Contenido

1. INTRODUCCIÓN

La Alianza de Bioversity International y el CIAT (en lo sucesivo "la Alianza" o "la Organización") considera la información como un recurso valioso para alcanzar sus objetivos. El Departamento de Integración Tecnológica comprende que dicho recurso es crítico para el funcionamiento eficiente de la Organización, por lo que debe dirigir sus operaciones de manera estratégica y táctica para crear, procesar, transmitir y almacenar información, de manera que se pueda garantizar su protección en todo momento.

Asimismo, la presente Política cumple con las normas internacionales para la protección de la confidencialidad, integridad y disponibilidad de la información que obre en su poder, mediante la aplicación de un proceso de gestión de riesgos y un marco de control establecido.

La ciberseguridad incluye las medidas tomadas con el fin de proteger una computadora o recursos digitales contra el acceso no autorizado de algún actor malintencionado. Una política sólida de ciberseguridad protege los activos de información haciendo frente a amenazas a la información procesada, almacenada y transportada en los sistemas de información interconectados.

La Junta Directiva de la Alianza ha asumido el compromiso de proteger la confidencialidad, integridad y disponibilidad de la información y los recursos de información asociados con las áreas de investigación y servicios. La presente Política respalda la seguridad de la información y recursos de información, su recuperación ante desastres, gestión de riesgos, de conformidad con las leyes y reglamentos aplicables en los países donde trabajamos y maximiza la capacidad de la Alianza de alcanzar sus metas y objetivos.

2. OBJETIVO Y PRINCIPIOS RECTORES

Esta Política proporciona principios para que el personal de la Alianza se asegure de que los recursos digitales sean utilizados de manera responsable; establece el compromiso de la Administración y Junta Directiva de la Alianza con la gestión de la ciberseguridad y sus esfuerzos para abordar los riesgos de los procesos básicos y actividades de apoyo de la Organización en relación con información digital. Alinea la gestión de la ciberseguridad, a cargo del Departamento de Integración Tecnológica (IT), con los objetivos de la Alianza. Es posible que esta política no elimine todos los riesgos y amenazas a los recursos digitales, pero reducirá su impacto cuando alguno de ellos se materialice.

La presente Política establece las obligaciones y responsabilidades del personal de la Alianza, sobre la base de los siguientes principios:

- Confidencialidad: solo los procesos y usuarios autorizados deben tener capacidad de acceder a los datos o modificarlos. La información se pondrá a disponibilidad únicamente de aquellos que tienen una necesidad legítima de acceder a ella.

- Integridad: los datos deben mantenerse en estado adecuado y nadie debería poder modificarlos de manera incorrecta, ya sea por accidente o con mala intención.

- Disponibilidad: los usuarios autorizados deben poder acceder a los datos en cualquier momento en que lo necesiten.

- La información es un recurso valioso: la información es un recurso de mucho valor para la Alianza y debe gestionarse en consecuencia.

- Principio de cumplimiento normativo: todos los sistemas informáticos cumplirán con la normativa legal que afecte la seguridad de la información, sobre todo aquella relacionada con la protección de datos personales y la seguridad de los sistemas, datos, comunicaciones electrónicas y servicios.

- Proporcionalidad: la implementación de controles que mitiguen los riesgos de la seguridad de los recursos deberá hacerse buscando un equilibrio entre medidas de seguridad, la naturaleza de la información y riesgo.

- Responsabilidad: todos los miembros de la Alianza deben ser responsables de su conducta en cuanto a ciberseguridad y privacidad mediante el cumplimiento con las normas y controles establecidos. Todos los miembros de la Alianza son responsables de garantizar un uso seguro y adecuado de la información. Es responsabilidad de todas aquellas personas que han recibido acceso a la información manejarla de manera adecuada, conforme a su clasificación.

- Mejora continua: el grado de eficacia de los controles de seguridad implementados en la Alianza se revisará de manera recurrente para aumentar la capacidad de adaptarse a la constante evolución del riesgo y el entorno tecnológico.

- Intercambio de información: los usuarios cuentan con acceso a la información necesaria para llevar a cabo sus funciones; por tanto, la información se comparte cuando sea permisible y adecuado.

- Seguridad de la información: la información se protege de la divulgación y uso no autorizados. Las amenazas a la seguridad y privacidad se controlan y se puede brindar capacitación al personal sobre el uso de la información y respeto de los derechos legales en caso de disputas.

- Copia de respaldo de la información: el acceso permanente a una plataforma compatible crítica que cuenta con respaldo de procesos de recuperación ante desastres evitará la pérdida de información que de otra manera se daría mediante el uso de una plataforma temporal sin respaldo. La información estará protegida de acuerdo con toda la legislación y políticas de la Alianza, en particular aquellas relacionadas con la PII, libertad de información y derechos humanos.

- Propiedad de la información: los activos de información contarán con un titular designado, quien tendrá la responsabilidad de definir los usos adecuados de la información y garantizar la implementación de las medidas de seguridad apropiadas para protegerla.

- Facilidad de uso de la información: para facilitar el hallazgo y recuperación, así como el trabajo conjunto con grupos a distancia, el uso de una ubicación de almacenamiento gestionada permitirá que todos encuentren y recuperen la información fácilmente.

- Eficiencia: la gestión centralizada de los recursos para optimizar su uso y permitir acceso a todo aquel miembro del personal que los necesite. Para recursos en la nube, la gestión centralizada facilita las economías de escala, así como la delegación de funciones al Departamento de IT, para que los equipos de investigación puedan concentrarse en su función principal y en cambio cuenten con expertos en IT, lo cual reduce el "tiempo de ejecución" y mejora la probabilidad de éxito.

- Responsabilidad de propiedad intelectual en el desarrollo de software: todo software, incluidos sistemas operativos y aplicaciones, debe gestionarse activamente. Se debe asignar a un individuo o delegado o una unidad de la organización, que sea responsable de cada elemento de software oficialmente distribuido.

- Legalidad, legitimidad y transparencia: los datos personales deben procesarse y recopilarse de manera legal, legítima y transparente, en relación con el individuo a quien se refieren dichos datos. Asimismo, se debe informar a las personas la forma en que se manejarán sus datos.

- Delimitación de la finalidad: el fin del procesamiento de los datos personales es especificado, explícito y legítimo. Los datos personales no deben procesarse para ningún otro fin. Cambios posteriores en el fin inicial pueden efectuarse únicamente hasta cierto punto y requieren de justificación y validación.

- Minimización de datos: asegurar que los datos personales son adecuados, relevantes y se limitan a lo necesario para un determinado fin.

- Exactitud: los datos personales deben ser exactos y, cuando sea necesario, mantenerse actualizados; debe tomarse cada medida razonable para asegurar que los datos personales que sean inexactos, según el fin para el que se están procesando, se borren o rectifiquen a la mayor brevedad.

- Restricciones de transferencia: los datos personales no deben transferirse a otros países (ni a otras oficinas regionales) que no ofrezcan un nivel adecuado de protección.

- Anonimidad: todos los datos personales publicados en acceso abierto deben ser anónimos para proteger la identidad de los individuos a quienes se refieren dichos datos.

3. ALCANCE

La presente política aplica a

- Todo el personal de la Alianza (incluidos los equipos de investigación y operaciones), miembros de la Junta Directiva, directores, personal temporal, consultores, proveedores y otras terceras partes que cuentan con acceso a datos institucionales (incluidos sistemas, redes y datos de investigación de la Alianza) y/o procesar datos personales en nombre de la Alianza.

- Toda la información y localidades desde las que se accede a los sistemas de la Alianza (incluido el uso desde casa). Donde haya vínculos que permitan a organizaciones ajenas a la Alianza acceder a cualquier tipo de información de la Alianza, esta debe confirmar que las políticas de seguridad que aplican cumplen con nuestros requisitos en materia de seguridad.

- Todo el personal que requiera la provisión de recursos informáticos en la nube, como servicios, plataformas e infraestructura que brinda apoyo a una amplia gama de actividades que conllevan procesamiento, intercambio, almacenamiento o gestión de datos institucionales.

- Todos los activos de información y datos recopilados, registrados, utilizados y distribuidos por la Alianza en bases de datos, archivos de datos, documentación del sistema, correo electrónico, manuales de usuario, materiales didácticos e información archivada.

- Datos personales de individuos identificables, tales como
    - Empleados actuales, pasados y potenciales
    - Donantes, socios
    - Cualquier individuo de quien recopilemos datos personales (por ejemplo, a través de encuestas o como parte de talleres impartidos por la Alianza, etc.)
    - Usuarios de los sitios web de la Alianza
    - Suscriptores y otras partes interesadas

- Mientras implementan sus proyectos, los empleados deben asegurarse de cumplir con la presente política.

4. SIGLAS Y DEFINICIONES

Siglas

AIARC	Asociación de Centros Internacionales de Investigación Agrícola
API	Interfaz de Programación de Aplicaciones
BPC	Plan de Continuidad de Labores
CSF	Marco de ciberseguridad
DRP	Plan de Recuperación ante Desastres
ERP	Planificación de los Recursos de la Empresa
HR	Recursos Humanos
IRB	Junta de Revisión Institucional

ISMS	Sistema de Gestión de la Seguridad de la Información
ISPMS	Sistema de Gestión de la Seguridad y Privacidad de la Información
MS	Microsoft
MFA	Autenticación Multifactorial
NIST	Instituto Nacional de Normas y Tecnología
OCS	Un Sistema Común (el sistema de ERP de la Alianza, también conocido como Agresso)
PII	Información Personal Identificatoria
IT	Departamento de Integración Tecnológica
URL	Localizador Uniforme de Recursos (se refiere a una solución web que especifica su ubicación en una red informática y el mecanismo para su recuperación)
VPN	Red Privada Virtual utilizada para acceder de manera remota a recursos que se encuentran "en las instalaciones", por ejemplo, una unidad de red ubicada en un servidor dentro del campus
WPA2	Acceso WiFi protegido 2: clave compartida previamente. Este es un método para asegurar el acceso a redes inalámbricas

Definiciones

Dispositivos administrados por la Alianza: dispositivos asignados al personal o consultores por parte del Departamento de IT.

Datos anónimos: información que no se relaciona con una persona física o identificable; datos personales que se han convertido en anónimos de manera tal que la persona a quien se refieren los datos ya no es identificable.

Titular del proceso laboral: individuo responsable de identificar los requerimientos del proceso, aprobar el diseño de ese proceso y gestionar el desempeño de dicho proceso. Debe encontrarse a un nivel de mando adecuado dentro de la organización y tener autoridad para comprometer recursos para actividades de gestión de riesgo específicas del proceso.

Datos confidenciales: información que es altamente sensible y está prevista para un momento, proceso, uso, distribución y acceso en específico. Los datos deben clasificarse como confidenciales cuando su divulgación, alteración o destrucción no autorizada puede causar un nivel significativo de riesgo para la Alianza o sus socios.

Informática en la nube: método con el que se utilizan recursos informáticos a través de internet, por medio de infraestructura, plataformas, software u otros recursos virtuales que son proporcionados ya sea por una empresa privada o un anfitrión externo y que se va pagando en la medida en que se va usando.

Ciberseguridad: consiste en todas las tecnologías y prácticas que mantienen los sistemas informáticos y datos electrónicos a salvo.

Datos: simples hechos o cifras, porciones de información, pero no la información en sí. Una vez que los datos se procesan, interpretan, organizan, estructuran o presentan de manera tal que se hacen comprensibles o útiles, se denominan información. La información proporciona contexto a los datos.

Administrador de datos: un empleado de la Alianza especialmente capacitado para supervisar el ciclo de vida de uno o más conjuntos de datos institucionales y orienta en cuanto a "cómo" aplicar los procedimientos y políticas de seguridad y privacidad en los procesos laborales.

Persona a quien se refieren los datos: persona física que puede ser identificada de manera directa o indirecta, particularmente por medio de un identificador, como un nombre, número de identificación, datos de ubicación, identificador en línea, o bien, uno o más factores específicos a la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona física. Todas las personas a quien se refieren los datos poseen derechos legales con respecto a su información personal.

Espacio digital de trabajo: conjunto de herramientas digitales personalizadas que permiten al personal llevar a cabo su trabajo de manera eficaz, así como lograr mejoras constantes en cuanto a colaboración y comunicación. Idealmente, la plataforma en que se llevan a cabo las actividades diarias debería estar completamente fusionada con las funciones típicas asociadas con una Intranet y no percibidas como una entidad independiente.

RGPD: Reglamento General de Protección de Datos de la Comunidad Europea.

Hardening: proceso de mejora de la seguridad del servidor a través de diversos medios, lo cual da como resultado un entorno operativo del servidor mucho más seguro. Esto se debe a las medidas avanzadas de seguridad que se implementan durante el proceso de *hardening* del servidor.

Infraestructura como Servicio (IaaS): servicio en el que el proveedor de nube gestiona la infraestructura del cliente y le cede la administración del resto de servicios, comenzando con el sistema operativo, la plataforma y todas las aplicaciones necesarias para su desarrollo. El proveedor es responsable de entregar los recursos que requieren las máquinas y asegurar su disponibilidad, pero es el cliente quien debe garantizar la disponibilidad de la aplicación y su seguridad.

Intranet: núcleo privado de información dentro de una organización que se utiliza para intercambiar información institucional y recursos informáticos de manera segura entre los empleados.

Dirección IP: dirección de protocolo de internet que consiste en una etiqueta numérica asignada a cada dispositivo conectado a una red informática que utilice un Protocolo de Internet para comunicación. La dirección IP cumple dos funciones principales: identificación de la interfaz del servidor o red y ubicación de la dirección.

Autenticación multifactorial: método de autenticación electrónica en el que un usuario informático obtiene acceso a un sitio web o aplicación, solo después de presentar satisfactoriamente dos o más evidencias (o factores) a un mecanismo de autenticación. Esto protege al usuario de que una persona desconocida trate de acceder a sus datos, como detalles personales de identidad o recursos financieros.

Datos personales: cualquier información relacionada con una persona física identificada o identificable.

Dispositivos personales: dispositivos propiedad de los empleados y no administrados o respaldados por la Alianza. El personal dispuesto a utilizarlos para propósitos laborales debe seguir las instrucciones normativas específicas.

Información personal identificatoria (PII): cualquier dato que pueda ser utilizado para identificar a un individuo en específico (p. ej., números de seguridad social, dirección postal o de correo electrónico, números telefónicos, dirección IP, ID de inicio de sesión, publicaciones en redes sociales o datos de imágenes digitales, geolocalización, biométricos y de comportamiento.

Plataforma como Servicio (PaaS): servicio en el que el proveedor de nube está a cargo de gestionar la plataforma a nivel de sistema operativo y hardware y pone a disposición una capa intermedia, donde los clientes pueden desarrollar sus soluciones. Se trata de un ejemplo típico del entorno de desarrollo de software y puede tener una administración mínima, limitada por las restricciones impuestas por el proveedor.

Datos privados: Los datos deben clasificarse como privados cuando su divulgación, alteración o destrucción no autorizada puede dar lugar a un nivel moderado de riesgo para la Alianza o sus socios. Los datos privados serán accesibles a todo el personal y no se publicarán fuera de la Organización.

Datos públicos: los datos pueden ser clasificados como públicos cuando pueden comunicarse sin restricciones y están previstos para el público en general y cuando su divulgación, alteración o destrucción no autorizada represente poco o ningún riesgo para la Alianza o sus socios.

Consejo Científico Informático: un grupo compuesto de un rango diverso de personal de la Alianza que brinda asesoría, orientación y dirección estratégica sobre iniciativas, infraestructura y prestación de servicios tecnológicos para la Alianza. Funge como embajador con comunidades de investigación y apoyo, representando y velando por sus intereses y necesidades en relación con tecnologías de la información y gestión de datos.

Software como Servicio (SaaS): servicio por el que el cliente es únicamente consumidor y el proveedor de nube se encuentra a cargo de la administración total de la solución. A nivel de cliente, normalmente solo algunos aspectos de presentación se personalizan.

Certificado SSL: el certificado de capa de conexión segura (SSL, del inglés *Secure Socket Layer*) es una tecnología de seguridad estándar para establecer un enlace cifrado entre un servidor y un cliente.

Colaboración en equipo: los sitios Team forman parte de Office 365, un estándar de CGIAR. Teams de MS permite que los equipos se comuniquen, realicen lluvias de ideas, planifiquen proyectos, conversen, discutan, llamen, editen archivos simultáneamente, etc. en un ambiente en común, accesible desde cualquier conexión a internet.

Solución web: un recurso publicado en internet y accesible a través de un URL o directamente a través de una dirección IP, como un sitio web, una base de datos, una aplicación, un servicio web, API, etc.

Cero confianza: modelo que sugiere que, por defecto, no se debe confiar en ningún usuario, aunque haya sido admitido dentro de la red, pues cualquiera puede ponernos en peligro.

5. FUNCIONES Y RESPONSABILIDADES

- Director de Integración Tecnológica: responsable de aprobar la estrategia de ciberseguridad y privacidad, presentar informes a la Junta Directiva, validar que los objetivos de la estrategia de ciberseguridad y privacidad estén alineados con los objetivos institucionales, aprobar proyectos y brindar orientación estratégica en relación con la estrategia y garantizar la implementación de dicha estrategia en el momento oportuno para asegurar que se cumpla con los objetivos.

- Coordinador de seguridad: responsable de establecer las políticas y procesos necesarios para asegurar la confidencialidad, integridad y disponibilidad de la información en la Alianza.

- Coordinador de privacidad: analiza los procesos de la Alianza en cuanto al cumplimiento de los reglamentos pertinentes e interactúa con los titulares de los procesos laborales para concertar mejoras a la protección de la privacidad de dichos procesos.

- Arquitecto de seguridad: define, implementa, monitorea y mejora la arquitectura de seguridad de la Organización. Comprende los objetivos institucionales aprobados, las políticas establecidas y las prioridades de inteligencia en cuanto a amenazas. Determina los controles necesarios para mantener los riesgos a un nivel aceptable.

- Equipo de apoyo de seguridad y privacidad: vela por la aplicación de las políticas de seguridad de la información en todos los parámetros.

- Administrador de datos: supervisa el ciclo de vida de uno o más conjuntos de datos institucionales y brinda apoyo permanente a los proyectos de investigación en la forma de aplicar las políticas y procedimientos de seguridad y privacidad en los procesos laborales.

- Subcomité de Integración Tecnológica en Seguridad y Privacidad: asigna la prioridad que merecen los objetivos institucionales que son críticos para la continuidad de la Organización; aprueba los objetivos de seguridad, bases de referencia y métricas, de acuerdo con la Junta Directiva y Equipo Directivo Senior y aprueba el programa de capacitación anual del personal en seguridad y privacidad.

- Subcomité de Integración Tecnológica en Soluciones Web: revisa la validez de las aplicaciones durante su ciclo de vida.

- Gerente de la Oficina Jurídica: brinda orientación en decisiones correspondientes a la interpretación de leyes y reglamentos.

- Titular del proceso laboral: identifica los objetivos institucionales para su función y negocia con el Equipo Directivo Senior los parámetros aceptables para la continuidad del trabajo y está a cargo de velar por que se adopte la Política de Seguridad y Privacidad dentro de su área de responsabilidad.

- Personal de la Alianza: tiene la responsabilidad de conocer y cumplir con la Política de Seguridad y Privacidad en su trabajo cotidiano, asegurando que la información confidencial que se produzca se proteja y se clasifique adecuadamente.

La siguiente matriz RACI muestra las responsabilidades, según el rol de cada uno, en cuanto a las actividades indicadas en la Política.

Actividades	Roles												
	Junta Directiva	Equipo Directivo Senior	Director de Integración Tecnológica	Coordinador de seguridad	Coordinador de privacidad	Arquitecto de seguridad	Equipo de apoyo de seguridad y privacidad	Administrador de datos	Subcomité de IT en Seguridad y Privacidad	Subcomité de IT en Soluciones	Gerente de la Oficina Jurídica	Titular del proceso laboral	Personal de la Alianza
Definir la política	C	A	A	R	R	R	I	C	C	C	C	C	
Desarrollar la evaluación del riesgo y metodología de tratamiento		C	A	R	R	R	I		C			C	
Controlar la implementación	I	I	A	C	C	R	I	C	C	C	C	C	I
Capacitación y sensibilización del personal			A	R	R	C	I	R	C			A	I
Monitorear y medir el desempeño	I	I	A	R	R	R	I	R	C	C	C	A/R	I
Revisión de la gestión del desempeño	C	C	A	R	R	R	I	I	C	C	C	C	I
Tratar las no conformidades, acciones correctivas y oportunidades de mejora			A	R	R	R	I	R	C	C	C	R	I

R: responsable A: debe rendir cuentas C: se le consulta I: se le informa

6. NORMAS GENERALES

Debido a desafíos y riesgos potenciales encontrados con anterioridad, se identificaron normas y principios específicos relacionados con las siguientes áreas prioritarias: clasificación de datos, protección de la privacidad, almacenamiento e intercambio de datos, provisión de servicios en la nube, trabajo seguro y soluciones web.

6.1 Clasificación de datos

Esta sección de la Política proporciona un marco para proteger los datos de riesgos, incluyendo, entre otros, la destrucción, modificación, diseminación, acceso, uso y eliminación sin autorización. Describe las medidas y responsabilidades necesarias para proteger las fuentes de datos. Se llevará a cabo de conformidad con la legislación en materia de protección de datos y privacidad en las diferentes regiones y países (como el RGPD), según corresponda a las actividades de la Alianza.

La clasificación de datos permite seleccionar subconjuntos de la información cuya protección debe hacerse con el mejor esfuerzo posible, dados los riesgos asociados con pérdida de información, sobre la base de la confidencialidad, integridad y disponibilidad de dicha información.

La clasificación de datos es una herramienta clave de seguridad que permite a la Alianza aplicar medidas de protección proporcionales al grado de confidencialidad de la información. Define responsabilidades con respecto al uso y manejo y establece el nivel adecuado de protección, basándose en riesgos y el grado de confidencialidad, criticidad e importancia de la información para la Alianza.

6.1.1 Cálculo de la clasificación

a) Principio de confidencialidad:

Este se alcanza ordenando los datos institucionales, de los servicios de investigación y apoyo, por clases: públicos, privados y confidenciales. Cada clase de datos se gestionará de diferente manera, donde los confidenciales representan la clase más crítica y requieren los mejores controles de seguridad y privacidad.

- Datos públicos: los datos deben clasificarse como públicos cuando su divulgación, alteración o destrucción no autorizada cause poco o ningún riesgo para la Alianza o sus socios. Dichos datos se encuentran disponibles para personal interno y personas externas. Aunque se necesitan pocos o ningún control para proteger la confidencialidad de los datos públicos, se requiere algún grado de control para prevenir su modificación o destrucción no autorizada.

  Los datos públicos incluyen, entre otros
  - Comunicados de prensa, información sobre cursos, datos anónimos o no identificables y códigos fuente publicados en servicios de acceso abierto y publicaciones científicas. Los datos no deben contener ninguna PPI, salvo que el propietario lo autorice expresamente.

- Datos privados: los datos deben clasificarse como privados cuando su divulgación, alteración o destrucción no autorizada pueda dar lugar a un nivel moderado de riesgo para la Alianza o sus socios. Los datos privados serán accesibles a todo el personal y no se publicarán fuera de la Organización. Cuando se necesiten para proporcionar un servicio o producto, pueden compartirse con los socios y proveedores bajo un acuerdo de confidencialidad. Se debe aplicar un grado moderado de control a los datos privados.

  Los datos privados incluyen, entre otros
  - Comunicaciones internas de la Alianza (por ejemplo, minutas, procedimientos, etc.)
  - Datos de proyectos de la Alianza que no se permite facilitar (de acuerdo con los convenios establecidos)
  - Datos administrativos de la Alianza
  - Informes de mercado de la Alianza
  - Por defecto, todos los datos de la Organización que no estén explícitamente clasificados como confidenciales o públicos deben manejarse como datos privados.

- Datos confidenciales: los datos deben clasificarse como confidenciales cuando su divulgación, alteración o destrucción no autorizada pueda representar un nivel significativo de riesgo para la Alianza o sus socios. Dichos datos son altamente sensibles y están previstos para un momento, proceso, uso, distribución y acceso en específico. Se debe aplicar el grado más alto de control a los datos confidenciales. Cuando se necesiten para proporcionar un servicio o producto, los socios y/o proveedores pueden agregarse al listado de control de acceso y los datos deben protegerse bajo un acuerdo de confidencialidad.

  Los datos confidenciales incluyen, entre otros
  - Información Personal Identificatoria, en consonancia con el RGPD
  - Datos protegidos por reglamentos de privacidad
  - Datos protegidos por acuerdos de confidencialidad
  - Información bancaria confidencial
  - Información confidencial de contratos
  - Información confidencial de los socios
  - Información estratégica de inteligencia de la Alianza
  - Información de autenticación que identifica a una persona: claves, MFA
  - Información financiera de la Alianza, excepto informes requeridos por los donantes
  - Información sobre impuestos federales de la Alianza
  - Información de pago (tarjetas de crédito, cuentas bancarias)

b) Principio de integridad:

La integridad se encuentra relacionada con el impacto de la modificación o destrucción no autorizada de la información para la Alianza y se clasifica en

- Bajo impacto: se puede esperar que la modificación o destrucción no autorizada de la información tenga un efecto adverso limitado para las operaciones, activos o personas dentro de la Alianza. Los datos se relacionan con
    - Datos obtenidos de fuentes públicas fácilmente reproducibles.

- Moderado impacto: se puede esperar que la modificación o destrucción no autorizada de la información tenga un efecto adverso importante para las operaciones, activos o personas dentro de la Alianza. Los datos se relacionan con
    - Comunicaciones internas de la Alianza (por ejemplo, minutas, procedimientos, etc.)

- Alto impacto: se puede esperar que la modificación o destrucción no autorizada de la información tenga un efecto adverso severo o catastrófico para las operaciones, activos o personas dentro de la Alianza. Los datos se relacionan con
    - Movimientos financieros.
    - Datos que se están procesando y aún no cuentan con copia de respaldo.

c) Principio de disponibilidad:

Asegura el acceso y uso oportuno y confiable de los datos y se clasifica en

- Bajo impacto de la disponibilidad: se puede esperar que la interrupción del acceso o uso de la información o de un sistema de información tenga un efecto adverso limitado para las operaciones, activos o personas dentro de la Alianza.

- Moderado impacto de la disponibilidad: se puede esperar que la interrupción del acceso o uso de la información o de un sistema de información tenga un efecto adverso importante para las operaciones, activos o personas dentro de la Alianza.

- Alto impacto de la disponibilidad: se puede esperar que la interrupción del acceso o uso de la información o de un sistema de información tenga un efecto adverso severo o catastrófico para las operaciones, activos o personas dentro de la Alianza.

El siguiente cuadro presenta los riesgos a los que cada tipo de datos (clasificados según los principios de seguridad y su criticidad) se encuentra expuesto y los controles aplicados para mitigar dichos riesgos.

		Principios de seguridad		
Criticidad		**Confidencialidad**	**Integridad**	**Disponibilidad**
Baja	**Riesgo**	Ninguno	Reputacional	Reputacional
	Controles aplicados	Etiquetado	Solo lectura	Recuperación ante desastres
Media	**Riesgo**	Limitado	Reputacional, pérdida de eficiencia, pérdida de oportunidades	Reputacional, pérdida de eficiencia, pérdida de oportunidades
	Controles aplicados	Control de acceso	Monitoreo del proceso laboral	Recuperación ante desastres
Alta	**Riesgo**	Violación de la privacidad, acciones legales, filtración de información financiera	Reputacional, pérdida de eficiencia, pérdida de oportunidades	Reputacional, pérdida de eficiencia, pérdida de oportunidades
	Controles aplicados	Control de acceso y cifrado	Monitoreo del proceso laboral	Recuperación ante desastres

6.1.2 Normas institucionales

- El personal debe definir todos los datos institucionales propios o con licencia de la Alianza siguiendo las definiciones de la sección 6.1.1 (Cálculo de la clasificación) precedente.
- El personal debe seguir los pasos para la clasificación de datos, de la manera que se presenta a continuación:

    - Valoración: el titular de los datos debe asignar un valor de acuerdo con los principios y categorías:

PRINCIPIOS	CATEGORÍA Y VALORACIÓN		
Confidencialidad	Público = 1	Privado = 2	Confidencial = 3
Integridad	Bajo = 1	Moderado = 2	Alto = 3
Disponibilidad	Bajo = 1	Moderado = 2	Alto = 3

    - Criticidad: define el alcance de la aplicación del proceso de recuperación de los datos ante desastres. El nivel de criticidad se calcula como la suma de los valores obtenidos de la valoración. Cuanto mayor sea la criticidad, menor deberá ser el tiempo de recuperación.

Confidencialidad + integridad + disponibilidad	Nivel de criticidad
3	Bajo
4	Bajo
5	Medio
6	Medio
7	Alto
8	Alto
9	Alto

- De acuerdo con la clasificación efectuada por el usuario, el Departamento de TI debe asegurar que
  - El acceso del usuario a los datos sea más restringido, conforme se pasa de datos públicos a confidenciales.
  - La copia de respaldo de los datos sea más redundante, conforme se pasa de bajo a alto impacto.

6.1.3 Responsabilidades y titularidad

- Toda información debe contar con un titular. Puede ser el autor del documento o departamento responsable de los datos o información.

- Aunque se reconoce que no es posible marcar cada uno de los documentos de la Alianza con una clasificación adecuada de la información, es responsabilidad de todos los miembros de la Alianza tener conocimiento de las tres clasificaciones de la información y la forma en que se debe manejar cada categoría.

- Para la mayoría de la información, es probable que la categoría que aplica sea obvia. Cuando exista ambigüedad, es responsabilidad del titular de los datos asegurar que el documento o información se marque claramente y que cualquier persona que cuente con acceso a la información tenga conocimiento de su estatus. Este es particularmente el caso de la información confidencial y privada.

6.2 Protección de la privacidad

Esta sección de la Política establece el modus operandi de la Alianza en relación con la gestión de los datos personales, con el objetivo de desarrollar ciencia respetuosa con las personas, cumplimiento con las normas y protección de los datos personales de los empleados.

La seguridad y privacidad de los datos personales es importante para la Alianza. La Alianza reconoce que se debe manejar determinada información sobre las personas para fines de investigación e institucionales, de conformidad con las leyes vigentes sobre protección de la privacidad y seguridad de los datos.

Tal información debe ser recopilada, conservada y utilizada únicamente para los fines claramente definidos, necesarios y adecuados y debe ser controlada y salvaguardada para garantizar la protección de la privacidad personal en la medida en que lo requiera la ley. Ello establece que todo procesamiento de datos personales dentro de la Alianza debe realizarse de conformidad con la legislación en materia de protección de datos y privacidad (como el RGPD) en las diferentes regiones y países donde opera la Alianza.

Normativa aplicable en materia de privacidad:

Alcance	Normativa	En vigencia desde
Todas las personas físicas	RGPD	25 de mayo de 2018

Otros países fuera de Europa en que opere la Alianza pueden contar con leyes específicas para la protección de datos. El personal debe indicar al coordinador de privacidad sobre nuevas normas locales de privacidad o cambios a estas que sea necesario analizar. En caso de que las normas locales sean más estrictas o tengan requerimientos diferentes en cuanto a privacidad, es probable que sea necesario hacer algunos ajustes a los procedimientos locales y así poder cumplir con la normativa.

La Alianza cumple con los principios relacionados con el procesamiento de datos incluidos en el RGPD, adaptados a su entorno.

6.2.1 Bases legales para el procesamiento de datos

Es responsabilidad de la Alianza cumplir con las leyes, reglamentos y normas de protección de datos, las cuales deben validarse en cada país, según las leyes específicas (el personal debe consultar con el departamento legal).

- Límite de almacenamiento: los datos personales se almacenan por un periodo razonable para que cumplan el propósito para el que fueron recopilados; los usuarios pueden verificar la Política de Retención de la Alianza.
- Consentimiento para el procesamiento de los datos: los datos personales pueden procesarse luego de obtener el consentimiento por parte de la persona a quien se refieren los datos.
- Datos de usuario e internet: si se recopilan, procesan y utilizan datos personales en sitios web o aplicaciones, se debe informar de ello a la persona a quien se refieren los datos en una declaración de privacidad que incluya, cuando corresponda, información sobre cookies o medidas técnicas similares.
- Procesamiento de datos para la relación laboral: en el tema de la relación laboral, los datos personales pueden procesarse, en caso de ser necesario, para iniciar, ejecutar y rescindir el contrato laboral. Cuando se inicia una relación laboral, los datos del candidato pueden ser sometidos a procesamiento. Si dicho candidato no es aprobado, sus datos deben borrarse en

cumplimiento del periodo de retención requerido, salvo que el candidato haya convenido en que permanezcan archivados para un futuro proceso de selección. También se necesita consentimiento para utilizar los datos para futuros procesos de solicitud. En la relación laboral existente, el procesamiento de los datos siempre debe estar relacionado con el propósito del contrato laboral, siempre que no aplique ninguna de las siguientes circunstancias para el procesamiento autorizado de datos:

- Telecomunicaciones e internet: la Alianza proporciona equipo telefónico, direcciones de correo electrónico, intranet e internet, junto con redes sociales internas, primordialmente para actividades laborales. Son herramientas y recursos institucionales que pueden utilizarse dentro de las normas legales aplicables y políticas internas, particularmente, la Política de Uso Aceptable de Recursos de IT. En caso de uso autorizado para fines personales, se debe cumplir con la ley sobre confidencialidad de las telecomunicaciones en las leyes nacionales pertinentes sobre telecomunicaciones, cuando corresponda.
- Transmisión de datos personales: si se transfieren datos personales a un receptor ajeno a la Alianza, dicho receptor debe convenir por escrito en mantener un nivel de protección de datos equivalente a la presente política de protección de la privacidad o según lo requiera la legislación aplicable.
- Procesamiento de datos subcontratado/por terceras partes: antes de iniciar con el procesamiento de datos, la Alianza debe cerciorarse de que el proveedor cumplirá con sus responsabilidades. El proveedor puede documentar el cumplimiento de los requisitos en materia de seguridad de datos mediante la presentación de un certificado adecuado. En función del riesgo del procesamiento de datos, las revisiones deben repetirse de forma periódica durante el término del contrato. La Alianza debe conservar el derecho de auditar el cumplimiento del proveedor.
- En caso de contratar un procesamiento de datos transfronterizo, se debe satisfacer los requisitos nacionales pertinentes a la divulgación de datos personales en el extranjero. En particular, los datos personales del Espacio Económico Europeo pueden ser procesados en un tercer país únicamente si el proveedor puede proporcionar evidencia de que cuenta con un estándar de protección de datos equivalente al RGPD y la presente política de privacidad.

6.2.2 Derechos de la persona a quien se refieren los datos

La Alianza debe garantizar los siguientes derechos a las personas cuya información procesa:

- El derecho de estar informado: las personas tienen derecho de saber cuáles de sus datos personales está procesando la Alianza y pueden solicitar una copia de dichos datos.
- El derecho de acceso: las personas tienen derecho de obtener acceso a sus datos y otra información personal.
- El derecho de rectificar: las personas tienen derecho de corregir sus datos personales si estos no son precisos o no están completos.
- El derecho de borrar: las personas tienen derecho de solicitar que se borren o eliminen sus datos personales cuando no hay una razón de peso para que la Alianza continúe utilizándolos. No se trata de un derecho general de borrar; existen excepciones.

- El derecho de restringir el procesamiento: las personas tienen derecho de "bloquear" o suprimir el uso adicional de sus datos personales. Cuando el procesamiento se restringe, la Alianza todavía puede almacenar sus datos personales, pero no puede darle usos adicionales.
- El derecho de portabilidad de datos: las personas tienen derecho de obtener y reutilizar sus datos personales para sus propios intereses en diferentes servicios.
- El derecho de objetar: las personas tienen derecho de objetar ciertos tipos de procesamiento, incluido aquel destinado a mercadeo directo.

6.2.3 Normas institucionales

- Es necesario que el personal de la Alianza solicite consentimiento de las persona a quien se refieren los datos para recopilar y manejar sus datos personales.
- El personal debe asegurar que todos los procesos, incluidos aquellos relacionados con investigación, cumplan con el RGPD.
- Para procesos de investigación que manejen PII, los investigadores deben revisar la relevancia de los datos solicitando a la IRB que valide la protección a las personas objeto de investigación.
- El personal debe adoptar los principios de privacidad por diseño y por defecto; esto debe formar parte de la planificación inicial del proyecto y el personal involucrado debe recibir capacitación de parte de guardianes de los datos sobre los fundamentos de la regulación de la privacidad para que puedan llevar a cabo fases importantes, tales como
  - Reconocer cuando el procesamiento de la PII forma parte de un proyecto.
  - Recopilar únicamente la PII mínima necesaria para el proyecto.
  - Especificar el momento en que la PII recopilada será eliminada permanentemente o transformada en anónima.
  - Comprender que la identificación de controles de seguridad para proteger la PII que está siendo procesada requiere de habilidades profesionales proporcionadas a nivel institucional como un servicio.
  - Identificar qué procesamiento de PII se descargará en socios y a qué países/jurisdicciones se transferirá la PII para su procesamiento.
  - Identificar, especificar en el contrato y monitorear la responsabilidad de los socios en el manejo de la PII.
  - Comunicar a las personas a quienes se refieren los datos y a un registro central de la Alianza, mediante notificaciones de privacidad y otros medios necesarios, qué/cómo/cuándo un proyecto procesará PII.
  - Comprender que la promoción de los derechos de las personas a quienes se refieren los datos requiere potencial trabajo adicional durante y después de finalizado el proyecto.
  - En caso de filtración de datos, estar preparado para comunicar lo que pasó a las partes involucradas.

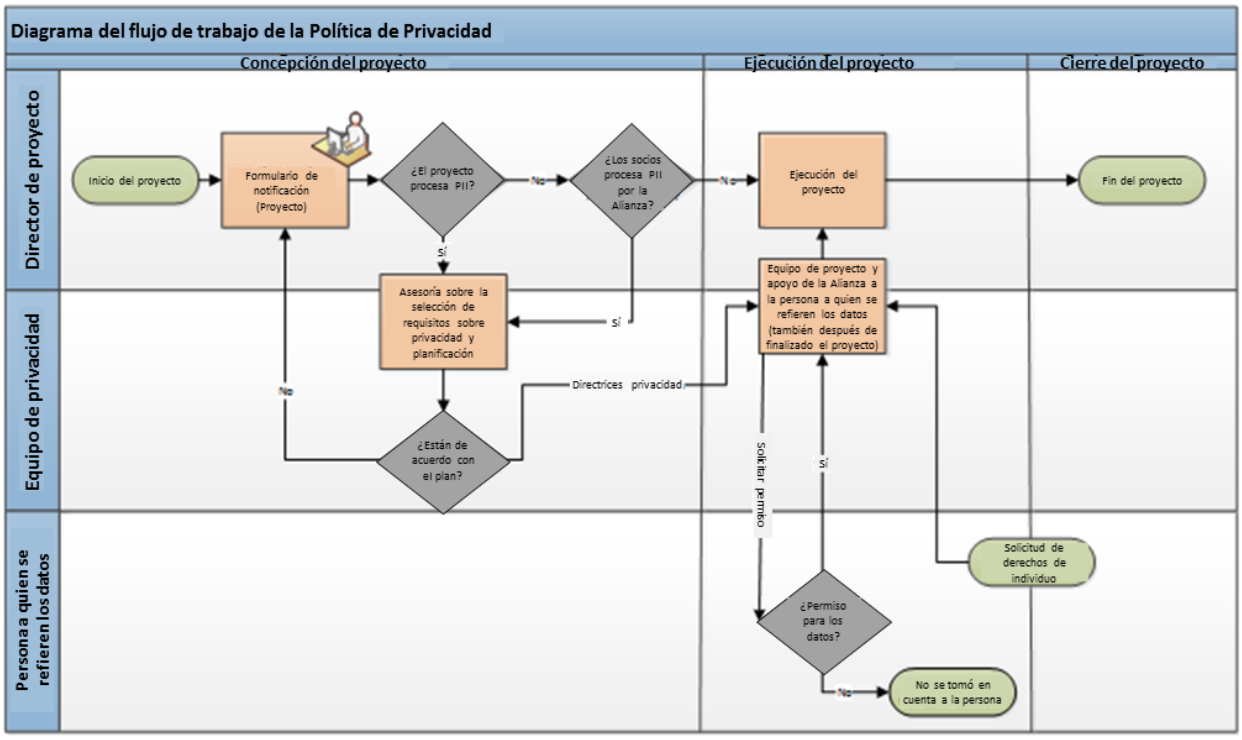
- Los titulares del proceso laboral son los responsables del procesamiento de los datos en el área a su cargo y deben velar por que se cumplan los requisitos legales y aquellos contenidos en la presente

Política. El cumplimiento de estos requisitos también es responsabilidad de los empleados que cuentan con acceso o manejan PII.

- Si organismos oficiales o donantes efectúan auditorías de protección de datos, se debe informar inmediatamente al coordinador de privacidad.
- El procesamiento incorrecto de los datos personales u otras infracciones de las leyes de protección de datos podrían ser causa de un proceso penal. Además, las infracciones de las cuales son responsables empleados individuales pueden dar lugar a sanciones según los reglamentos de la Alianza.
- El personal de la Alianza debe salvaguardar los datos personales de acceso o divulgación no autorizados (ya sea de origen interno o externo), procesamiento ilegal, así como de pérdida, modificación o destrucción accidental. Esto aplica independientemente de si los datos son procesados de manera electrónica o impresa.

6.2.4 Procedimientos de implementación

El diagrama del flujo de trabajo a continuación muestra los pasos necesarios para la aplicación de la presente Política.



6.3 Almacenamiento e intercambio de datos

La tecnología permite al personal trabajar desde cualquier parte y en cualquier momento con miembros del equipo, socios o colaboradores a distancia. El conjunto de herramientas que puede utilizarse para el almacenamiento e intercambio de datos aumenta día con día, aunque muchas de ellas no cuentan con respaldo o responden a un conjunto mínimo de estándares de seguridad establecidos por la Alianza y CGIAR.

Por ello, cambiarse a una infraestructura de almacenamiento de datos e información gestionada y respaldada por el Departamento de IT, asegurada con un procedimiento de recuperación ante desastres, es clave para permitir a los equipos colaborar de manera eficiente en tiempo y espacio con la mínima interrupción posible. Esta es también la base para convertirse en una organización en la que la información digital se almacena en ubicaciones previsibles, lo cual permite al personal utilizar y producir servicios informativos avanzados.

Esta sección de la Política establece las obligaciones del personal de la Alianza en cuanto a uso del almacenamiento de información y herramientas durante su trabajo cotidiano, con el respaldo del Departamento de IT.

6.3.1 Normas institucionales y repositorios recomendados para seguridad y privacidad

a) Proceso de colaboración: el uso de plataformas de almacenamiento gestionadas por el Departamento de IT ayuda en el manejo de la información y datos en todos los procesos de la Alianza, tanto para funciones de investigación como de apoyo, permitiendo así que la información protegida se pueda compartir de manera rápida y segura con aquellos que la necesitan para llevar a cabo sus actividades laborales. Este proceso es un esfuerzo institucional en el que cada empleado de la Alianza debe asegurar el almacenamiento de datos en los repositorios recomendados.

- El personal debe almacenar los archivos que elabore como parte de sus proyectos y actividades de servicios de investigación y apoyo en el repositorio recomendado gestionado por la Alianza.
- El Departamento de IT ha elaborado un plan de recuperación ante desastres para proteger información crítica, incluidos todos los archivos almacenados en servicios contratados, como OneDrive, carpetas de SharePoint y carpetas del sitio Teams. No existe garantía de recuperar archivos en otras áreas de almacenamiento (p. ej., en el entorno de escritorio, memorias USB, discos duros externos, etc.).
- Al compartir documentos, sobre todo con colaboradores o socios externos, el personal debe definir la fecha de caducidad de acceso externo del documento o carpeta o llevar un registro de carpetas compartidas fuera de la Organización.
- Es posible que el personal cuente con conexión limitada a internet o se encuentre trabajando temporalmente en una localidad sin conexión. Por tanto, el personal puede trabajar en una versión local de los documentos y debe asegurarse de sincronizarla con la plataforma en línea una vez se pueda volver a conectar a internet.
- Durante el desarrollo de un proyecto, es posible que el personal necesite trabajar con socios y donantes en otras plataformas (Box, Dropbox, GSites, etc.). Cualquier información almacenada en dichas plataformas debe ser posteriormente copiada en la ubicación centralizada adecuada, de conformidad con los repositorios recomendados que se hayan definido.

- La información confidencial debe protegerse mediante mecanismos de cifrado durante la totalidad de su ciclo de vida y únicamente deben acceder a ella los miembros del personal de la Alianza que la necesiten.
- El personal no debe contar con copias de archivos almacenadas en diferentes ubicaciones para evitar la duplicación de datos. Los documentos oficiales deben colocarse en una única ubicación, de acuerdo con los repositorios clave recomendados que se mencionan a continuación y que cuentan con copia de respaldo en el Departamento de IT.

b) Repositorios clave recomendados

La sección a continuación define los repositorios y el tipo de datos que deben almacenarse en cada uno de ellos.

- Espacio Digital de Trabajo (intranet en MS SharePoint desde diciembre de 2020).
    - El personal debe tener todos los archivos relacionados con su trabajo almacenados en el espacio digital institucional indicado. Tener todos los archivos almacenados en un área prevista permitirá mejorar la comunicación interna entre equipos de trabajo. Este tipo de almacenamiento también ofrece funciones avanzadas, como cifrado para proteger datos personales, cuando el tipo de datos lo requiera.
    - El personal de la Alianza procurará compartir archivos para edición a través del espacio digital de trabajo, pues aquí se maneja el historial del archivo y permite a los usuarios regresar a una versión previa del documento, cuando lo necesiten.
    - Los usuarios externos, como socios y colaboradores, pueden tener acceso al espacio digital de trabajo. Sin embargo, el manejo del contenido y sus permisos serán responsabilidad del empleado.

- OneDrive
    - A todos los miembros del personal de la Alianza se les proporciona espacio OneDrive en la nube para almacenamiento general de archivos relacionados con su trabajo. Los archivos almacenados en OneDrive no son visibles al resto de la Organización.
    - El personal puede compartir archivos/carpetas de su OneDrive con otros dentro y/o fuera de la Organización.
    - El personal debe asegurarse de que el archivo/carpeta que comparte a través de OneDrive sea posteriormente trasladado al espacio digital de trabajo una vez que la interacción haya finalizado. Si no existe una ubicación especificada previamente en el espacio digital de trabajo para dicha información, esta debe crearse mediante una solicitud al Departamento de IT.
    - El almacenamiento de PII y datos personales en este repositorio sin mecanismos de protección de la confidencialidad podría ser un riesgo para su información personal y la Alianza, representando un importante riesgo de seguridad y privacidad para la Organización.
    - El personal procurará hallar y utilizar un repositorio diferente para el almacenamiento seguro de su propia información personal y privada.
    - El personal procurará mantener sincronizados los archivos de uso constante; los archivos que no se usan con frecuencia pueden mantenerse en línea para que se pueda acceder a ellos en cualquier momento. Como servicio de almacenamiento en la nube, OneDrive puede sincronizar archivos localmente en el puerto de una computadora, de manera que una persona pueda trabajar en el archivo sin conexión a internet y que más adelante pueda cargar el archivo de vuelta a la nube.
    - Cuando un empleado se va o se cambia a otro proyecto o departamento/unidad (esto también aplica al personal de apoyo), el supervisor tiene la responsabilidad de trabajar con

la persona que se va y los equipos de Gestión de Datos y *Open Science* para asegurar que todo dato almacenado en OneDrive de relevancia para la Organización sea trasladado al espacio digital de trabajo.
    - El Departamento de IT brinda apoyo en el proceso de creación de la copia de respaldo de la información almacenada en el espacio OneDrive del usuario, lo cual no contempla una evaluación de la calidad de dicha información.
    - Cuando los empleados se van de vacaciones, deben asegurarse de que el acceso a sus archivos de trabajo por otros miembros del personal sea acordado con su supervisor.

- ERP: OCS: Agresso
    - Todos los documentos importantes, legalmente vinculantes y firmados deben almacenarse en el módulo OCS correspondiente y deben conservarse por un cierto número de años, de acuerdo con la normativa vigente; los usuarios pueden verificar la Política de Retención de la Alianza (es decir, acuerdos con donantes, acuerdos con socios, memorandos de entendimiento, convenios de acogida, etc.).

    - Si aún no existe un módulo para un tipo de documento legalmente vinculante, el personal debe asegurarse de que el documento se archive de forma manual. El personal puede remitir archivos en OCS a URL externos que dirijan a otras ubicaciones, tales como el espacio digital de trabajo.

- Almacenamiento de datos de investigación
    - El personal puede utilizar, ya sea la nube que maneja el Departamento de IT, o bien, las plataformas dentro de la sede, según sea necesario, para asegurar que la información se encuentre completamente amparada por una copia de respaldo y se sigan las buenas prácticas definidas por las auditorías y donantes. Los datos almacenados deben clasificarse siguiendo los principios descritos en las secciones 6.1 (Clasificación de datos) y 6.2 (Protección de la privacidad) y dicha clasificación debe ser reportada al Departamento de IT.
    - El Departamento de IT ha establecido la creación de una copia de respaldo para proteger información previamente acordada con investigadores, almacenada en la nube o en servidores dentro de la sede. Debe firmarse un acuerdo en cuanto al nivel de servicio entre el titular de la información y el Departamento de IT con el fin de asegurar que se están creando copias de respaldo de la información correcta y que se aceptan las condiciones de periodicidad y retención.

- Otras clases de almacenamiento
    - Repositorios de acceso abierto
        - El personal debe utilizar los repositorios institucionales de acceso abierto (como Dataverse y CGspace) para publicar sus productos de información y datos, siguiendo los lineamientos de la Política de Patrimonio Intelectual y Derechos de Propiedad Intelectual.

- Aplicaciones web (internas/externas)
  - Al desarrollar aplicaciones web internas o externas como productos esperados de proyectos, el personal debe asegurarse de que sean desarrolladas siguiendo los estándares de la Alianza, para garantizar su respaldo continuo (ver sección 6.6 Soluciones web, más adelante).

- Repositorios locales
  - El personal no debe almacenar información fuera de las ubicaciones designadas. No existe garantía de recuperar archivos en otras áreas de almacenamiento (p. ej., equipo local, memorias USB, discos duros externos, etc.)
  - El personal puede almacenar información en unidades de red (G, M, O en Roma y Z en Palmira). A estas se puede acceder desde fuera de las instalaciones mediante una VPN, que debe ser asignada y monitoreada por el Departamento de IT, con el fin de reducir los riesgos de seguridad. Estos repositorios pueden usarse temporalmente, mientras se trasladan los datos al espacio digital de trabajo.

El cuadro a continuación muestra los repositorios más adecuados recomendados para almacenamiento, según el tipo de datos, disponibles en la Alianza

	Repositorios clave			
Tipos de archivo	Espacio digital de trabajo (intranet)	OneDrive	ERP OCS	Almacenamiento de investigación (dapadfs, clúster de yuca, etc.)
Archivos de equipo	X			
Archivos de unidad	X			
Archivos de proyecto	X			
Políticas y guías	X			
Documentos firmados y escaneados (servicios administrativos y financieros)			X	
Almacenamiento general de archivos de trabajo		X		
Intercambio en directo		X		
Datos de investigación para aplicaciones específicas (bases de datos, aplicaciones, datos del banco de germoplasma, GrinGlobal, fenotipificación, genotipificación, SIG, BMS, etc.)				X

6.4 Prestación de servicios en la nube

Esta sección de la Política define las obligaciones del personal y del Departamento de IT en cuanto a la adquisición, suministro, *hardening*, mantenimiento y soporte para recursos en la nube.

Los servicios en la nube son una alternativa excelente para la implementación de nuevas soluciones tecnológicas dentro de un entorno dinámico, flexible, sumamente disponible y confiable. Con el fin de lograrlo, es fundamental contar con medidas de seguridad establecidas y crear conciencia sobre la parte que toca a los usuarios, en cuanto a las implicaciones de esta nueva forma de trabajar y las responsabilidades asumidas por el cliente y el proveedor de la nube.

La adopción de servicios en la nube va en aumento dentro de la comunidad científica. Esta Política presenta las mejores prácticas y procesos de aprobación para utilizar servicios informáticos en la nube que reducen los riesgos de IT y garantizan la eficiencia económica de la Alianza.

6.4.1 Normas institucionales

- El personal de la Alianza debe aceptar que el Departamento de IT gestione las cuentas de servicios en la nube. El Departamento de IT será el administrador de los proveedores de la nube de la Alianza, con el fin de gestionar el acceso a los recursos en la nube y velar por su seguridad, reduciendo así los esfuerzos operativos en materia de seguridad, la facturación y etiquetado de recursos.
- El personal no puede comprar o adquirir directamente soluciones en la nube con cuentas personales o de los proyectos.
- La adquisición de dichos servicios debe seguir los procedimientos de compras del Departamento de Finanzas y Operaciones.

6.4.2 Funciones y responsabilidades

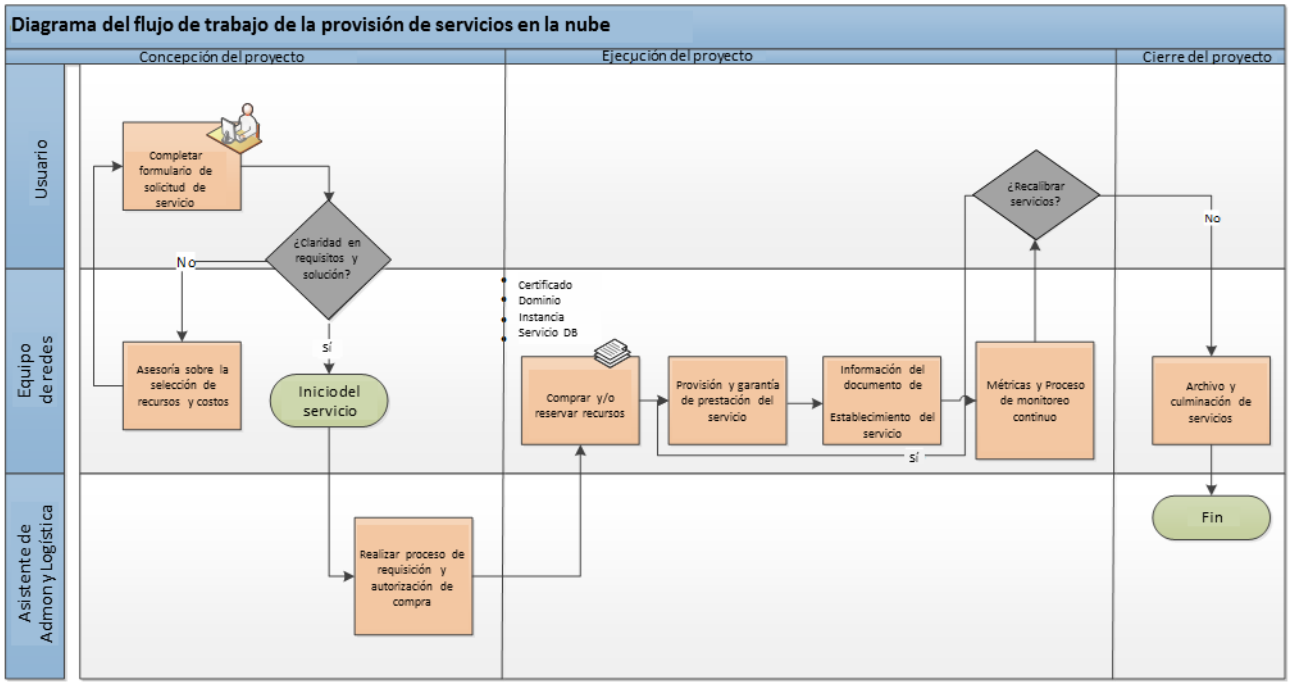
- Personal de la Alianza:
    - Para dar inicio al proceso de adquisición de servicios en la nube, el personal debe informar primero a la Unidad de Infraestructura de Red y Seguridad del Departamento de IT sobre su necesidad específica, completando un formulario de solicitud de servicios en la nube del Departamento de IT y proporcionando toda la información requerida.

- La Unidad de Infraestructura de Red y Seguridad:
    - Brindará asistencia en el cálculo del costo de los servicios en la nube requeridos.
    - Elaborará un acuerdo con el personal, informando sobre el proyecto, subvención, fondos, límite de los fondos, plazo, etc.
    - Cuando los fondos se asignen, prestará los servicios en la nube según el acuerdo, incluido el *hardening* y configuración de seguridad de dichos servicios.

- Monitoreará el uso de los servicios en la nube según el acuerdo y enviará alertas e informes para asegurar que el proyecto no se salga del presupuesto y los servicios en la nube prestados se encuentren en su punto óptimo en todo momento.
- Otorgará acceso, basándose en el principio del mínimo privilegio, verificando el nivel de acceso con la parte interesada cada seis meses.

6.4.3 Procedimientos de implementación

La figura a continuación muestra el flujo de trabajo recomendado para prestar soluciones de servicios en la nube para el personal de la Alianza.



6.5 Trabajo seguro

Esta sección de la Política define un marco que los usuarios deberán seguir a fin de asegurarse de tener un entorno de trabajo seguro cuando se encuentren fuera de las instalaciones de la Alianza. El personal trabajará principalmente desde casa y a veces con sus dispositivos personales.

6.5.1 Normas institucionales

- El personal debe contar con una MFA habilitada en sus cuentas de correo electrónico.
- El personal puede acceder a sus dispositivos gestionados únicamente a través de la cuenta designada por el Departamento de IT.

- Los dispositivos de la Alianza solo pueden utilizarse con fines laborales, esto incluye el correo electrónico institucional.
- El personal debe procurar conectarse solo a redes WiFi que utilicen el mejor protocolo de seguridad.
- El personal debe asegurarse de que todos los datos confidenciales estén cifrados cuando estén en tránsito y almacenados (de acuerdo con la Política de Clasificación de Datos).
- El personal de la Alianza debe procurar estar disponible cuando lo solicite el Departamento de IT para eliminar cualquier vulnerabilidad y efectuar actualizaciones en los dispositivos administrados por la Alianza que estén utilizando.
- El personal no debe procesar información confidencial de la Alianza en dispositivos personales.
- El personal debe acceder a información relacionada con su trabajo únicamente utilizando aplicaciones permitidas por el Departamento de IT.
- El personal puede conectarse mediante una VPN para tener acceso a servicios, en caso de necesitarlo y no contar con disponibilidad de un servicio basado en la nube.
- El personal debe asegurarse de que los datos sean cifrados al recopilar y/o almacenar información confidencial en un dispositivo móvil de la Alianza.
- El personal debe procurar utilizar las herramientas recomendadas por la Alianza para realizar conferencias web.

6.6 Soluciones web

Una solución web se define como un recurso publicado en internet y accesible a través de un URL o directamente a través de una dirección IP, como un sitio web, una base de datos, una aplicación, un servicio web, API, etc.

Esta sección de la Política someterá el proceso de publicación en la web a una supervisión uniforme, de manera tal que se tomen las medidas adecuadas de antemano, para implementar un sistema que esté razonablemente protegido. La Política garantiza la continuidad del apoyo por parte del Departamento de IT para las tecnologías utilizadas durante el ciclo de vida de la solución web.

6.6.1 Normas institucionales

- Cualquier empleado que actúe como director de un proyecto que contemple una solución web que se publique internamente o en internet debe informar a la Unidad de Infraestructura de Red y Seguridad al inicio de dicho proyecto, para que el Departamento de IT comprenda los requisitos y pueda, ya sea brindar apoyo según se necesite, o bien, asistir en la prestación de dichos servicios.

- El director de proyecto, en conjunto y de mutuo acuerdo con la Unidad de Infraestructura de Red y Seguridad, elaborará un plan de soluciones web para un proyecto, basado en los estándares institucionales actuales en materia de desarrollo y seguridad, el cual contemplará

- **Qué:** una descripción del sistema final que se entregará. Esto incluye tecnologías, bases de datos y lenguajes utilizados para desarrollar la aplicación y controles de seguridad del código fuente que se realizarán para las pruebas de aceptabilidad. Como parte de la documentación del proyecto, se debe contar con un plan de sostenibilidad y/o estrategia de salida.
- **Quién:** especificaciones de quienes serán responsables de alojar la solución web. Esto incluye la gestión de credenciales de administración, dominio y administración del certificado SSL.
- **Cuándo:** un cronograma para la puesta en marcha del sistema e información sobre el ciclo de vida.
- **Dónde:** todo código de fuente, datos relacionados y documentación (incluidos, entre otros, manuales y guías) deben centralizarse en el repositorio de códigos de la Alianza (ver la Política de Patrimonio Intelectual y Derechos de Propiedad Intelectual).
- **Monitoreo:** deben definirse métricas para monitorear el sistema en términos de desempeño y protección de seguridad y se deben entregar dos veces al año al Consejo Científico Informático para que revise la validez, relevancia e importancia estratégica de las aplicaciones durante su ciclo de vida.
- **De vuelta al trabajo:** mecanismos de recuperación ante desastres y reparación de infracciones contra la seguridad.
- **Cumplimiento de las normas de la Alianza:** el director de proyecto velará por que quienquiera que se contrate para efectuar el trabajo reciba la información pertinente y utilice las tecnologías y requisitos establecidos en el Plan de Soluciones Web del Proyecto.

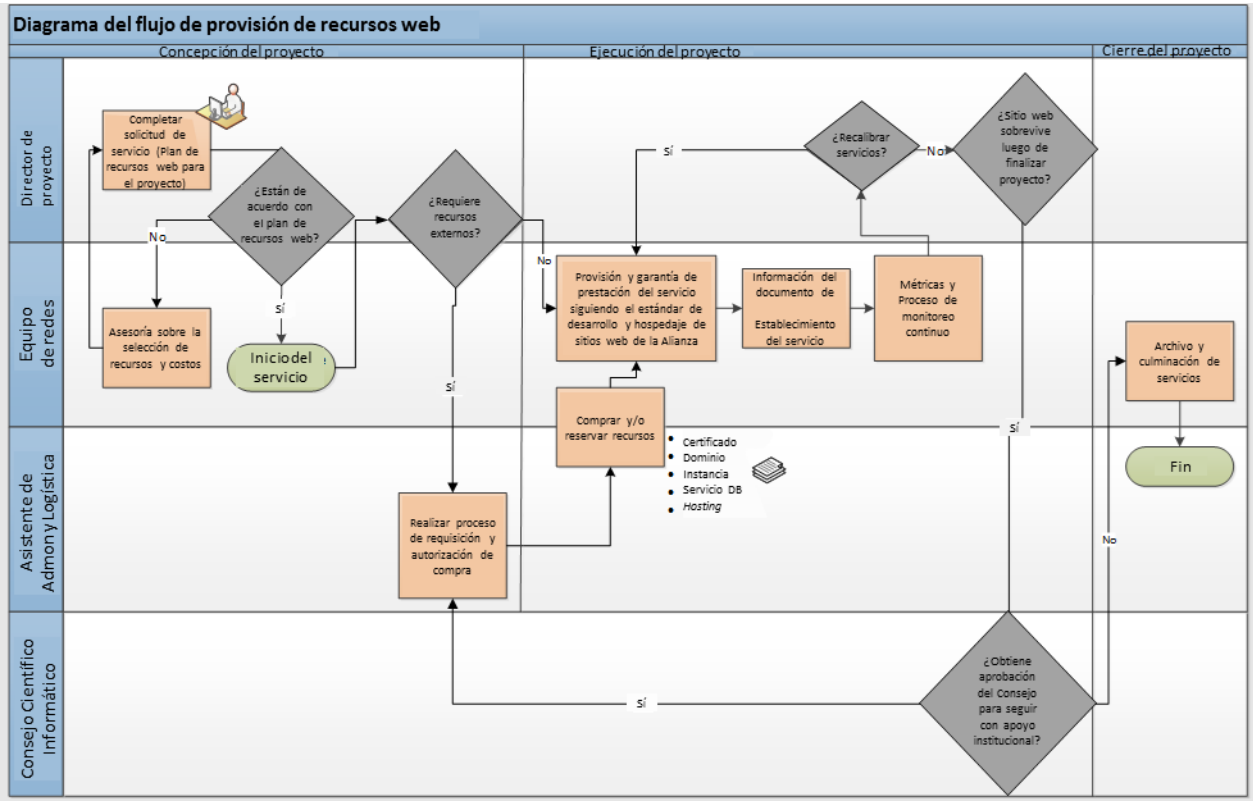
6.6.2 Funciones y responsabilidades

- Cualquier empleado que funja como director de proyecto debe participar en las siguientes actividades para cada solución web:
  - Participar en el registro y/o actualización del inventario de soluciones web publicadas y evaluar su nivel actual de riesgo, implicaciones en cuanto al RGPD y criticidad de la aplicación para el trabajo.
  - Redactar y aprobar medidas de mitigación estándar a ser implementadas para los tipos de información y servidores de publicación.
  - Proporcionar a dirección la información necesaria para decidir el ciclo de vida de cada solución web, sobre la base de su prioridad, costo, relevancia e importancia estratégica para la Alianza.
  - Elaborar un plan para la implementación de las medidas necesarias durante el ciclo de vida de la aplicación.

- El Departamento de IT:
  - Junto con el director de proyecto, será el responsable de definir la arquitectura de las soluciones web desde el inicio del proyecto.
  - Monitoreará las soluciones web durante su ciclo de vida.
  - Brindará apoyo continuo para mantener las medidas de mitigación aprobadas para cada solución web al nivel de riesgo seleccionado.
  - Definirá e implementará el plan de recuperación ante desastres para las soluciones web, de acuerdo con su criticidad.

6.6.3 Procedimientos de implementación

El diagrama del flujo de trabajo a continuación muestra los pasos necesarios para la implementación de la presente política en materia de soluciones web.



7. DENUNCIA DE INFRACCIONES

- Si se sospecha de infracciones a la presente Política, se debe informar al Coordinador de seguridad y al Coordinador de privacidad (alliance-secpriv@cgiar.org). Los informes de infracciones son considerados datos confidenciales hasta que se clasifiquen de otro modo.

8. POLÍTICAS RELACIONADAS / REFERENCIAS PARA OBTENER MÁS INFORMACIÓN

- Reglamentaciones
  - Legislación sobre protección de datos y privacidad a escala mundial:
    - Legislación sobre Protección de Datos y Privacidad a Escala Mundial | UNCTAD
    - **RGPD:** Para obtener más detalles sobre la normativa del RGPD, por favor consulte
      - Data protection | European Commission (europa.eu) (English)
      - Protección de datos | Comisión Europea (europa.eu) (Español)

- Políticas de la Alianza
  - Política de Patrimonio Intelectual y Derechos de Propiedad Intelectual
  - Política de Uso Aceptable de Recursos de IT
  - Política de Ética en la Investigación
  - Política de Retención

9. AUTORIDAD SOBRE LA POLÍTICA

El Coordinador de seguridad y el Coordinador de privacidad del Departamento de Integración Tecnológica son los responsables de la presente política, la cual será aprobada por el Equipo Directivo Senior. Se volverá a evaluar cada año para determinar si todos los aspectos del programa están actualizados y vigentes en los entornos actuales de trabajo y se modificará según se requiera. La fecha de entrada en vigencia de la presente Política revisada es el 1 de marzo de 2021. Esta Política remplaza a políticas anteriores en la misma materia, las cuales quedan anuladas.

10. CONTROL DE VERSIONES

VERSIÓN	FECHA DE APROBACIÓN DE LA VERSIÓN MÁS NUEVA	DESCRIPCIÓN DE CAMBIOS	ELABORADO POR:
00	17 de febrero de 2021	Primera versión la Política de Ciberseguridad y Privacidad	Dario Valori, Santiago Restrepo, Dolly Gómez, Idris Jones

Revisado por:	Aprobado por:
	Aprobado el 17 de febrero de 2021
David Abreu Director del Departamento de Integración Tecnológica	Equipo Directivo Senior