a3sec

‹BLINDAMOS ACTIVOS DIGITALES GLOBALMENTE›

POLÍTICA GENERAL DE PRIVACIDAD Y PROTECCIÓN DE DATOS

‹ ESPAÑA / MÉXICO / COLOMBIA /ECUADOR›

Contenido

1. INFORMACIÓN GENERAL

- **Responsable del tratamiento:** Grupo A3sec
- **Dirección:** Cl. 98 #70-91, Bogotá D.C, Colombia / C. de Aravaca, 6, Moncloa - Aravaca, 28040 Madrid, España
- **NIT**: 9007804612 **CIF:**B86560950
- **Correo electrónico:** dataprotection@a3sec.com

2. USUARIOS

El acceso y/o uso de este sitio web del Grupo A3sec atribuye la condición de usuario, que acepta, desde dicho acceso y/o uso, las condiciones generales reflejadas en este documento, Estas disposiciones se aplican a todos los usuarios del sitio, independientemente de otro acuerdo específico que pueda existir en relación de contratación de servicios o procesos de empleabilidad de funcionarios, proveedores o contratistas.

3. USO DEL PORTAL

https://a3sec.com/ proporciona el acceso a información, servicios, contenidos de internet pertenecientes al Grupo A3sec o sus licenciantes y usuarios que puedan tener acceso. El usuario asume la responsabilidad del uso del portal, Esta responsabilidad se extiende al registro que fuese necesario a determinados servicios y contenidos.

4. POLÍTICA DE PRIVACIDAD

4.1. OBJETO

El objeto del presente documento es:

- Establecer la "**Política General de Privacidad y Protección de datos"** en adelante la política, con el fin de detallar cómo se recogen, utilizan, almacenan y protegen los datos personales de los usuarios de acuerdo con las leyes vigentes.

- Identificar los datos de carácter personal en adelante "***DCP"*** tratados por el Grupo A3sec, tanto como Responsable del tratamiento como Encargado de Tratamiento para terceros, y los tratamientos realizados.

- Recoger las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente para la protección de datos de carácter personal bajo la responsabilidad del Grupo A3sec.

- Establecer los procesos de actualización y el sistema de controles del cumplimiento de esta Política General y de la normativa aplicable.

Este documento es de lectura obligatoria para todas las partes interesadas. El Grupo A3sec determinará aquellos apartados que se pondrán a disposición de cualquier tercero que acceda a datos tratados bajo la responsabilidad de la Organización.

Las definiciones utilizadas en este documento se encuentran en el apartado 4.4.

4.2. ÁMBITO DE APLICACIÓN

- Este documento será aplicado, con el fin de brindar trámite de manera expedida y conforme a las leyes regulatorias en materia de protección de datos, dando a conocer la responsabilidad demostrada por el **Grupo A3sec** a los derechos de los titulares de la información.

- **Todos los DCP tratados por el Grupo A3sec,** tanto como Responsable del Tratamiento y como Encargado del Tratamiento.

- **Todas las personas que intervienen en el tratamiento**, tanto personal del Grupo A3sec, como personas terceras trabajando dentro del mencionado ámbito material (el "**Personal**").

- **Los datos personales** proporcionados por las diferentes partes.

- **Todos recursos automatizados y soportes no automatizados que contienen y/o tratan datos de carácter personal** que se hallan bajo la responsabilidad del **Grupo A3sec,** incluyendo los sistemas de información, soportes y equipos

empleados, clientes, proveedores o cualquier parte interesada para su tratamiento.

Se incluyen dentro del ámbito material:

- Los **centros de tratamiento y locales** donde se encuentren ubicados los ficheros y se almacenen los soportes que los contengan.
- Los **archivos y los equipos servidores** donde se ubican los Ficheros, así como el entorno (despachos, armarios, software, hardware) de los mismos.
- Los **puestos de trabajo**, bien locales o remotos, desde los que se puede tener acceso a los ficheros.
- Los **sistemas de información y aplicaciones** utilizados para el acceso a los ficheros y tratamiento de los datos.

4.3. ACTUALIZACIÓN

El presente documento se mantendrá en todo momento actualizado y será revisado siempre que:

- Se produzcan cambios relevantes en los tratamientos de DCP y/o los sistemas de información que contienen o tratan DCP;
- Existan cambios en el Grupo A3sec, que afecten a los procedimientos y medidas recogidos en este documento;
- Se modifiquen las disposiciones vigentes en materia de seguridad de los datos de carácter personal.
- El **Delegado de datos personales** mantendrá permanentemente actualizada toda la información y documentación incluida en esta política.

4.4. DEFINICIONES

A todos efectos del presente documento se entienden por:

- **Datos de carácter personal (DCP)**: toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
- **Encargado de Tratamiento o encargado**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del Responsable de Tratamiento.
- **Interesado**: es la persona física identificada o identificable.
- **Responsable de Tratamiento o responsable**: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.
- **Tratamiento**: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- **Violación de la seguridad de los datos personales**: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

4.5. TRATAMIENTO DE DATOS

4.5.1. Inventario y registro de tratamientos

Los Anexos de la sección 8 contienen:

- 8.1 el Inventario de Datos
- 8.2 el Inventario de Sistemas
- 8.3 el Registro de Actividades de Tratamiento
- 8.4 Registro de Terceros Encargados
- 8.5 Registro de Transferencias internacionales de datos

Estos Anexos se actualizarán cada vez que haya un cambio en el tratamiento de DCP del Grupo A3sec

Los datos personales recogidos serán tratados para las siguientes finalidades específicas:

Prestación de Servicios:

- Para la gestión, administración, prestación, ampliación y mejora de nuestros servicios de monitoreo de ciberseguridad, garantizando que su uso solo se encuentra autorizado para los fines del contrato de prestación de servicios contribuyendo a la seguridad e integridad de sus redes y sistemas informáticos.
- Suministrar información a terceros con los cuales el Grupo A3sec tenga relación contractual y sea necesario entregarla para el cumplimiento del objeto contratado.
- Transferir o transmitir datos personales para cumplir con las regulaciones antilavado de activos que se le aplican.
- Transmitir datos personales a terceros con los cuales el Grupo A3sec tenga un vínculo contractual o haya suscrito un contrato de procesamiento de datos y sea necesario entregarla para dar cumplimiento a los servicios prestados al cliente y el brindar cumplimiento del objeto contractual.
- Efectuar las gestiones pertinentes para el desarrollo del objeto social en lo que tiene que ver con el objeto contratado celebrado con el titular de la información.

Gestión de la Relación Comercial:

- Para mantener y gestionar la relación contractual con nuestros clientes, incluyendo la gestión de pagos, facturación y cobros.
- Contactar al titular autorizado vía correo electrónico para envío de facturación o movimientos de cuenta en relación con obligaciones derivadas de la relación entre las partes.
- Realizar contacto vía correo electrónico con el titular de los datos para generar envíos de material comercial, así como todo lo que cubra procesos de licitación y de servicios contratados por el Grupo A3sec.
- Brindar respuesta a consultas, quejas y comentarios.

Marketing y Publicidad:

- Para enviar comunicaciones comerciales y promocionales, en los casos en que se haya consentido expresamente.
- Realizar invitaciones a eventos y ofrecer productos y servicios.
- Efectuar encuestas de satisfacción a clientes con los cuales se tenga relación de manera contractual.
- Contactar al titular autorizado para envío de noticias por campañas y fidelización.

Seguridad:

- Para mantener la seguridad de nuestras instalaciones, sistemas y datos.

Datos personales de empleados:

- El Grupo A3Sec tiene un interés legítimo en tratar los datos personales de nuestro personal, (en adelante, "Miembro del personal"). Sin embargo, Incluso si no es estrictamente necesario, al dar acuse de recibo de este documento, el empleado autoriza a recopilar y tratar los datos personales durante el empleo o contratación en la manera que se establece a continuación y según se indica en el contrato formalizado.
- Establecer, gestionar y mantener la relación contractual, incluido el pago de tu remuneración a través de instituciones financieras e interactuar con las agencias tributarias y oficinas de seguridad social, sindicatos, mutualidades y entidades de seguros.
- Llevar a cabo, en su caso, un control del tiempo y acceso a las instalaciones (video-vigilancia).
- Evaluar la aptitud para el trabajo o tarea, con el fin de ofrecer servicios de capacitación y transición profesional, así como para gestionar contratos y tareas, y para los procesos de selección, evaluación y mejora profesional.
- Informar sobre los productos y servicios y los esquemas de pago y/o incentivos
- Para controlar el uso de nuestros sistemas de información (incluyendo computadoras, servidores, PC y dispositivos móviles como tabletas, laptops y teléfonos propiedad del Grupo A3sec. móviles) y, en las condiciones establecidas por la ley, tus comunicaciones por correo electrónico, para verificar el cumplimiento de tus obligaciones y deberes

en el marco de tu relación y tus funciones laborales dentro de Grupo A3Sec, así como también

- Para la prevención y / o investigación de fraudes y otros crímenes o agravios.
- Gestionar y defender cualquier reclamación y acción legal, para cumplir con órdenes judiciales y otras obligaciones legales y requisitos reglamentarios, Para todos los demás fines autorizados por la ley.
- Grupo A3Sec recopila, trata y divulga tus datos personales confidenciales solo cuando es necesario para cumplir con las obligaciones impuestas por la ley o si existe un motivo imperativo comercial para hacerlo según lo permitido por la ley aplicable o con el consentimiento del miembro del personal. tus datos personales serán almacenados por Grupo A3Sec durante toda la vigencia de nuestro contrato contigo y, posteriormente, bloqueados, por el período prescrito por la ley para atender a cualesquiera responsabilidades o razones legales o administrativas (generalmente 6 años)
- Para llevar a cabo nuestro negocio, tus datos serán tratados y comunicados a las siguientes entidades (limitando dichos datos a lo que es necesario para realizar el contrato de estas entidades con Grupo A3Sec y, en tu caso, por la razón legal

Proveedores:

- Revisión de Comportamiento: Analizar el comportamiento del archivo malicioso (acciones realizadas, conexiones establecidas).
- Negociar y ejecutar los contratos o cualquier otro negocio jurídico que surja entre el Grupo A3Sec y el proveedor.
- Hacer estudios de seguridad relacionados con el proveedor persona natural.
- Verificar los datos de los representantes legales de los proveedores persona jurídica.
- Verificar la idoneidad de los proveedores personas naturales y de los empleados de los proveedores
- personas jurídicas en virtud de la ejecución del contrato.
- Para la determinación de obligaciones pendientes, la consulta de información financiera e historia crediticia y el reporte a centrales de información de obligaciones incumplidas, respecto de sus deudores.

4.5.2. Cumplimiento Legal

Para cumplir con nuestras obligaciones legales y regulatorias, tales como obligaciones fiscales, contables y de archivo:

- El Grupo A3sec podrá llevar a cabo, el tratamiento de información personal acerca de sus clientes, con el fin de prestar los servicios contratados y demás actividades relacionadas con su objeto social, los contratos celebrados con clientes se regirán por lo dispuesto en la presente política y la ley del país de origen del cliente.

- El Grupo A3sec asume que la información personal de terceros, cuyo responsable sea el Cliente y que reconozca al Grupo A3sec en razón o con ocasión del contrato celebrado ha sido tratada con a lo dispuesto a ley del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) de España, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México, la Ley Orgánica de Protección de Datos Personales de Ecuador y la Ley Estatutaria 1581 de 2012 de Protección de Datos de para Colombia, y demás normativa vigente en cada momento.

4.6. MEDIDAS DE SEGURIDAD

Implementamos una serie de medidas técnicas y organizativas para proteger los datos personales contra el acceso no autorizado, la pérdida, alteración, divulgación o destrucción. Esto incluye:

- **Cifrado de Datos**: Control aplicado a datos tanto en tránsito como en reposo.
- **Controles de Acceso:** Restricciones de acceso a los datos personales solo a personal autorizado.
- **Auditorías Periódicas:** Evaluaciones y auditorías periódicas de nuestras prácticas de seguridad y protección de datos.
- **Formación:** Programas de formación continua para nuestros empleados en materia de protección de datos y seguridad.

-

4.7. DERECHOS DE LOS TITULARES DE DATOS

Los usuarios tienen derechos específicos en relación con sus datos personales, conforme a la normativa aplicable. Estos derechos incluyen:

- **Derecho de Acceso:** Obtener confirmación de si estamos tratando sus datos personales y, en tal caso, acceder a los mismos.
- **Derecho de Rectificación:** Solicitar la corrección de datos inexactos o incompletos.
- **Derecho de Supresión (Derecho al Olvido**): Solicitar la eliminación de sus datos personales cuando ya no sean necesarios para los fines para los que fueron recogidos.
- **Derecho a la Limitación del Tratamiento:** Solicitar la limitación del tratamiento de sus datos personales en determinadas circunstancias.
- **Derecho a la Portabilidad de los Datos:** Recibir sus datos personales en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable del tratamiento.
- **Derecho de Oposición:** Oponerse al tratamiento de sus datos personales en determinadas circunstancias, como en el caso de marketing directo.

Para ejercer estos derechos, puede ponerse en contacto con nosotros a través del correo electrónico [Correo Electrónico de Contacto].

4.8. TRANSFERENCIAS INTERNACIONALES

En caso de que sea necesario transferir datos personales fuera del Espacio Económico del país de origen con normativa equivalente, nos aseguraremos de que dichas transferencias se realicen cumpliendo con las garantías adecuadas, tales como cláusulas contractuales tipo aprobadas por la Comisión Europea o mecanismos equivalentes.

4.9. PLAZAS DE CONSERVACIÓN

Los datos personales se conservarán únicamente durante el tiempo necesario para cumplir con los fines para los cuales fueron recabados y conforme a los plazos legales de retención de datos. Posteriormente, los datos serán eliminados de manera segura,

salvo que deban mantenerse para cumplir con una obligación legal o para el ejercicio o defensa de reclamaciones.

4.10. ANÁLISIS DE RIESGOS

El Anexo 6.1 contiene un análisis de riesgos relativos al tratamiento de DCP de la Empresa.

El **Comité de Seguimiento de la Privacidad** (**"CSP")** monitorizará e informará al Responsable de Privacidad la aplicación de las medidas de control establecidas y el Análisis de Riesgos.

4.11. ACTUALIZACIÓN

Estos Anexos serán revisados y controlados en el seno del Comité de Seguimiento establecido.

4.12. ORGANIZACIÓN DE LA PRIVACIDAD

4.12.1 Roles y Gobernanza

Grupo A3Sec, designa el Delegado de datos personales con las siguientes funciones:

- Revisar y realizar propuestas de cambios para esta PGP
- Supervisar el cumplimiento de la normativa de protección de datos personales.
- Identificar cambios en la normativa de datos personales y comunicarlas al comité de seguridad y privacidad.
- Coordinar la respuesta ante posibles violaciones de datos personales.
- Actuar como punto de contacto con las autoridades de protección de datos.
- Sugerir controles de protección de datos en proyectos o procesos que impliquen alto riesgo.
- Difundir y socializar concienciación sobre protección de datos personales.
- Mantener la Política General de Protección de datos revisada, actualizada y aprobada por el Comité de Seguridad y Privacidad.
- Atender los lineamientos y requerimientos que tenga a su cargo de Protección de Datos Personales.
- Ser el punto de contacto para solicitudes internas y externas sobre privacidad en la organización.

Se establece un **Comité de Seguridad y Privacidad** como responsable del tratamiento, el cual se encuentra compuesto por la Dirección de España, Colombia y México del Grupo A3sec como participantes se encuentra el Delegado de datos personales.

El Comité tiene como funciones:

- Revisar la aplicación de esta PGP periódicamente, aplicando los puntos de control establecidos en el Apartado 6.5.
- Revisar y realizar propuestas de cambios para esta PGP
- Establecer los propósitos para los cuales, se recogen y procesan los datos personales, así como los métodos y procesos utilizados para mantener su protección de datos.
- Asegurar el cumplimiento de la responsabilidad legal y las obligaciones normativas vigentes.
-

Se establecen como **Encargados del Tratamiento** de **DCP** de cada área de la Empresa y clientes a los colaboradores que por su competencia y funciones procesan o administran de cualquier forma **DCP**. los cuales son designados en el *manual de funciones.*

El Encargado de Tratamiento tiene como funciones:

- Garantizar la custodia de la aceptación de uso y almacenamiento de datos personales en procesos digitales y físicos.
- Procesar los datos personales conforme a lo establecido por el Grupo A3sec y respetando las directrices de los clientes.
- implementar las medidas técnicas y organizativas necesarias para garantizar un nivel de protección adecuado
- Asegurar que los datos personales cumplan procesos de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad.
- Comunicar y asistir al Delegado de Datos Personales en respuesta de solicitudes si así es requerido.

Asegurar el cumplimiento de la normativa de protección de datos en las plataformas técnicas.

4.13. PROTOCOLOS

Se establecen los siguientes protocolos internos a los efectos de garantizar el cumplimiento de la normativa de protección de DCP (indicados en el Anexo 7):

Protocolo	Documento	Objetivo
Incidencias	Protocolo Incidencias	Documentar las incidencias de datos personales y, en su caso, notificar al Responsable de tratamiento/interesados/autoridad de control
Ejercicio de Derechos ARCOPOL	Protocolo Arcopol	Responder a ejercicio de derechos de interesados
Nuevos tratamientos DCP	Protocolo Nueva Actividad de Tratamiento	Llevar a cabo una Evaluación de Impacto relativa a la Protección de Datos, en caso de riesgo a los derechos y libertades de los interesados.
Altas y Bajas de empleados y proveedores	Protocolo altas/bajas de empleados y staff	Asegurar la confidencialidad y formación de los empleados.
Altas y Bajas de proveedores	Cuestionario de proveedores y lista de verificación de seguridad.	Diligencia en la verificación de la calidad de los procesadores de datos.
Altas y bajas de clientes	Protocolo altas/bajas de clientes	Asegurar la confidencialidad y formación de los clientes

Los protocolos están incluidos en esta PGP en la Sección 7 (Protocolos)

4.14 . OBLIGACIONES DEL PERSONAL- FORMACIÓN

Se hará una efectiva gestión de los DCP bajo la responsabilidad del Grupo A3sec:

- Las personas a las que se aplica este documento de seguridad con acceso a y uso de DCP cumplirá los deberes establecidos en **Obligaciones del Personal.**
- El **Responsable de Seguridad** ha establecido mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos diferentes a los autorizados.
- La necesidad de creación de nuevos ficheros con datos de carácter personal y la modificación o baja de los presentes en el inventario de ficheros, será comunicado al **Responsable de Seguridad.**
- Exclusivamente el personal autorizado podrá conceder, alterar o anular el acceso autorizado sobre los datos y los recursos, con la conformidad de los criterios establecidos por el **Responsable de Seguridad**.

Todo el Personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo. Deben firmar la Política de Confidencialidad para Empleados.

Constituye una obligación del Personal notificar al **Responsable de Seguridad** las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este documento.

Para asegurar que todo el Personal conoce las normas de seguridad que afectan a la Empresa desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, dispone de los siguientes documentos del conocimiento de esta *política*, y sus anexos.

El Personal ha sido informado de sus obligaciones y funciones de acuerdo con siguiente procedimiento:

- Cada persona ha firmado un compromiso de confidencialidad, ya sea en su contrato laboral o en el contrato de servicios.
- Cada persona puede acceder directamente a esta Política General de Privacidad en el repositorio documental del Grupo A3Sec, implementado en Google Drive, Sección OFICINA GENERAL, Subsección GDPR.

- Cada persona ha recibido sesiones formativas sobre las obligaciones y funciones ante los datos de carácter personal (coordinadas por el Responsable de Seguridad, junto con el departamento de Talento Humano).

Cualquier persona que infrinja esta normativa será sujeto a la disciplina laboral, considerándose un incumplimiento laboral (en función de la casuística como una falta leve, grave o muy grave).

4.15. GESTIÓN DE INCIDENCIAS

Definición de Incidencia:
Se considera "incidencia de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este PGP, y en particular las Normas de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal.

Con el objeto de dar debido cumplimiento a lo establecido, la Empresa dispone este procedimiento de notificación, gestión y respuesta de las incidencias.

El Anexo 7.1 contiene el protocolo de Incidencias

a) Tipo de Incidencias que se deben notificar

A continuación, se presenta una lista de incidencias que serán inexcusablemente registradas. Esta lista podrá ser ampliada con otro tipo de incidencias que pudieran haber quedado omitidas:

1. **Incidencias que afecten a la identificación y autenticación de los usuarios:**
   - Pérdida de confidencialidad de contraseñas.
   - Detección de accesos irregulares (intentos fallidos de accesos, accesos fuera de horas de oficina, etc.) tras la revisión de "logs".
   - Períodos de desactivación de las herramientas de seguridad.
   - Comunicación de los usuarios de sospechas de que alguien ha suplantado su identidad.

2. **Incidencias que afecten a los derechos de acceso a los datos:**
   - Solicitudes de modificación de derechos de acceso sobre datos.
   - Solicitudes de modificación de derechos de acceso sobre herramientas de gestión de acceso y utilidades con accesos privilegiados.

3. **Incidencias que afecten a la gestión de soportes.**
   - Comunicación de pérdida de soportes.
   - Comunicación de localización de soportes en lugares inadecuados.
   - Errores de contenido en soportes recibidos y enviados.

4. **Incidencias que afecten a los procedimientos de copias de salvaguarda y recuperación:**
   - Errores detectados en los procesos de realización de copias de salvaguarda.
   - Procedimientos de recuperación de datos realizados.

5. **Incidencias que afecten a ficheros no automatizados (en papel)**
   - Soportes o documentos con datos hallados fuera de la Entidad sin custodia.
   - Detección de copias no autorizadas de datos del Fichero.

6. **Incidencias que afecten al cumplimiento de las normas de seguridad establecidas:**
   - Cualquier incumplimiento de las medidas de seguridad y protección de datos personales.

7. Cualquier otra incidencia de las observadas como consecuencia de la ejecución de los controles definidos para garantizar el cumplimiento de lo dispuesto en el Documento de Seguridad (auditorías bienales, revisiones mensuales, etc).

b) Procedimiento de Notificación de Incidencias

Cualquier persona que forme parte de la plantilla de la Empresa o se halle prestando sus servicios en la misma (aún cuando sea de forma temporal) deberá notificar inmediatamente, al Responsable de Seguridad, cualquier incidencia que detecte y que afecte o pueda afectar a la seguridad de los datos y recursos protegidos.

La notificación se hará a través de cualquier medio que asegure la confidencialidad de la incidencia, conforme el protocolo en Anexo 7.1.

El retraso en la notificación de incidencias constituirá un quebranto de la buena fe contractual, sancionable según la normativa laboral aplicable.

c) Registro de Incidencias

El Responsable de Seguridad, de conformidad con el RGPD, artículo 33 n. 5, mantiene un registro en formato electrónico de las incidencias.

En el Anexo 7.1 se adjunta el modelo de formato que el Responsable de Seguridad utilizará para el registro de incidencias. Dichos registros serán almacenados, por el Responsable de Seguridad, a efectos históricos durante el tiempo requerido para cumplir obligaciones legales y de auditoría (al menos 5 años).

d) Respuesta a Incidencias

El Responsable de Seguridad gestionará las incidencias de seguridad que pudieran producirse, debiendo iniciar su resolución en un plazo inferior a 10 días desde la notificación.

El Responsable de Seguridad supervisará el trabajo de subsanación de la anomalía detectada y anotará en el registro de la incidencia todas las acciones y medidas tomadas para resolver o minimizar dicha incidencia.

A efectos de control, se incluye en el propio registro de la incidencia la información que permite verificar el cumplimiento del tiempo de respuesta ante incidencias.

4.16 CONTROL PERIÓDICOS Y AUDITORÍAS

a) Controles periódicos para verificar cumplimiento de normas

El **Responsable de Seguridad** realizará los controles periódicos indicados en el Anexo 6 de está política.

b) Auditorías

De forma periódica, cuando se considere necesario y apropiado, se realizará una auditoría de los sistemas de información y del personal objeto del alcance del documento de Seguridad para los ficheros que requieren la implementación

de medidas de nivel medio. La auditoría podrá ser interna o externa, según se considere oportuno en el momento de su realización.

También será necesaria la realización de una auditoría cuando se produzcan modificaciones sustanciales en los sistemas de información y organizativos con repercusión en la seguridad de los datos protegidos.

El objeto de la auditoría será medir el grado de cumplimiento de las medidas de seguridad establecidas por la Normativa de Datos y de los procedimientos, instrucciones y políticas desarrolladas en las Normas de Seguridad.

El Responsable de Seguridad analizará el informe de auditoría y elevará las conclusiones obtenidas, junto con propuestas de mejora, al Responsable del Fichero para que adopte las medidas correctoras adecuadas.

El informe de auditoría será custodiado por el Responsable de Seguridad, por si fuera requerido por la Agencia de Protección de Datos.

Todo el personal de la Empresa y los proveedores de servicios externos que tengan acceso a los datos personales deberán prestar en todo momento su colaboración para llevar a cabo los controles necesarios y su correspondiente auditoría a requerimiento del Responsable de Seguridad.

4.17 CUMPLIMIENTO DE PRINCIPIOS FUNDAMENTALES

4.17.1 Legitimación y Finalidades

Definición de legitimación

Se considera "tratamiento lícito o legal" un tratamiento llevado a cabo sobre la base del consentimiento del Interesado, o si es necesario para la ejecución de un contrato del que el interesado es parte, por el cumplimiento de una obligación legal, para proteger el interés vital del interesado u otra persona física, para la realización de una tarea llevada a cabo en interés público o en ejercicio de la autoridad oficial, o si el procesamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

Los DCP solamente se tratarán para finalidades legítimas del Grupo A3Sec y con el consentimiento informado de los interesados.

El Registro de Actividades de Tratamiento indica la legitimación y el consentimiento prestado de cada tratamiento de DCP realizada por la Empresa.

El Delegado de datos personales controlará la legitimidad de cada tratamiento de DCP.

La Empresa mantendrá un sistema de información adecuado para poder asociar cada tratamiento de DCP con un consentimiento informado del interesado.

La legitimación actual se establece a continuación:

Categoría Interesados (RAT)	Legitimación
Empleados	Ejecución de contrato, interés legítimo
Solicitantes, personas que facilitan el CV a la empresa	Consentimiento
Interlocutores/contacto de proveedores	Ejecución de contrato, interés legítimo
Interlocutores usuarios registrados	Ejecución de contrato, interés legítimo
Interlocutores/contacto de clientes	Ejecución de contrato, interés legítimo
Interlocutores/contacto de clientes potenciales	Ejecución de contrato, interés legítimo

4.18 TRATAMIENTOS SENSIBLES

Definición de datos sensibles: Se consideran "datos sensibles" cualquier información personal que revelen origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o afiliación sindical, o datos genéticos, datos biométricos, datos relacionados con la salud o datos sobre la vida sexual de una persona natural o sexual orientación

La Empresa no realizará tratamiento de datos calificados como Sensibles (ver Definiciones) ni de Categorías Especiales (ver Definiciones), sin cumplir el siguiente procedimiento:

- Notificación del tratamiento previsto al Responsable de Privacidad de la Empresa
- Identificación de los datos a tratar y las actividades de tratamiento

- Análisis de riesgos, realizado bajo la supervisión del Responsable de Privacidad
- Informe de aplicación de medidas organizativas, técnicas y legales para asegurar el correcto nivel de protección
- Autorización firmada por el Responsable de Privacidad.

➔ ***Actualmente, según el RAT, la Empresa no trata datos sensibles. Ver análisis de la necesidad de un DPO y DPIA en Anexo 6.6 y 6.7***

4.16.1 Minimización de datos

Definición de minimización de datos:

El principio de minimización de los datos prescribe que los datos personales deben ser **adecuados, relevantes y limitados** a lo que sea **necesario** en relación con el objetivo para el que se tratan.

La Empresa procesa sólo los datos que sean estrictamente necesarios para sus propósitos, como declarado en el RAT.

A continuación, se analiza la adecuación de los datos con las finalidades

Categorías interesados	Tipos de datos	Finalidades
Empleados	Datos de identificación y contacto	Gestión de RRHH
Solicitantes, personas que facilitan el CV a la empresa	Datos de identificación y contacto, experiencia profesional y académica	Reclutamiento
Interlocutores/contacto de proveedores	Datos de identificación y contacto	Gestión comercial y elaboración de contratos
Interlocutores usuarios registrados	Datos de identificación y contacto	Gestión comercial con los usuarios registrados
Interlocutores/contacto de clientes	Datos de identificación	Gestión de la relación comercial
Interlocutores/contacto de clientes potenciales	Datos de identificación	Mantener el contacto comercial

Después del análisis de los datos en la tabla más arriba, la Empresa considera que todos los datos tratados son necesarios para la finalidad indicada.

La Empresa implementa las siguientes medidas para asegurar un tratamiento mínimo de datos:

- Los formularios de contacto y alta en Internet solamente contienen los campos estrictamente necesarios para el propósito (contacto, alta de usuario, etc.)
- La información recogida automáticamente está eliminada en los plazos mínimos (cookies, etc.) y se diseña para recoger solamente aquellos datos necesarios para las finalidades
- La empresa revisa periódicamente todos los archivos en papel y elimina cualquier archivo que pueda contener datos de carácter personal .
- La empresa implementa una política de retención indicada a continuación y elimina o bloquea cuantos datos sean necesarios para minimizar los tratamientos.
- La empresa implementa procesos de Alta y Baja de empleados, clientes, proveedores con el objetivo de asegurar un tratamiento mínimo de datos (ver Anexo 7.4)

4.17. RETENCIÓN, BLOQUEO Y CANCELACIÓN DE DATOS

Definición de principio de limitación del plazo de conservación de datos

El principio de limitación de conservación de los datos prescribe que los datos deben ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.

La Empresa guardará los datos durante los siguientes plazos:

Categorías interesados	Tipos de datos	Plazo de supresión
Empleados	Datos de identificación y contacto	Duración del contrato laboral y los 6 años posteriores
Solicitantes, personas que facilitan el CV a la empresa	Datos de identificación y contacto, experiencia profesional y académica	Desde la fecha de la entrevista y los 2 años posteriores
Interlocutores/contacto de proveedores	Datos de identificación y contacto	Previstos por la legislación fiscal respecto a la prescripción de responsabilidades. Duración del contrato y los 10 años posteriores
Interlocutores usuarios registrados	Datos de identificación y contacto	Duración del contrato y los 10 años posteriores
Interlocutores/contacto de clientes	Datos de identificación	Duración del contrato y los 10 años posteriores
Interlocutores/contacto de clientes potenciales	Datos de identificación	Duración del contrato y los 10 años posteriores

Los datos se guardarán en los sistemas **activos** de la empresa indicados en este documento mientras se requieren para las finalidades indicadas (por ejemplo, final de la relación contractual). Una vez cumplidas las finalidades (ver casos a continuación), se cancelarán en los sistemas activos de la empresa y se guardarán únicamente en copias de seguridad **bloqueadas y encriptadas**, a los que únicamente el Responsable de Seguridad podrá acceder, durante los plazos indicados (plazos que correspondan bajo la normativa laboral, contable, fiscal y lucha contra el fraude fiscal y de seguridad social). Transcurrido dicho plazo, se eliminarán totalmente, salvo aquellos datos que se desasociación y se destinen a fines históricos o estadísticos. Si los datos se encuentran en documentos, la supresión o la disociación, en su caso, se realizará utilizando al efecto una trituradora de papel.

Casos de cancelación y bloqueo de datos:

- A solicitud del interesado
- Inactividad de la cuenta de usuario/cliente después de **6 meses**, una vez el usuario haya sido informado de la baja.

- Finalización de la relación del interesado con la empresa (laboral, cliente, proveedor)

El Responsable de Seguridad verificará al menos una vez cada 6 meses el cumplimiento de este apartado.

La cancelación de los datos de carácter personal se realizará mediante el bloqueo, que en función del sistema de tratamiento será:

- **Bloqueo lógico**: Cuando los datos de carácter personal se encuentren almacenados en aplicaciones o bases de datos ubicadas en los sistemas de información de la entidad. Este bloqueo se solicitará al departamento de soporte informático mediante el formulario de solicitud de bloqueo de datos de carácter personal para que proceda a realizar el correspondiente desarrollo.
- **Bloqueo físico**: Cuando los datos estén almacenados en soportes físicos o documentos, se procederá almacenar los soportes en un lugar de acceso restringido en las oficinas del Dept de Administración, y solamente podrá acceder el Responsable de Seguridad del Grupo A3Sec.

4.18. CALIDAD DE DATOS

Definición de calidad de datos

El principio de calidad de los datos prescribe que los datos personales deben ser correctos y actualizados, y formatearlos correctamente.

Garantizar la calidad de los datos es un proceso continuo. Al final de respetar tal principio, la empresa lleva a cabo las siguientes actividades:

Categorías de interesados / datos	Actividades para garantizar la calidad de datos
Empleados	- Validación con herramientas de validación automática (p.ej. validación de las direcciones de correos electrónicos, de falta de ortografía) - Verifica a intervalos periódicos que los datos sean consistentes y actuales

	- Eliminación/corrección de datos no actuales o consistentes
Candidatos	- Verifica a intervalos periódicos que los datos sean consistentes y actuales - Eliminación/corrección de datos no actuales o consistentes
Interlocutores clientes	- Verifica a intervalos periódicos que los datos sean consistentes y actuales - Eliminación/corrección de datos no actuales o consistentes
Interlocutores clientes potenciales	- Verifica a intervalos periódicos que los datos sean consistentes y actuales - Eliminación/corrección de datos no actuales o consistentes
Interlocutores proveedores	- Verifica a intervalos periódicos que los datos sean consistentes y actuales - Eliminación/corrección de datos no actuales o consistentes
Usuarios registrados	- Verifica a intervalos periódicos que los datos sean consistentes y actuales - Eliminación/corrección de datos no actuales o consistentes

4.19. DERECHOS INTERESADOS

En virtud de las leyes de protección de datos, los interesados tienen derecho a:

- ***Solicitar acceso** a sus datos personales (comúnmente conocida como "solicitud de acceso a un sujeto de datos"). Esto le permite recibir una copia de los datos personales que la Empresa tiene sobre el interesado y verificar que esté procesándolos legalmente.*
- ***Solicitar la corrección** de los datos personales que la Empresa tiene sobre el interesado. Esto le permite corregir cualquier dato incompleto o inexacto que la Empresa tenga sobre el interesado.*
- ***Solicitar el borrado** de sus datos personales. Esto permite solicitar a la Empresa que elimine los datos personales cuando no haya una buena razón para que continúe procesándolos. También el interesado tiene derecho a solicitar a la Empresa que elimine sus datos personales cuando haya ejercido con éxito su derecho a oponerse al procesamiento (ver a continuación), cuando la Empresa podría haber procesado su información ilegalmente o cuando deba borrar sus datos personales en cumplimiento de la ley local.*
- ***Objetar el tratamiento** de sus datos personales cuando aun teniendo un interés legítimo (o de un tercero) haya algo acerca de su situación particular que haga que desee oponerse al tratamiento en este ámbito, ya que considere que tiene un impacto en su derechos y libertades fundamentales. También tiene derecho a objetar cuando la Empresa trate sus datos personales para fines de*

marketing directo. En algunos casos, la Empresa puede demostrar que tiene fundamentos legítimos convincentes para tratar su información que anulan estos derechos.

- ***Solicitar la limitación** del tratamiento de sus datos personales. Esto permite al interesado pedir la Empresa que suspenda el tratamiento de sus datos personales en los siguientes escenarios: (a) si desea que establezca la precisión de los datos; (b) cuando el uso de los datos es ilegal pero no desea que los borremos; (c) cuando necesite que la Empresa retenga los datos, incluso si ya no los necesita para ejercitar o defender reclamaciones legales; o (d) se ha opuesto al uso de sus datos, pero la Empresa debe verificar si tiene razones legítimas para usarlos.*
- ***Solicitar la transferencia** de sus datos personales a él mismo o a un tercero. La Empresa tendrá que proporcionar al interesado, o a un tercero que el interesado haya elegido, sus datos personales en un formato estructurado, de uso común y legible. Este derecho sólo se aplica a la información automatizada que el interesado autoriza mediante consentimiento a utilizar, así como a la información necesaria para la celebración de cualquier contrato con el interesado.*
- ***Retirar el consentimiento** en cualquier momento en el que la Empresa dependa del consentimiento para tratar sus datos personales. Sin embargo, esto no afectará a la legalidad de ningún tratamiento llevado a cabo antes de que retirara su consentimiento. Si el interesado retira su consentimiento, es posible que la Empresa no pueda proporcionarle ciertos productos o servicios.*

Grupo A3Sec ha implementado las siguientes medidas para hacer que esos derechos sean efectivos:

- Creación de una dirección de correo electrónico específica donde los interesados pueden dirigir sus solicitudes: *dataprotection@a3sec.com*
- Se establece un protocolo especial (Protocolo ARCO), para establecer las acciones necesarias en caso de solicitudes ARCO.

a) Recuperación de datos personales

Cuando sea necesaria la recuperación de datos personales, el Responsable de Seguridad lo tratará como una incidencia, debiendo abrir registro de la misma.

4.20. PRIVACY BY DESIGN

Definición de Protección de datos desde el diseño

El término "Protección de datos desde el diseño" significa que el Responsable del tratamiento deberá, en el momento de la determinación de los medios para el tratamiento y en el momento del tratamiento en sí, implementar las medidas técnicas y organizativas apropiadas, como la seudonimización, que están diseñadas para implementar los principios de protección de datos

de manera efectiva e integrar las salvaguardas necesarias en el procesamiento para cumplir con los requisitos del RGPD

Grupo A3Sec, con el fin de garantizar el cumplimiento de lo exigido y, por ende, proteger los derechos de los interesados titulares de los datos personales, aplica las siguientes medidas:

- En el proceso de recabar los datos personales, únicamente se recogen los datos personales de los interesados que son estrictamente necesarios;
- La calidad de los datos es revisada de manera constante, comprobando periódicamente la coherencia y la pertinencia de los datos y eliminando los que no son pertinentes.
- Han sido implementadas medidas de seguridad tanto técnicas como físicas que garantizan un tratamiento de los datos personales por Grupo A3Sec acordes a los estándares de seguridad exigidos por la normativa de protección de datos. Además, Grupo A3Sec mantiene un registro o autoriza el acceso a los datos personales;
- Ha sido implementada una política estricta que todos los empleados y contratistas independientes siguen en relación con los datos personales;
- Las partes interesadas pueden ejercer fácilmente los derechos de los interesados poniéndose en contacto con la Empresa por correo electrónico o postal.
- La forma de ejercer los derechos de los interesados se indica en la política de privacidad del sitio web, así como en todos los contratos.
- Grupo A3Sec, en virtud del principio de minimización de los datos y limitación del plazo de conservación, eliminará todos los datos personales cuando ya no sean necesarios y se almacenarán (bloquean) por razones administrativas y de responsabilidad jurídica.

5. MEDIDAS DE PROTECCIÓN Y POLÍTICA DE SEGURIDAD

Medidas de Seguridad

La Empresa tiene la obligación de implementar medidas de seguridad para garantizar un nivel de seguridad apropiado para el riesgo, que incluye:

- La seudonimización y el criptografía de datos personales;
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad, trazabilidad, autenticidad y flexibilidad constantes de los sistemas y servicios de tratamiento;
- La capacidad de restablecer la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico;

Es un proceso para probar y evaluar regularmente la efectividad de las medidas técnicas y organizativas para garantizar la seguridad del procesamiento haciendo cumplir mediante su *Política Corporativa de Seguridad de la Información.*

>_Control de cambios

Versión	Fecha	Descripción del cambio	Responsable de la aprobación del cambio
1.0	Enero 2021	Versión inicial	ACROSS LEGAL SLP
2.0	Junio 2021	Versión actualizada	ACROSS LEGAL SLP
3.0	19/11/2021	Versión oficial vigente	Comité de Seguridad
3.0	23/11/2022	Versión revisada.	Comité de Seguridad
3.0	23/11/2023	Versión revisada.	Comité de Seguridad
4.0	27/08/2024	se incluye cumplimiento legal, Funciones del encargado de tratamiento, se modifican algunos títulos del documento referente al ENS.	Comité de Seguridad