POLÍTICA DE GESTIÓN DE ACCESOS, CREDENCIALES Y CONTROL DE IDENTIDADES

DIGEVO VENTURES SpA

RUT N°76.414.748-0

1. Objeto

La presente Política de Gestión de Accesos, Credenciales y Control de Identidades, en adelante la "Política", tiene por objeto establecer los principios, reglas, responsabilidades y controles mínimos aplicables al otorgamiento, modificación, revisión, suspensión y revocación de accesos a sistemas, plataformas, cuentas, repositorios, servicios cloud, bases de datos, herramientas colaborativas, credenciales y demás activos tecnológicos de Digevo Ventures SpA.

Su finalidad es asegurar que solo las personas autorizadas accedan a los recursos necesarios para el cumplimiento de sus funciones, resguardando la confidencialidad, integridad, disponibilidad y trazabilidad de la información y de los sistemas corporativos. Esta lógica coincide con la Política de la Seguridad de la Información de Digevo Ventures SpA.

2. Alcance

La presente Política aplica a:

a) todos los trabajadores, ejecutivos, asesores, consultores, prestadores, practicantes, proveedores y terceros que accedan, directa o indirectamente, a sistemas o información de Digevo Ventures SpA;
b) todos los entornos de trabajo de Digevo Ventures, incluyendo cuentas corporativas, correo, herramientas colaborativas, plataformas digitales, repositorios, entornos cloud, bases de datos, sistemas internos, servicios SaaS, VPN, credenciales de terceros, tokens, secretos y APIs; y
c) todos los accesos asociados a productos, plataformas y operaciones de Digevo Ventures, incluyendo, entre otros, Evolution, Powercamp,, sitios web, repositorios de desarrollo y servicios complementarios.

3. Obligatoriedad

Toda persona a quien resulte aplicable la presente Política deberá conocerla y cumplirla íntegramente. La Compañía podrá requerir la aceptación expresa de esta Política, en formato físico o digital, como condición para el otorgamiento o mantención de accesos.

Las obligaciones contenidas en la presente Política se entienden incorporadas a los contratos de trabajo y a los contratos de prestación de servicios, según corresponda.

4. Principios rectores

La gestión de accesos en Digevo Ventures se regirá por los siguientes principios:

a) Mínimo privilegio.
Toda persona deberá contar únicamente con los accesos estrictamente necesarios para cumplir sus funciones. Este mismo principio está expresamente recogido en la Política de Seguridad de la Información de Digevo Ventures.

b) Necesidad de acceso.
Ningún acceso deberá otorgarse por conveniencia, costumbre o anticipación sin necesidad real y actual.

c) Identidad individual y trazabilidad.
Todo acceso deberá estar asociado a una identidad individual, verificable y auditable. Las acciones sobre recursos críticos deben quedar registradas en logs auditables.

d) Segregación de privilegios.
Los accesos privilegiados deberán limitarse, separarse por función y mantenerse bajo control reforzado.

e) Temporalidad.
Los accesos deberán mantenerse solo mientras exista una necesidad legítima, contractual u operativa.

f) Seguridad reforzada en accesos críticos.
Los accesos de administración, producción, bases de datos, infraestructura, despliegue y gestión de credenciales deberán contar con controles reforzados, incluyendo MFA y revisión periódica.

g) Cumplimiento de normativa de protección de datos personales.
El tratamiento de datos personales que se realice en el contexto de la gestión de accesos deberá ajustarse a la normativa vigente en materia de protección de datos personales, debiendo adoptarse las medidas de seguridad necesarias para resguardar dichos datos conforme a su naturaleza y a la Política de Privacidad y Protección de Datos Personales de Digevo Ventures.

4. Jerarquía

En caso de conflicto entre la presente Política y otros documentos internos, prevalecerá aquella que establezca estándares más estrictos en materia de seguridad de la información, salvo instrucción expresa en contrario de la Gerencia General.

5. Clasificación general de accesos

Para efectos de esta Política, los accesos se clasifican en:

a) **Accesos básicos:** correo, calendario, herramientas internas de uso general y plataformas colaborativas;
b) **Accesos operativos:** sistemas necesarios para ejecutar funciones de proyecto, soporte, operación, análisis o administración;
c) **Accesos privilegiados:** paneles de administración, repositorios críticos, entornos productivos, bases de datos, infraestructura cloud, VPN, llaves maestras, gestores de credenciales y secretos; y
d) **Accesos de terceros o servicios:** cuentas técnicas, usuarios de integración, APIs, tokens, cuentas de servicio, bots, conectores y claves automatizadas.

6. Reglas generales de otorgamiento de acceso

Todo acceso deberá cumplir, como mínimo, con las siguientes reglas:

a) solicitud previa del acceso;
b) justificación funcional u operativa;
c) validación del responsable directo o del área usuaria;
d) aprobación de la instancia competente según criticidad;
e) asignación individualizada de usuario o credencial;
f) registro del acceso otorgado; y
g) aplicación de controles de seguridad adecuados al nivel de riesgo.

No se deberán crear accesos permanentes sin respaldo, autorización o registro.

7. Modelo de roles y permisos

Digevo Ventures deberá operar bajo un esquema de accesos basado en roles, perfiles y niveles de autorización, evitando asignaciones arbitrarias o excesivas.

En línea con la Política de Seguridad de la Información, los accesos deberán organizarse con jerarquías de rol y restricciones por función, distinguiendo, entre otros, perfiles equivalentes a administrador total, administrador de plataforma, administrador de base de datos, desarrollador senior, desarrollador junior, soporte y auditor. El protocolo además establece que los accesos críticos deben mantenerse especialmente restringidos y que ciertos perfiles deben tener límites máximos de titulares.

La asignación de permisos deberá considerar:

a) rol efectivo de la persona;
b) entorno al que accederá;
c) criticidad del recurso;

d) posibilidad de modificar, borrar, exportar o administrar información; y
e) riesgos asociados al acceso.

En el caso de plataformas propias de la Compañía, tales como Evolution, PowerCamp y sus sitios web asociados, la gestión de accesos deberá adaptarse al modelo operativo específico de cada solución.

En particular, PowerCamp y la plataforma Evolution operan bajo un esquema de acceso diferenciado que considera:

a) usuarios finales, que acceden a contenidos, herramientas y funcionalidades personalizadas a través de cuentas individuales;

b) mentores, facilitadores o administradores de programa, que cuentan con accesos intermedios para seguimiento, acompañamiento y revisión del progreso de los usuarios;

c) roles administrativos y técnicos, responsables de la gestión de la plataforma, configuración, soporte, monitoreo y operación tecnológica;

d) componentes automatizados y servicios de inteligencia artificial (como Darwin), que operan mediante cuentas de servicio, APIs o integraciones, sujetas a controles reforzados de credenciales, autenticación y monitoreo.

La asignación de accesos en estas plataformas deberá considerar la naturaleza del rol, el tipo de información tratada, incluyendo datos personales y datos de negocio de los emprendedores, y el nivel de criticidad del entorno.

Asimismo, deberán implementarse controles diferenciados para entornos productivos, de desarrollo y de prueba, asegurando la segregación de funciones y la protección de la información en cada uno de ellos.

Los sitios web públicos, aun cuando no cuenten con autenticación de usuarios finales, deberán considerar controles de acceso para sus componentes administrativos, infraestructura, integraciones y servicios asociados.

8. Aprobación de accesos

Los accesos deberán aprobarse conforme al siguiente criterio general:

a) accesos básicos u operativos: por el responsable del área o del sistema, con trazabilidad;
b) accesos privilegiados: por la Gerencia General, la jefatura designada o el responsable formal de seguridad o tecnología que haya sido autorizado para ello; y
c) accesos excepcionales, temporales o de alto riesgo: mediante autorización expresa y registrada.

La aprobación podrá centralizarse en la Gerencia General o en el responsable designado, pero siempre deberá quedar registro verificable del otorgamiento.

9. Accesos privilegiados

Se consideran accesos privilegiados, entre otros:

a) infraestructura cloud;
b) bases de datos de producción;
c) paneles de administración;
d) repositorios con ramas principales o despliegue a producción;
e) VPN;
f) gestores de contraseñas o bóvedas de secretos;
g) llaves maestras, certificados, DNS y secretos de aplicación; y
h) cuentas con capacidad de crear, modificar o eliminar usuarios o permisos.

Estos accesos deberán sujetarse a medidas reforzadas. La Compañía podrá utilizar cuentas genéricas, técnicas o compartidas en los siguientes casos:

a) entornos de demostración;
b) cuentas de servicio o integración;
c) accesos operativos donde no sea posible la individualización inmediata.

En estos casos, se deberán aplicar controles compensatorios, tales como:

a) limitación de privilegios;
b) uso restringido a funciones específicas;
c) control de distribución de credenciales;
d) rotación periódica;
e) migración progresiva hacia esquemas de identidad individual.

10. Gestor corporativo de credenciales

Digevo Ventures deberá utilizar un gestor corporativo de contraseñas o repositorio seguro de credenciales para almacenar, compartir y administrar accesos sensibles.

Mientras no se implemente un gestor corporativo de credenciales, el uso de credenciales compartidas deberá limitarse a casos estrictamente necesarios, debiendo cumplir condiciones mínimas de control, tales como:

a) restricción de acceso a personas autorizadas;
b) uso de canales controlados (evitando exposición pública o masiva);
c) registro del uso cuando sea posible;
d) revisión periódica.

La Compañía avanzará progresivamente hacia la implementación de un gestor corporativo de credenciales (por ejemplo, Bitwarden u otro equivalente), con el objetivo de eliminar el uso de credenciales compartidas no controladas.

11. Política de contraseñas

Toda contraseña o secreto de acceso gestionado por personas usuarias deberá cumplir estándares mínimos de robustez, considerando la criticidad del recurso.

Sin perjuicio de que los parámetros técnicos podrán definirse en anexos o estándares operativos por sistema, Digevo Ventures adoptará como mínimo los siguientes criterios:

a) longitud suficiente acorde al riesgo del acceso;
b) complejidad adecuada para accesos administrativos y productivos;
c) prohibición de reutilización insegura;
d) obligación de cambio inmediato ante sospecha de compromiso; y
e) rotación periódica en accesos críticos.

La gestión de contraseñas deberá considerar la naturaleza del sistema y el tipo de usuario, distinguiendo al menos entre:

a) Plataformas digitales con autenticación de usuarios, tales como Evolution y PowerCamp, donde el acceso se realiza mediante credenciales (usuario y contraseña), ya sea definidas por el propio usuario o provisionales entregadas por la Compañía. En estos casos, deberán aplicarse requisitos básicos de seguridad, tales como el uso de combinaciones de letras mayúsculas, minúsculas y números, así como mecanismos para el cambio de contraseña cuando corresponda;

b) sitios web públicos sin autenticación, donde no existe gestión de credenciales de usuarios finales, sin perjuicio de los controles aplicables a la administración interna del sitio; y

c) entornos internos y sistemas tecnológicos de la Compañía, tales como servicios cloud (AWS, Azure), repositorios de código (GitHub, GitLab), bases de datos y herramientas administrativas, donde deberán aplicarse controles de seguridad reforzados, incluyendo contraseñas robustas, gestión adecuada de accesos y, cuando sea posible, autenticación multifactor.

En todos los casos, se deberá promover el uso de credenciales seguras, únicas y bajo responsabilidad individual.

En caso de entrega de credenciales iniciales por parte de la Compañía, se deberá requerir su cambio en el primer inicio de sesión cuando la plataforma lo permita

En el caso de credenciales compartidas o cuentas técnicas, éstas deberán:

a) utilizar contraseñas robustas y únicas;
b) almacenarse preferentemente en un repositorio seguro;
c) evitar su difusión en canales abiertos como Slack, correo o documentos no protegidos;
d) ser rotadas periódicamente o cuando exista sospecha de exposición.

En el caso de las plataformas propias de la Compañía tales como “Evolution” o “Powercamp”, deberán definirse estándares específicos de contraseñas según el tipo de usuario y la criticidad del acceso.

En particular:

a) los usuarios finales, deberán cumplir requisitos adecuados de seguridad equilibrando protección y usabilidad,
b) los roles administrativos, técnicos o de gestión de plataformas deberán cumplir requisitos reforzados de longitud y complejidad,
c) las cuentas de servicio, APIs, integraciones y componentes automatizados. incluyendo funcionalidades basadas en inteligencia artificial como Darwin, deberán utilizar credenciales robustas, aleatorias y gestionadas mediante mecanismos seguros; y
d) deberán establecerse medidas diferenciadas para entornos productivos, de desarrollo y prueba.

De hecho, se establecen requisitos de contraseñas orientados a asegurar un nivel adecuado de seguridad, incluyendo el uso de combinaciones de letras mayúsculas, minúsculas, números y, cuando corresponda, caracteres especiales.

Asimismo, se promueve el uso de contraseñas robustas y únicas, evitando su reutilización en múltiples servicios.

Sin perjuicio de lo anterior, la Compañía podrá definir estándares más exigentes para accesos críticos o administrativos, en la medida en que evolucionen sus capacidades tecnológicas y de seguridad.

Estos criterios deberán considerarse como referencia para otras plataformas cuando resulte aplicable.

12. Autenticación multifactor (MFA)

Digevo Ventures promoverá la implementación progresiva de mecanismos de autenticación multifactor (MFA), especialmente en los accesos a sistemas internos y entornos tecnológicos críticos.

En particular, se priorizará su adopción en:

a) servicios cloud (por ejemplo, Azure, AWS u otros);
b) repositorios de código (como GitHub, GitLab u otros);

c) accesos a bases de datos y entornos productivos; y
d) plataformas o herramientas con privilegios administrativos.

Actualmente, algunos accesos pueden gestionarse mediante credenciales compartidas o mecanismos heredados. En estos casos, la Compañía deberá avanzar en su formalización, fortalecimiento y control, promoviendo la asignación de accesos individuales y la incorporación de MFA cuando las herramientas lo permitan.

En el caso de plataformas orientadas a usuarios externos, tales como Evolution y PowerCamp, o sitios web, la implementación de MFA dependerá de las capacidades de la solución y de la evaluación entre seguridad y experiencia de usuario, no siendo obligatoria en todos los casos.

La adopción de MFA se realizará de manera gradual, en línea con la madurez tecnológica de la organización y como parte de su proceso de mejora continua en seguridad de la información.

13. Altas de acceso

Toda alta de acceso deberá realizarse una vez verificados:

a) identidad de la persona;
b) vínculo vigente con Digevo Ventures;
c) necesidad concreta del acceso;
d) perfil o rol aplicable; y
e) aprobación correspondiente.

La activación deberá registrarse indicando, al menos:

a) nombre del titular;
b) sistema o recurso;
c) rol asignado;
d) fecha de alta;
e) aprobador; y
f) fecha de expiración o revisión, cuando corresponda,
g) clasificación del tipo de acceso.

14. Modificación de accesos

Todo cambio de funciones, proyecto, rol, criticidad o relación contractual deberá gatillar una revisión y ajuste de permisos.

Cuando una persona cambie de funciones:

a) se deberán revocar los accesos que ya no correspondan;
b) solo podrán mantenerse los estrictamente necesarios; y
c) no se deberán acumular privilegios históricos por cambios de puesto.

En la medida en que la Compañía cuente con mecanismos formales de gestión de accesos

15. Accesos temporales y excepcionales

Los accesos temporales, de contingencia o excepcionales deberán:

a) otorgarse por plazo acotado;
b) quedar expresamente justificados;
c) ser aprobados por la instancia competente;
d) quedar registrados; y
e) ser revocados una vez cumplida su finalidad.

No se deberán convertir accesos excepcionales en permanentes por omisión o inercia operativa.

16. Recuperación de acceso y pérdida de contraseña

Cuando una persona usuaria pierda su acceso o requiera recuperación de contraseña, deberá seguirse un procedimiento controlado de verificación de identidad y restablecimiento seguro.

En plataformas como Evolution o PowerCamp, los mecanismos de recuperación de acceso dependerán de las funcionalidades disponibles, debiendo promoverse prácticas seguras como la verificación básica de identidad y el cambio de contraseña posterior.

17. Sospecha de compromiso de credenciales

En caso de incidentes de seguridad o contingencias operativas, la Compañía podrá adoptar medidas extraordinarias de control de accesos, incluyendo restricciones generales, bloqueo de sistemas o reasignación de privilegios, con el objeto de resguardar la continuidad operacional.

Ante sospecha de compromiso de credenciales, la Compañía deberá adoptar medidas razonables, tales como:

a) bloqueo o cambio de credenciales;
b) revisión básica de actividad reciente;
c) actualización de accesos relacionados; y
d) documentación del incidente cuando corresponda.

Estas acciones se ejecutarán progresivamente en función de la capacidad operativa.

18. Baja de accesos y offboarding

Toda terminación de relación laboral, contractual o funcional deberá activar un proceso de revocación de accesos.

Como regla general:

a) en el menor plazo posible desde el término, deberán desactivarse correo, cuentas corporativas, accesos a plataformas, Slack, VPN y demás sistemas relevantes;
b) deberán revocarse o actualizar, cuando corresponda, tokens, claves API, accesos técnicos y secretos asociados;
c) las contraseñas compartidas a las que la persona tenía acceso deberán ser evaluadas para su cambio, según el nivel de criticidad del acceso; y
d) deberá mantenerse trazabilidad básica del proceso de baja, en la medida de lo posible.

En el caso de plataformas operadas por la Compañía, tales como Evolution y PowerCamp, la gestión de bajas de acceso se realizará en función de las capacidades de cada sistema.

En particular, se deberá procurar:

a) la desactivación, bloqueo o eliminación de cuentas de usuarios cuando corresponda por motivos de seguridad, inactividad, solicitud del usuario o decisiones operativas de la Compañía, y no necesariamente por la finalización de su participación en un curso o programa;
b) la revocación o ajuste de accesos administrativos, técnicos o de soporte asociados a la operación de la plataforma;
c) la revisión de accesos a componentes críticos, tales como bases de datos, servicios cloud o repositorios vinculados; y
d) la adopción de medidas razonables para resguardar la seguridad de la información, considerando la naturaleza del servicio y los datos tratados.

La implementación de estas medidas dependerá del diseño y funcionalidades de cada plataforma, así como de la capacidad operativa de la Compañía.

19. Revisión periódica de accesos

Digevo Ventures deberá revisar periódicamente los accesos vigentes, especialmente respecto de:

a) usuarios administrativos;
b) accesos a producción;
c) bases de datos;
d) VPN;
e) servicios cloud;
f) terceros con acceso activo; y

g) cuentas sin uso reciente o innecesarias,
h) accesos a plataformas (roles administrativos en Evolution y Power Campus).

Estas revisiones deberán realizarse al menos trimestralmente para accesos críticos o con la frecuencia que determine el estándar operativo aplicable. El protocolo de Evolution contempla revisiones periódicas de accesos activos como parte del esquema de cumplimiento y auditoría.

20. Cuentas compartidas y cuentas de servicio

Digevo Ventures deberá minimizar el uso de cuentas compartidas.

Las cuentas compartidas solo podrán existir cuando:

a) sean técnicamente inevitables;
b) estén bajo control de un repositorio seguro;
c) tengan responsables asignados;
d) su uso quede trazable; y
e) sus secretos sean rotados periódicamente o ante cambios de personal,
f) en plataformas, evitar cuentas administrativas genéricas.

Las cuentas de servicio, integraciones y APIs deberán usar credenciales aleatorias, robustas y administradas bajo controles reforzados.

21. Activos públicos sin autenticación

Los activos públicos de la Compañía, como el sitio web institucional, no requieren autenticación de usuarios finales.

No obstante, deberán aplicarse controles sobre:

a) accesos administrativos al CMS o backend;
b) credenciales de hosting, dominio y despliegue;
c) repositorios de código asociados;
d) integraciones externas (formularios, APIs, analítica, etc.).

Estos accesos deberán gestionarse conforme a esta Política, especialmente en lo relativo a cuentas privilegiadas y credenciales técnicas.

22. Registro y trazabilidad

Toda asignación, cambio, suspensión, revocación o incidente relevante de acceso deberá quedar registrado.

Los logs, registros o evidencias deberán permitir reconstruir:

a) quién solicitó el acceso;
b) quién lo aprobó;
c) qué acceso fue otorgado o retirado;
d) desde cuándo;
e) en qué sistema; y
f) qué acciones relevantes ocurrieron sobre recursos críticos.

23. Responsabilidades

23.1 Gerencia General

Corresponde a la Gerencia General:

a) aprobar esta Política y sus actualizaciones;
b) velar por su implementación general;
c) aprobar o designar la aprobación de accesos privilegiados; y
d) resolver excepciones de alto riesgo.

23.2 Responsable de seguridad, tecnología o administración de sistemas

Corresponde a la función responsable:

a) ejecutar el otorgamiento y revocación de accesos;
b) mantener actualizado el registro de permisos críticos;
c) administrar MFA, bóvedas y controles técnicos;
d) revisar accesos activos; y
e) coordinar la respuesta ante incidentes de credenciales.

23.3 Jefaturas o responsables de área

Corresponde a las jefaturas:

a) solicitar accesos solo cuando exista necesidad real;
b) validar cambios de rol o salidas; y
c) informar oportunamente altas, modificaciones y bajas.

23.4 Usuarios y terceros autorizados

Toda persona con acceso deberá:

a) usar únicamente sus credenciales personales o autorizadas;
b) resguardar contraseñas y factores MFA;
c) no compartir claves por canales inseguros;
d) reportar pérdida, sospecha de compromiso o uso indebido; y
e) cumplir esta Política y los procedimientos complementarios.

El acceso a sistemas y credenciales implica el deber de confidencialidad respecto de la información a la que se tenga acceso, obligación que subsistirá incluso después del término de la relación con la Compañía

24. Prohibiciones

Se prohíbe expresamente:

a) compartir contraseñas o códigos MFA por medios informales;
b) utilizar cuentas de otro usuario;
c) mantener accesos innecesarios o heredados;
d) otorgar privilegios sin autorización;
e) almacenar secretos en documentos abiertos o chats;
f) conservar accesos de excolaboradores;
g) usar cuentas compartidas sin control; y
h) omitir el reporte de pérdida o sospecha de compromiso de credenciales.

25. Incumplimientos

El incumplimiento de esta Política podrá dar lugar a la adopción de medidas administrativas, contractuales, disciplinarias o legales, según la naturaleza del vínculo con Digevo Ventures y la gravedad de los hechos.

En el caso de trabajadores de la Compañía, dichas infracciones podrán ser calificadas como incumplimientos graves de las obligaciones que impone el contrato de trabajo.

Respecto de terceros, el incumplimiento podrá constituir una infracción contractual grave, habilitando a la Compañía para ejercer las acciones y remedios que correspondan conforme al respectivo contrato y la legislación vigente

26. Revisión y actualización

La presente Política deberá revisarse al menos una vez al año y, adicionalmente, cada vez que:

a) se incorporen nuevos sistemas críticos;
b) exista un incidente relevante;
c) cambien las estructuras de roles o plataformas;
d) se detecten brechas de control; o
e) cambie la normativa o el marco corporativo aplicable.

27. Vigencia

La presente Política entrará en vigencia desde su aprobación formal por la Gerencia General de Digevo Ventures SpA.

DIGEVO VENTURES

GERENTE GENERAL
DIGEVO VENTURES

Santiago, 02 de Enero de 2026.