones y/o profesionales especialistas en el tema (ambientes, materiales, energía, cercanía a medios inseguros, mecanismos de seguridad y respaldo, etc.).

- El Proyecto Especial Alto Mayo proporcionará un ambiente adecuado para la conservación de medios magnéticos y equipos.
- El Proyecto Especial Alto Mayo mantendrá en condiciones óptimas la limpieza, la seguridad, el mantenimiento y la funcionalidad de cada uno de los elementos que forman parte del centro de datos de la entidad.
- El Proyecto Especial Alto Mayo proporcionará el ambiente adecuado para la conservación de los documentos de tipo archivístico y bibliográfico.

- **Controles de Acceso a los Ambientes**

  Las visitas a los ambientes donde se procese, almacene y comunique la información del Proyecto Especial Alto Mayo, deben de ser identificadas, autorizadas, registradas y supervisadas por un empleado autorizado durante la permanencia en dichos ambientes.

- **Seguridad del Personal**

Permite conocer al personal del Proyecto Especial Alto Mayo, cuál es el rol y participación respecto a la seguridad de la información.

- **Concientización del Personal**

  La Oficina de Administración comunicará y capacitará a todo el personal, independientemente de su régimen laboral o contractual,

respecto de las Normas y Procedimientos de Seguridad de Información de la institución, asimismo, velará por su cumplimiento.

- **Ética y Disciplina**

  El personal del Proyecto Especial Alto Mayo, independientemente de su régimen laboral o contractual, deberá firmar el Compromiso de Aceptación y Cumplimiento de las Normas y Procedimientos Generales de Tecnologías de Información y Comunicación (Ver Apéndice N° 01). Además, deberá cumplir con las disposiciones contenidas en el Código de Ética de la Función Pública y demás normativa relacionada.

- **Responsabilidades del Personal**

  El personal del Proyecto Especial Alto Mayo, independientemente de su régimen laboral o contractual, es responsable de la seguridad de la información a la que tiene acceso, según las funciones o actividades que realice.

- **Contratos con Terceros**

  En los contratos que se celebren con terceros se deberá incluir la prohibición de divulgar los aspectos relativos a la confidencialidad, integridad y disponibilidad de la información a la que fuera autorizado a tener acceso, los cuales se rigen bajo el Acuerdo de Confidencialidad (Ver Apéndice N° 02).

- **Administración de Activos de Información**

  Permite proteger adecuadamente los activos de información del Proyecto Especial Alto Mayo, de acuerdo a su clasificación, la misma que comprende:

- **Clasificación de Información**

  Toda la información utilizada por el Proyecto Especial Alto Mayo deberá ser clasificada y administrada de acuerdo a su nivel de confidencialidad, integridad y disponibilidad.

- **Inventario de Activos de Información**

  Los activos de información del Proyecto Especial Alto Mayo deben ser identificados e inventariados, según su clasificación por los propietarios y responsables de dichos activos.

- **Dispositivos de Almacenamiento**

  El uso de dispositivos para el almacenamiento de información debe ser autorizado por los propietarios de la información y debe ser, exclusivamente, para fines de gestión o laborales y relacionados a las actividades propias del Proyecto Especial Alto Mayo.

- **Reasignación o Dada de Baja de Equipos**

  Los equipos que contengan dispositivos de almacenamiento de información del Proyecto Especial Alto Mayo, deben de comprobarse que dicha información haya sido sobrescrita o eliminada antes de su reasignación o dada de baja.

- **Seguridad de las Comunicaciones**

  Permite el control de las conexiones a las redes del Proyecto Especial Alto Mayo, encriptar y desencriptar la información de acuerdo a su clasificación y regular el uso de los servicios de telefonía fija, correo electrónico, internet e intranet; la misma que comprende:

- **Conexión de Componentes de Red**

  La conexión de todo componente de la red debe ser realizada bajo procedimientos y estándares de seguridad que protejan a los equipos y a la información que circula por las redes internas y externas del Proyecto Especial Alto Mayo.

- **Retiro o Desplazamiento de Activos de Información**

  El retiro y/o desplazamiento de activos de información de los ambientes de procesamiento, almacenamiento y comunicación de información sólo procede con la autorización del responsable de los activos y utilizando los medios de transporte autorizados por el Proyecto Especial Alto Mayo.

- **Sistemas de Telefonía**

  Los equipos de anexos internos y teléfonos directos deberán ser utilizados, exclusivamente, para los fines propios de la gestión o trabajo, salvo casos de llamadas de emergencia.

- **Protección de la Información en la Red**

  Se debe implementar controles o mecanismos de prevención, detección y eliminación de software malicioso que ingrese a la red del Proyecto Especial Alto Mayo.

- **Conexión a Internet**

  Los accesos a internet a través de las redes del Proyecto Especial Alto Mayo, son exclusivamente para fines de gestión o laborales, los que serán asignados solo al personal que por su función lo amerite, previa autorización del jefe de la dependencia correspondiente.

- **Conexión a Intranet**

  La intranet es de uso exclusivo del personal del Proyecto Especial Alto Mayo. La información publicada en este medio debe contar con la autorización del propietario de la información y es solo de uso interno.

- **Correo Electrónico**

  Se otorga el uso del correo electrónico al personal del Proyecto Especial Alto Mayo, solo para fines de gestión o laborales, debiendo contar con mecanismos de protección contra archivos adjuntos y mensajes no autenticados.

  Todo correo electrónico que contenga información confidencial deberá indicar en el asunto la palabra "CONFIDENCIAL", a modo de rotulación.

  Solo el personal debidamente autorizado tendrá la potestad de enviar correos electrónicos a destinatarios externos, en representación del Proyecto Especial Alto Mayo.

- **Encriptación**

  Toda la información clasificada, debe ser protegida en su almacenamiento y transporte electrónico, con algoritmos de encriptación vigentes y aprobados para su utilización por el Proyecto Especial Alto Mayo, de acuerdo a la clasificación que se le asigne.

  Se debe implementar medidas de seguridad que garanticen la confidencialidad de las claves de encriptación usadas por el Proyecto Especial Alto Mayo.

- **Desarrollo, Adquisición y Mantenimiento de Sistemas de Información**

  Los sistemas desarrollados por el Proyecto Especial Alto Mayo o contratados a terceros, deben contar con normas y procedimientos de seguridad para el desarrollo, adquisición y mantenimiento de sistemas de información, que permita proteger la información de agentes no autorizados; la misma que comprende:

- **Proceso de Desarrollo y Mantenimiento**

  El proceso de desarrollo y mantenimiento de sistemas de información debe ajustarse a las normas y procedimientos, estándares y metodologías implantadas en el Proyecto Especial Alto Mayo, así como con los acuerdos establecidos con los proveedores del servicio.

- **Adquisición de Sistemas de Información**

  En el proceso de adquisición de sistemas de información se debe especificar y cumplir los requisitos de seguridad de información, que garanticen la integridad de los sistemas existentes en el Proyecto Especial Alto Mayo, lo cual debe estar especificado en los contratos con los proveedores.

- **Ambientes de Desarrollo y Producción**

  El ambiente de desarrollo debe de mantenerse siempre separado del ambiente de producción, debiendo existir controles de acceso adecuados para cada uno de ellos.

- **Control de Cambios**

  Se debe garantizar la operatividad de los sistemas informáticos a través de la implementación de controles, pruebas y verificación, antes de su pase a producción, bajo un adecuado nivel de segregación de funciones.

- **Derecho de Propiedad Intelectual**

  El Proyecto Especial Alto Mayo tiene la propiedad exclusiva sobre la patente, derechos de autor y otros derechos de propiedad intelectual de todo aquello que sus empleados y servicios contratados de terceros desarrollen para el Proyecto Especial Alto Mayo. "Esta cláusula debe incluirse expresamente en los contratos".

  Se debe asegurar que el software del Proyecto Especial Alto Mayo (adquirido o desarrollado internamente) cumpla con la normativa vigente.

  Los productos de software o modificados internamente a nombre del Proyecto Especial Alto Mayo, son propiedad exclusiva del Proyecto Especial Alto Mayo.

  El software desarrollado internamente por el personal del Proyecto Especial Alto Mayo, deberá inscribirse a nombre del Proyecto Especial Alto Mayo en el registro intelectual respectivo, con el objeto de acogerse a los resguardados que estipula la Ley de Propiedad Intelectual.

- **Continuidad de Servicios de Sistemas de Información**

  Asegurar un nivel aceptable de operatividad y disponibilidad de los servicios críticos, ante fallas de los sistemas de información que sostienen a los procesos del Proyecto Especial Alto Mayo; la misma que comprende:

  - **Plan de Continuidad**

    El Proyecto Especial Alto Mayo debe implementar un Plan de Continuidad de los Sistemas y Servicios de Información para garantizar la operatividad y disponibilidad de los sistemas y servicios brindados, ante cualquier falla o interrupción en los mismos.

  - **Respaldo de la Información**

    Toda información crítica o sensible del Proyecto Especial Alto Mayo debe ser almacenada y respaldada en medios magnéticos mientras dure su vigencia.

- **Manejo de Incidencias de Seguridad de Información**

  Administrar adecuadamente las incidencias y debilidades de seguridad de información presentadas en los sistemas de información, minimizando sus ocurrencias e impacto sobre los procesos del Proyecto Especial Alto Mayo; la misma que comprende:

  - **Respuesta Ante Incidencias**

    Se debe contar con planes de respuesta ante incidencias y debilidades de seguridad que afecten la operatividad de los sistemas informáticos del Proyecto Especial Alto Mayo, y que

permita restaurar los servicios afectados en el menor tiempo posible.

- **Administración de las Incidencias**

  Se deben instalar mecanismos para monitorear y cuantificar los tipos, ocurrencias e impacto de las incidencias, que permita implementar controles para minimizar su frecuencia e impacto en el Proyecto Especial Alto Mayo.

- **Mejora Continua del Sistema de Gestión de la Seguridad de la Información**

  El Proyecto Especial Alto Mayo mejorará continuamente la efectividad del sistema de gestión de la seguridad de la información a través del uso de la norma y procedimientos de seguridad de la información, objetivos de seguridad, resultados de auditorías, análisis de eventos monitoreados, acciones correctivas y preventivas, y revisión gerencial.

7. Glosario de Términos

Con la finalidad de facilitar la lectura y aplicación de las políticas, éstos contienen un Glosario de Términos.

ACEPTACION DEL RIESGO: Decisión de aceptar el riesgo.

ACTIVO: (Seguridad de la Información) Es cualquier información o sistema relacionado con la captura, generación, tratamiento, almacenamiento y presentación de la misma, el cual tienes un valor para la institución. Estos pueden ser:

- **Activo de información:** Archivos, bases de datos, manuales procedimientos operativos o de soporte, contratos y acuerdos, material de formación, información financiera, documentos con información de investigación y desarrollo, correo físico y electrónico, libros revistas, etc.
- **Activos de software:** Software de aplicación, software del sistema, herramientas y programas de desarrollo.
- **Activos físicos:** Instalaciones (sala de servidores, cableado y LAN), equipos de cómputo, de comunicaciones, medios magnéticos, u otro equipo técnico.
- **Activos de servicios:** Servicios de comunicaciones, informáticos, documentarios, de información e informáticos y generales.
- **Personas:** Personal empleado, sus calificaciones, habilidades y experiencia y conocimientos.
- **Intangibles:** Reputación e imagen institucional, secretos comerciales, patentes, registros de marca, confianza de los clientes, ventaja competitiva ética productividad relación de negocios (proveedores, clientes, sociedad) logros e imagen corporativa.

ANÁLISIS DEL RIESGO: Uso sistemático de información para identificar amenazas y estimar el riesgo.

AMBIENTE DE ALMACENAMIENTO: Espacio acondicionado para resguardar la información, copias de respaldo y documentación.

AMBIENTE DE COMUNICACIÓN: Espacio acondicionado donde se establece comunicación entre los equipos y los sistemas de información.

AMBIENTE DE DESARROLLO: Espacio acondicionado donde se elabora y se pone a prueba la herramienta informática.

AMBIENTE DE PROCESAMIENTO: Espacio acondicionado donde se ingresa, se procesa y se distribuye la información.

AMBIENTE DE PRODUCCIÓN: Espacio acondicionado donde se despliega la herramienta informática para su uso.

ASIGNACIÓN Y CONTROL DE PRIVILEGIOS: Consiste en otorgar facultades de acceso a la información a un usuario autorizado, de acuerdo a las funciones delegadas.

AUTENTICACIÓN: Proceso que permite verificar la identidad de un usuario cuando éste intenta acceder a un sistema de información.

CERTIFICADO: Documento digital emitido por una entidad independiente que garantiza la identidad de los sistemas y personas en internet. La seguridad del certificado está protegida por técnicas criptográficas.

CIFRADO: Codificación de datos mediante diversas técnicas matemáticas que garantizan su confidencialidad en la transmisión.

CLASIFICACIÓN DE INFORMACIÓN: Es un proceso que permite asignar un nivel de protección adecuado a los activos de información, de acuerdo a su nivel de confidencialidad, integridad y disponibilidad.

CLAVE DE ACCESO: Conjunto de caracteres alfanuméricos, conocidos exclusivamente por el usuario propietario y que le permite el acceso a la información del Proyecto Especial Alto Mayo.

CLAVE DE ENCRIPTAMIENTO: Código que permite acceder a la información de los sistemas encriptados.

CÓDIGO MALICIOSO: Cualquier programa con una intención molesta, malévola o ilegal. Generalmente están diseñados para ejecutarse sin la intervención del usuario.

COMPONENTE DE RED: Es todo equipo o medio informático o de comunicación que pertenece a la red del Proyecto Especial Alto Mayo.

CONFIDENCIAUDAD: Garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado.

CONTRASEÑA: Conjunto de letras, números y símbolos, o incluso frases, utilizadas para autenticar usuarios en un sistema informático. Para que el uso de contraseñas sea efectivo es necesario escogerlas de manera que sean difíciles de adivinar para un atacante.

COOKIE: Información que, remitida por un servidor de internet al navegador, es devuelta posteriormente en cada nueva conexión. Pueden utilizarse con intenciones legítimas, como la identificación de usuarios, o malévolas, como el almacenamiento no consentido de pautas de navegación.

CORREOS ENCADENADOS: Son mensajes de correo electrónico donde se solicita que el mensaje sea reenviado a otras personas para que éstas a su vez los reenvíen. Es una de las posibles fuentes de problemas con el correo electrónico, ya que a veces contienen noticias falsas, pueden ser portadores de virus, etc.

CRIPTOGRAFÍA: Disciplina que se ocupa de la seguridad de la transmisión y el almacenamiento de la información.

CUSTODIO DE LA INFORMACIÓN: Es el empleado que protege y resguarda la información.

DENEGACIÓN DE SERVICIO: Ataque informático que, sin afectar a la información contenida en un sistema, lo deja incapacitado para prestar servicio. La denegación puede conseguirse mediante la saturación o el bloqueo de las máquinas.

DECLARACION DE APLICABILIDAD: Documento que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la institución.

DISPONIBILIDAD: Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados de acuerdo a los niveles establecidos.

ENCRIPTACIÓN: Medida de seguridad que permite codificar y decodificar la información del Proyecto Especial Alto Mayo, de tal manera que no sea legible o fácil de entender por personas no autorizadas.

FILTRADO DE CONTENIDOS: Conjunto de tecnologías que permiten un control de la información transmitida por servicios de internet. El filtrado de contenidos se utiliza para bloquear virus enviados por correo electrónico, para controlar el acceso a internet de menores, etc.

ESTIMACIÓN DEL RIESGO: Proceso total de análisis y evaluación del riesgo.

EVENTO DE LA SEGURIDAD DE LA INFORMACIÓN: Ocurrencia identificada en un sistema servicio o red indicando una posible brecha de la política de seguridad de la información o falla de las salvaguardas o una situación desconocida previa que puede ser relevante.

EVALUACION DEL RIESGO: Proceso de comparación del riesgo estimado frente al criterio de riesgo para determinar el significado del riesgo.

FIREWALL: Sistema de red que controla a que máquinas y servicios se puede acceder dentro de una red. Puede ser un sistema especializado o un programa instalado (firewall personal). Cuando este control se realiza sobre la información trasmitida y no simplemente sobre la conexión el sistema empleado es un proxy.

FILTRADO DE CONTENIDOS:

FIREWALL PERSONAL: Firewall instalado como un programa en una máquina que controla exclusivamente los accesos a ésta. Suele emplearse en ordenadores domésticos con conexión directa a internet.

FIRMA ELECTRÓNICA: Información digital asociada a una operación en particular realizada en internet que, junto con los certificados, permite garantizar la identidad de los participantes en una transacción.

GENERACIÓN Y ACCESOS A REGISTROS (LOGS): Consiste en recopilar los datos mínimos necesarios para generar registros a fin de poder reconstruir una acción, transacción u operación para fines de auditoría.

GESTION DEL RIESGO: Actividades coordinadas para dirigir y controlar el riesgo en una organización.

GUSANO: Tipo de código malicioso cuya característica principal es que se copia de unos sistemas a otros a través de internet.

INGENIERÍA SOCIAL: Técnicas que intentan atacar la seguridad de los sistemas informáticos engañando a sus usuarios y administradores. La mayoría de las técnicas de ingeniería social son similares a los timos.

INCIDENTE DE LA SEGURIDAD DE LA INFORMACION: Una serie de eventos no deseados que tienen una probabilidad significativa de comprometer operaciones del negocio y amenazar la seguridad de la información.

INTEGRIDAD: La información no puede ser alterada ni eliminada por cambios no autorizados o accidentales.

INTRUSIÓN: Intromisión informática en la que el atacante consigue obtener un control completo sobre la máquina. Durante una intrusión el atacante puede obtener y alterar todos los datos de la máquina, modificar su funcionamiento e incluso atacar a nuevas máquinas.

PERFIL DEL USUARIO: Es el nivel de autorización a la información que se le asigna a un empleado de acuerdo a las funciones encomendadas.

PLAN DE CONTINUIDAD: Conjunto de procedimientos a seguir en caso se presente una ocurrencia inesperada, permitiendo asegurar la continuidad de los procesos.

PROPIETARIO DE LA INFORMACIÓN: Es el empleado o dueño de la información que le es asignada para el desempeño de las actividades a su cargo.

PROXY: Sistema informático cuya misión es hacer de intermediario entre un sistema y otro a través de internet. Entre las misiones de un proxy están acelerar el acceso a internet, filtrar los contenidos a los que se ha accedido y proteger los sistemas evitando su comunicación directa.

RIESGO RESIDUAL: Riesgo remanente después de un tratamiento del riesgo.

RIESGO INFORMÁTICO: Es la posibilidad de ocurrencia de alguna situación inesperada que no permita operar normalmente los medios de tecnología de información.

SEGREGACIÓN DE FUNCIONES: Es la delimitación de funciones que permite controlar y/o reducir el mal uso o modificación no autorizado de los sistemas de información y/o servicios.

SEGURIDAD DE INFORMACIÓN: Preservar la confidencialidad, integridad y disponibilidad de la información; además, también pueden ser involucradas otras características como la autenticación, responsabilidad, no-repudio y fiabilidad.

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (ISMS): Es la parte del sistema integral de gestión, basado en un enfoque del riesgo del

negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

SOFTWARE MALICIOSO: Programas no autorizados que ingresan a la red para causar daño a la institución (virus informáticos, gusanos, caballos de Troya, bombas lógicas, etc.).

SPAM: Correo comercial no solicitado que se envía a través de internet. El volumen y contenido del SPAM puede dificultar notablemente el uso de servicios de correo electrónico.

TECNOLOGÍA DE INFORMACIÓN: Es el conjunto de elementos que brindan soporte directo o indirecto a los procesos. Está compuesta por infraestructura (equipos, redes, sistemas base y aplicaciones) e información (bases de datos, procesamiento y transmisión de información).

TERCEROS: Se considera como terceros a las personas o entidades que brindan servicios al Proyecto Especial Alto Mayo bajo diferentes modalidades de contrato.

TRATAMIENTO DEL RIESGO: Proceso de selección e implementación de controles para minimizar el riesgo.

TROYANO: Código malicioso camuflado dentro de otro programa aparentemente útil e inofensivo. Los troyanos pueden ir incluidos dentro de programas conocidos, de forma que es necesario controlar la fuente de donde se obtiene el software.

USUARIO DE LA INFORMACIÓN: Es la dependencia o la persona autorizada que hace uso de la información.

VIRUS: El tipo más conocido de código malicioso. Programa que se copia dentro de otros programas e intenta reproducirse el mayor número de veces posible. Aunque no siempre es así, la mayoría de las veces el virus,

además de copiarse, altera o destruye la información de los sistemas en los que se ejecuta.

8. Disposición Complementaria

Los procedimientos correspondientes a las Tecnologías de la Información y Comunicación, aprobados mediante documentos resolutivos, que detallan algunos de los aspectos citados en las políticas, no han sido alterados y siguen teniendo vigencia y su cumplimiento es obligatorio por todos las direcciones y oficinas integrantes del Proyecto Especial Alto Mayo (Ver Apéndice N° 03).

APENDICE N° 01

COMPROMISO DE ACEPTACION Y CUMPLIMIENTO DE LAS NORMAS Y PROCEDIMIENTOS GENERALES DE TECNOLOGIAS DE INFORMACION Y COMUNICACION

Yo.....

.....identificado con D.N.I. N° ..... domiciliado en

.....

.....

.....

DECLARO BAJO JURAMENTO tener pleno conocimiento de las **"Normas y Procedimientos Generales de Tecnologías de la Información y Comunicación"**; y demás responsabilidades y conductas no aceptadas respecto a la seguridad de la información del Proyecto Especial Alto Mayo, comprometiéndome a salvaguardar la integridad, disponibilidad y confidencialidad de la información.

Responsabilidades:

- Me comprometo a conocer y cumplir con las **"Normas y Procedimientos Generales de Seguridad de la Información"** y todo otro documento normativo que el Proyecto Especial Alto Mayo considere implantar para cumplir con los requisitos legales y/o salvaguardar la integridad, disponibilidad y confidencialidad de la información.
- Asumo la responsabilidad sobre los sistemas y recursos puestos a mi disposición por el Proyecto Especial Alto Mayo para el desarrollo de las funciones que se me encomendó. Me responsabilizo por la seguridad de los mismos.
- Me responsabilizo por la notificación a la Gerencia General - Informática y a mis jefes inmediatos, en caso de verificar el mal uso de los recursos por

parte de algún otro personal interno o externo al Proyecto Especial Alto Mayo.

- Me comprometo a utilizar sólo aquel software que esté autorizado por el órgano competente y que me haya sido asignado para el desarrollo de las funciones encomendadas.
- Asumo la responsabilidad en el uso y manipulación de la información sobre la que tengo autorización, la que me comprometo a efectuar y proteger en base a los niveles de clasificación que tenga dicha información.
- Me comprometo a no acceder, copiar ni transferir información para la cual no tengo la autorización adecuada.

Conductas No Aceptadas

Todas aquellas indicadas en la ley como figuras penales relativas a informática, tales como:

- Distribución maliciosa o inutilización de sistemas de información, sus partes o componentes, obstaculización o modificación de su funcionamiento o modificación no autorizada de los datos contenidos en el sistema.
- Acceso o intromisión en sistemas para apoderarse, usar o conocer indebidamente la información contenida en él.
- Daño, alteración o destrucción maliciosa de los datos contenidos en un sistema de información.
- Revelación o difusión maliciosa de datos contenidos en un sistema.
- Conductas contrarias a la ley, en base a lo establecido en el Decreto Legislativo N° 822, Ley sobre el Derecho de Autor, acerca de la legislación de derechos de autor y propiedad intelectual, que regula la adquisición y el uso de software, o cualquier otra ley promulgada al respecto.
- Copiar o distribuir software, datos, códigos y manuales sin la expresa autorización del titular de los derechos de autor.

- Usar copias no autorizadas de software (sin la debida licencia). Esto incluye la ejecución simultánea de software en dos o más computadores salvo que conste debidamente autorizado en la licencia de uso.
- Fabricar, adquirir o utilizar cualquier elemento que sirva para remover o burlar, aspectos de seguridad del software legalmente adquirido.
- El no cumplimiento de este compromiso formal, será considerado por el Proyecto Especial Alto Mayo como una falta grave que atenta tanto contra la legalidad vigente como contra las normas internas, y lo faculta para adoptar las medidas administrativas que estime pertinente.

Moyobamba, ... de ..... del 20.....

.....
NOMBRES Y APELLIDOS:
D.N.I.:

Este apéndice deberá formar parte de los documentos que el personal debe firmar a su ingreso a prestar sus servicios o laborar en el Proyecto Especial Alto Mayo.

APENDICE N° 02

ACUERDO DE CONFIDENCIALIDAD

Este Acuerdo de Confidencialidad (el "Acuerdo") efectivo el día ....., es firmado entre EL Proyecto Especial Alto Mayo y ...., en adelante denominado EL TERCERO.

Por cuanto **EL TERCERO** ha recibido la solicitud para realizar ciertos servicios (los "Servicios") para el Proyecto Especial Alto Mayo; y por cuanto, en conexión con la provisión de tales Servicios, el Proyecto Especial Alto Mayo puede proporcionar a EL TERCERO cierta información considerada "Información Confidencial". En consecuencia, por lo anterior **El Proyecto Especial Alto Mayo y EL TERCERO** acuerdan lo siguiente:

1) Toda información confidencial debe ser etiquetada como "Información Confidencial" en forma escrita por El Proyecto Especial Alto Mayo antes de ser proporcionada a EL TERCERO para propósito de este documento, siendo EL TERCERO responsable de no revelar la "Información Confidencial" a ningún tercero sujeto a los términos y condiciones establecidos en este documento.
2) El término "Información Confidencial" no debe incluir ninguna información:
   a) Que no esté designada como "Información Confidencial", según lo señala el párrafo 1 de este Acuerdo.
   b) Disponible al público (incluyendo sin limitación cualquier información obtenida de cualquier agencia gubernamental y disponible al público).
   c) EL TERCERO tenga disponibilidad sobre una base no confidencial de una tercera parte.
   d) Revelada por el cliente a una tercera parte sin sustancialmente la misma restricción establecida en este Acuerdo.

e) Solicitada a ser revelada por EL TERCERO por orden de una corte o jurisdicción competente, agencia administrativa o entidad del gobierno, o por cualquier ley, norma o regulación, o por mandato de comparecencia, o cualquier otro proceso legal o administrativo, o mediante normas profesionales o regulatorias aplicables.

f) Revelada por EL TERCERO en conexión con cualquier procedimiento judicial u otro que involucre a EL TERCERO y al Proyecto Especial Alto Mayo relacionado con este Acuerdo y los Servicios.

g) Revelada con el consentimiento escrito de El Proyecto Especial Alto Mayo.

3) EL TERCERO está de acuerdo que la Información Confidencial entregada por El Proyecto Especial Alto Mayo y será usada por EL TERCERO solamente en conexión con la provisión de estos Servicios.

4) EL TERCERO debe llevar a cabo sus obligaciones bajo este Acuerdo usando las mismas normas de seguridad que utiliza para proteger su propia información, o por lo menos un razonable grado de seguridad.

5) Las obligaciones establecidas en este documento con respecto a esta "Información Confidencial", continuará en toda su extensión y efectos por un período de 5 años desde la fecha efectiva de este Acuerdo, o un período menor a 3 años en caso que así lo acuerden las partes.

6) Este Acuerdo se rige por las leyes de la República de Perú.

Encontrándose las partes conformes con la ejecución de este Acuerdo, los representantes autorizados de las partes firman este documento en duplicado en señal de conformidad.

En la ciudad de Moyobamba, el ..... de..... del 20....

El Proyecto Especial Alto Mayo

Por: .....

Título: .....

EL TERCERO:

Por: .....

Este apéndice deberá ser incluido en los contratos que el Proyecto Especial Alto Mayo formalice con terceros para la prestación de servicios.

APENDICE N° 03

Procedimientos vigentes y vinculados a las "Normas y Procedimientos Generales de Tecnologías de la Información y Comunicación" del Proyecto Especial Alto Mayo.

1. Directiva N° 002-2013-GRSM-01.06: "Normas y Reglas de Uso de los Recursos de Tecnologías de Información y Comunicaciones" del Proyecto Especial Alto Mayo, aprobado por Resolución Gerencial N° 102-2013-GRSM-PEAM-01.00.
2. Directiva N° 008-2014-GRSM-PEAM-01.00: "Políticas y Procedimientos para el Respaldo de Información" en el Proyecto Especial Alto Mayo, aprobado por Resolución Gerencial N° 161-2014-GRSM-PEAM-01.00.
3. Norma de Control de Acceso al Centro de Procesamiento de Datos del Proyecto Especial Alto Mayo.
4. Directiva N° 003-2012-GRSM-PEAM-01.00: Normas para la producción y almacenamiento de microformas en el Proyecto Especial Alto Mayo, aprobado por Resolución Gerencial N° 038-2012-GRSM-PEAM-01.00.