3HSASCORP

POLÍTICA INTEGRAL DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

Colombia | Versión 2.0 reforzada

Responsable identificado en el documento base	3HSAS / 3HSASCORP (razón social exacta por confirmar)
NIT informado	900602045-1 (verificar dígito de verificación y razón social)
Domicilio informado	Bogotá D. C., Colombia
Canal de consultas y reclamos informado	chall@3hsascorp.com (verificar que esté activo y monitoreado)
Teléfono informado	+57 315 326 6949
Sitio web informado	https://www.3hsascorp.com/
Fecha de versión	20 de noviembre de 2026
Aprobación y entrada en vigencia	A partir de su aprobación formal por 3HSASCORP

Documento marco para clientes, candidatos, trabajadores, proveedores, aliados y demás titulares.

CONTROL DEL DOCUMENTO Y ADVERTENCIA DE IMPLEMENTACIÓN

Esta versión amplía y fortalece el documento base entregado por 3HSASCORP. Está diseñada para las actividades de consultoría de talento, reclutamiento, selección, executive search, headhunting, talent mapping, recruitment intelligence y administración de bases de datos de candidatos.

IMPORTANTE: la política no constituye por sí sola una autorización individual ni sanea tratamientos anteriores. Antes de publicarla, 3HSASCORP debe completar las verificaciones señaladas en el apartado “Datos que deben validarse antes de publicación”, aprobar los procedimientos internos y revisar la legitimidad de las hojas de vida históricas.

La presente es una propuesta de cumplimiento construida con base en la información suministrada y el marco normativo colombiano consultado. No equivale a concepto jurídico vinculante ni sustituye la validación final por abogado colombiano con acceso a contratos, flujos tecnológicos, bases de datos y prácticas reales de la compañía.

1. IDENTIFICACIÓN DEL RESPONSABLE Y MARCO NORMATIVO

3HSASCORP, cuya razón social, naturaleza jurídica y datos registrales deberán verificarse antes de publicar esta Política (en adelante, “la Compañía”), tratará datos personales en calidad de Responsable cuando decida sobre las finalidades y medios del tratamiento. Cuando actúe por instrucciones documentadas de un cliente u otro tercero Responsable, tendrá la calidad de Encargado respecto de ese tratamiento específico.

El tratamiento se regirá, principalmente, por el artículo 15 de la Constitución Política; la Ley Estatutaria 1581 de 2012; el Decreto 1074 de 2015, en lo pertinente; las disposiciones que los modifiquen, adicionen o sustituyan; y las instrucciones y criterios de la Superintendencia de Industria y Comercio (SIC). También se observarán las normas laborales, comerciales, civiles, tributarias y sectoriales que resulten aplicables a cada operación.

La calificación de 3HSASCORP como Responsable o Encargado no depende únicamente del nombre que se asigne en un contrato: se determinará atendiendo a quién define realmente las finalidades y los medios esenciales del tratamiento.

2. OBJETO, ALCANCE Y ÁMBITO DE APLICACIÓN

Esta Política establece los criterios para recolectar, recibir, consultar, verificar, organizar, analizar, almacenar, actualizar, usar, circular, transmitir, transferir, conservar, anonimizar y suprimir datos personales contenidos en archivos físicos, sistemas, plataformas, correos, formularios, hojas de cálculo, grabaciones y demás repositorios administrados por la Compañía.

Aplica a toda persona natural cuyos datos sean tratados por 3HSASCORP, incluyendo:

- Candidatos, aspirantes, postulantes, referidos, profesionales identificados mediante búsqueda directa y personas incluidas en procesos de executive search, headhunting, talent mapping o recruitment intelligence.
- Personas cuyas hojas de vida, perfiles profesionales, datos de contacto, entrevistas, referencias, resultados de pruebas o informes se encuentren almacenados en repositorios actuales o históricos de la Compañía.
- Clientes, prospectos, representantes, contactos empresariales y personas de organizaciones contratantes.
- Trabajadores, exempleados, contratistas, consultores, proveedores, aliados y asesores.
- Visitantes, usuarios del sitio web y personas que interactúen con canales digitales de la Compañía.

La Política cobija las bases de datos existentes a la fecha de entrada en vigor y las que se creen posteriormente, sin que ello implique que la mera existencia de un registro habilite automáticamente todos los usos aquí descritos. Cada operación deberá contar con autorización o fundamento jurídico válido, finalidad informada y controles adecuados.

3. DEFINICIONES

Autorización: Consentimiento previo, expreso e informado del titular, obtenido por un medio que permita su consulta posterior, cuando sea exigible.

Base de datos: Conjunto organizado de datos personales sometidos a tratamiento.

Dato personal: Información vinculada o que pueda asociarse a una persona natural identificada o identificable.

Dato público: Dato que, conforme a la ley, no sea semiprivado, privado o sensible. Que un dato sea visible en internet no significa automáticamente que cualquier uso ulterior sea libre o ilimitado.

Dato privado, semiprivado y sensible: Categorías sujetas a distintos niveles de reserva y protección. Son sensibles, entre otros, los datos de salud, biométricos, orientación política, convicciones religiosas o filosóficas, vida sexual y aquellos cuyo uso indebido pueda generar discriminación.

Titular: Persona natural a quien corresponden los datos personales.

Responsable: Persona natural o jurídica que decide sobre la base de datos o las finalidades y medios del tratamiento.

Encargado: Persona natural o jurídica que realiza el tratamiento por cuenta del Responsable y conforme a sus instrucciones.

Transmisión: Comunicación de datos a un Encargado para que los trate por cuenta del Responsable, dentro o fuera de Colombia.

Transferencia: Comunicación de datos a otro Responsable, dentro o fuera de Colombia.

Hoja de vida o perfil profesional: Documento o conjunto de datos que contiene información de identificación, contacto, formación, experiencia, competencias, trayectoria, referencias y demás información profesional de un candidato.

Talent mapping / recruitment intelligence: Actividades de investigación y análisis del mercado laboral para identificar, clasificar y estudiar talento potencial. No autorizan por sí mismas la recolección indiscriminada ni la divulgación de datos personales.

Anonimización: Proceso que impide razonablemente identificar o reidentificar al titular. La seudonimización, por sí sola, no equivale a anonimización.

4. PRINCIPIOS RECTORES

La Compañía observará los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad, confidencialidad y responsabilidad demostrada. En aplicación de estos principios:

- Solo tratará datos para finalidades legítimas, específicas, explícitas e informadas al titular.
- Solicitará autorización cuando sea exigible y conservará evidencia verificable de su obtención, alcance, fecha, canal y versión del aviso o formato presentado.
- Recolectará únicamente información adecuada, pertinente y necesaria para la finalidad concreta; evitará solicitar datos excesivos.
- Mantendrá los datos razonablemente exactos, completos, actualizados, comprobables y comprensibles, y habilitará mecanismos de corrección.
- Restringirá el acceso según funciones y necesidad de conocer; no permitirá la circulación indiscriminada de hojas de vida ni informes.
- Aplicará medidas de seguridad proporcionales al volumen, naturaleza, sensibilidad, contexto y riesgos del tratamiento.
- No utilizará la información para finalidades incompatibles con las informadas, salvo que exista una nueva autorización o fundamento jurídico válido.
- Podrá demostrar, mediante soportes, políticas, registros, contratos, capacitaciones y controles, las medidas adoptadas para cumplir sus obligaciones.

5. CATEGORÍAS DE DATOS QUE PODRÁN SER TRATADOS

5.1. Datos de identificación y contacto

Nombre, tipo y número de documento cuando resulte necesario, datos de contacto, ciudad, dirección, correo electrónico, teléfono y datos profesionales de contacto.

5.2. Datos profesionales y de candidatos

Hojas de vida; historial laboral; cargos; empleadores; fechas y funciones; logros; formación académica; certificaciones; licencias; idiomas; competencias; portafolios; publicaciones profesionales; referencias; aspiraciones laborales; disponibilidad; ubicación geográfica general; pretensiones salariales cuando sean pertinentes; entrevistas; notas

profesionales; resultados de pruebas y evaluaciones relacionadas con un cargo; y trazabilidad de la participación en procesos.

5.3. Datos de verificación

Información necesaria y proporcional para verificar identidad, formación, experiencia, licencias, referencias y requisitos objetivos del cargo, siempre dentro de la finalidad informada, con autorización o fundamento jurídico aplicable y respetando las restricciones legales. Las verificaciones de antecedentes, listas restrictivas o información judicial se realizarán únicamente cuando sean pertinentes, legalmente procedentes y con controles reforzados.

5.4. Datos comerciales, contractuales y financieros

Información de clientes, representantes, proveedores y contratistas relacionada con propuestas, cotizaciones, contratos, facturación, pagos, obligaciones y gestión de la relación.

5.5. Datos laborales y de seguridad social

Información requerida para selección, vinculación, administración de la relación laboral o contractual, nómina, seguridad social, obligaciones tributarias y de seguridad y salud en el trabajo, según corresponda.

5.6. Datos técnicos y de interacción digital

Registros de acceso, identificadores técnicos, dirección IP, cookies, formularios, trazas de uso, metadatos y registros de comunicaciones digitales, cuando sean efectivamente recolectados y se informe su uso.

5.7. Datos sensibles y de menores

La Compañía evitará recolectar datos sensibles. Solo los tratará cuando exista una excepción legal aplicable o autorización explícita, previa e informada, y cuando sean estrictamente necesarios para una finalidad legítima. Informará que el titular no está obligado a autorizar su tratamiento, salvo los casos previstos en la ley. No solicitará datos de niños, niñas y adolescentes para sus procesos ordinarios de selección; cualquier excepción deberá contar con análisis jurídico específico y garantías reforzadas.

6. FINALIDADES DEL TRATAMIENTO

6.1. Candidatos, aspirantes y profesionales identificados

- Recibir, registrar, organizar, custodiar y administrar hojas de vida y perfiles profesionales remitidos directamente por el titular o recibidos por canales legítimos.
- Identificar y contactar profesionales para informarles sobre oportunidades laborales o procesos de selección compatibles con su perfil, únicamente cuando exista autorización o fundamento jurídico válido para ese contacto.
- Desarrollar procesos de reclutamiento, selección, executive search, headhunting, talent mapping y recruitment intelligence para clientes actuales o potenciales, dentro de las finalidades informadas.
- Evaluar la correspondencia entre la trayectoria, experiencia, formación, competencias y requisitos objetivos de una vacante.
- Realizar entrevistas, pruebas y evaluaciones pertinentes al cargo; elaborar matrices de comparación, informes ejecutivos y conceptos profesionales; y documentar la trazabilidad del proceso.
- Verificar, cuando sea pertinente y legalmente procedente, la información suministrada por el candidato, sus referencias, formación, experiencia, certificaciones y requisitos del cargo.
- Presentar al cliente contratante perfiles, hojas de vida, informes, resultados y recomendaciones estrictamente necesarios para la evaluación del candidato, de acuerdo con la autorización y el aviso entregado.
- Conservar el perfil en una base de talento para futuras oportunidades, búsquedas o procesos, únicamente si esa finalidad fue informada y se cuenta con autorización o fundamento jurídico válido.
- Atender consultas, reclamos, solicitudes de actualización, revocatoria o supresión; y cumplir obligaciones legales o defender derechos en actuaciones administrativas o judiciales.

6.2. Clientes, prospectos y contactos empresariales

- Atender solicitudes, consultas, quejas, reclamos y requerimientos.
- Preparar y presentar propuestas, cotizaciones, ofertas y diagnósticos; gestionar negociaciones, contratos, órdenes de servicio, facturación, cobro y pagos.
- Prestar, administrar, evaluar y mejorar los servicios; gestionar la relación comercial, el servicio posventa y la comunicación operativa.
- Enviar información comercial, invitaciones, novedades y contenidos sobre servicios relacionados, cuando exista autorización o fundamento jurídico aplicable y se respeten las opciones de oposición.

6.3. Trabajadores, exempleados, contratistas y proveedores

Gestionar selección, vinculación, ejecución y terminación de relaciones laborales o contractuales; pagos; obligaciones laborales, de seguridad social, contables y tributarias; control de acceso; seguridad; cumplimiento legal; auditorías; y defensa de derechos.

6.4. Finalidades transversales

- Cumplir obligaciones legales, requerimientos de autoridades competentes y órdenes judiciales.
- Prevenir fraude, proteger activos, sistemas, instalaciones, información y derechos de la Compañía, de titulares y de terceros.
- Gestionar continuidad operativa, auditorías, control interno, gestión de riesgos y calidad del servicio.
- Realizar análisis estadísticos y de desempeño, preferiblemente con datos agregados o efectivamente anonimizados.
- Administrar proveedores tecnológicos y servicios de almacenamiento, comunicaciones, videoconferencia, gestión documental, evaluación o analítica, bajo contratos y controles adecuados.

7. REGLAS ESPECIALES PARA HOJAS DE VIDA Y BASES DE TALENTO

7.1. Hojas de vida históricas y preexistentes

Esta Política comprende las hojas de vida y perfiles que 3HSASCORP tenga almacenados antes de su publicación, incluidos archivos físicos, correos, hojas de cálculo, carpetas compartidas, plataformas de selección, repositorios de entrevistas e informes. Sin embargo, la inclusión de estos registros en el ámbito de la Política no equivale a una autorización retroactiva.

La Compañía realizará un inventario y una revisión de legitimidad de los registros históricos para identificar, como mínimo: origen del dato; fecha y canal de recepción; evidencia de autorización; finalidades autorizadas; alcance de la comunicación a clientes; vigencia o actualidad; categorías de datos; ubicación de almacenamiento; y terceros con acceso.

Cuando no exista evidencia suficiente de autorización o de otra base jurídica válida para una finalidad concreta, 3HSASCORP suspenderá el uso no indispensable, restringirá el acceso y adelantará la regularización mediante contacto y obtención de autorización válida, o procederá a la supresión o anonimización cuando corresponda. La publicación de esta Política no subsana por sí sola la falta de autorización previa.

7.2. Conservación para futuras oportunidades

La conservación de una hoja de vida para vacantes futuras constituye una finalidad que debe ser informada de forma clara y contar con autorización o fundamento jurídico válido. La autorización para participar en una vacante específica no se interpretará automáticamente como autorización indefinida para integrar una base general de talento.

Como regla interna de minimización, 3HSASCORP revisará la vigencia de los perfiles de su base de talento, como mínimo, cada veinticuatro (24) meses desde la última actualización o confirmación del titular. Este plazo es un criterio operativo de revisión y no un término legal universal. Cumplido el plazo sin actualización o confirmación, la Compañía podrá contactar al titular para renovar la vigencia; si no obtiene respuesta o no cuenta con fundamento para continuar, restringirá el perfil y lo suprimirá o anonimizará, salvo deber legal o necesidad legítima documentada de conservación.

7.3. Compartir hojas de vida con clientes

La entrega de una hoja de vida identificada, datos de contacto, informes de entrevista o resultados de evaluación a un cliente deberá limitarse a los datos pertinentes para la vacante y al alcance informado al candidato. Antes de remitir información identificable, 3HSASCORP verificará que el candidato haya sido informado sobre la comunicación a clientes potenciales o determinados y que exista autorización o fundamento jurídico aplicable.

Cuando sea posible en una etapa inicial, se utilizarán perfiles anonimizados o seudonimizados. La identidad y los datos de contacto se revelarán cuando sea necesario para avanzar en el proceso y exista cobertura jurídica suficiente. El cliente receptor deberá asumir obligaciones de uso limitado, confidencialidad, seguridad, conservación y atención de derechos, según su rol.

7.4. Datos obtenidos de fuentes profesionales públicas

La Compañía podrá consultar fuentes profesionales y de acceso público para actividades legítimas de identificación de talento, observando la normativa, los términos de uso de las plataformas y los principios de finalidad, necesidad, circulación restringida y calidad. La disponibilidad pública de un dato no habilita su extracción masiva, enriquecimiento ilimitado, conservación indefinida ni divulgación indiscriminada. Se documentará la fuente y la finalidad de la consulta cuando resulte pertinente.

7.5. Referencias y terceros

La Compañía procurará obtener referencias directamente de personas designadas por el candidato o con conocimiento legítimo de su trayectoria. Informará al candidato sobre la verificación y evitará recopilar datos personales de terceros que no sean necesarios. Si se reciben datos de terceros, se tratarán con acceso restringido y se evaluará el deber de información que corresponda.

7.6. Evaluaciones, informes y decisiones

Las pruebas y evaluaciones deberán guardar relación con el perfil del cargo, ser proporcionales y aplicarse con criterios profesionales. Los informes distinguirán hechos verificados, información declarada, observaciones, resultados de instrumentos y apreciaciones técnicas. No se presentarán inferencias como hechos comprobados. La decisión final de selección corresponde al cliente empleador, sin perjuicio de las responsabilidades propias de cada parte.

La Compañía no adoptará decisiones con efectos jurídicos o significativamente similares basadas exclusivamente en tratamientos automatizados, sin revisión humana significativa, cuando ello resulte contrario a la normativa aplicable o a los derechos del titular. Los sistemas de IA o analítica, si se utilizan, serán herramientas de apoyo sujetas a supervisión humana, validación de calidad, controles de sesgo, trazabilidad y limitación de datos.

7.7. Datos sensibles en selección

No se solicitarán ni utilizarán datos sensibles para filtrar o clasificar candidatos, salvo necesidad estricta, excepción legal o autorización explícita y garantías adecuadas. Se evitará incorporar a informes datos de salud, biométricos, orientación política, religión, afiliación sindical, vida sexual u otras categorías sensibles que no sean pertinentes y legalmente tratables. No se utilizarán datos sensibles para decisiones discriminatorias.

8. AUTORIZACIÓN, AVISO DE PRIVACIDAD Y PRUEBA

Cuando sea exigible, la autorización será previa, expresa e informada y podrá obtenerse por escrito, formulario electrónico, casilla no premarcada, mensaje de datos, grabación u otro mecanismo legalmente admisible que permita su consulta posterior. El silencio, la inacción o la mera publicación de la Política no equivalen a autorización.

Al solicitar la autorización, la Compañía informará, como mínimo: identidad y datos de contacto del Responsable; tratamiento y finalidades; derechos del titular; carácter facultativo de respuestas sobre datos sensibles o de niños, niñas y adolescentes; y medios para consultar la Política y ejercer derechos.

La evidencia deberá permitir demostrar quién autorizó, cuándo, por qué canal, qué texto y versión aceptó, qué finalidades cubrió y si hubo modificaciones posteriores. Los formatos deberán permitir distinguir, cuando corresponda,

la autorización para el proceso específico, la inclusión en la base de talento para futuras oportunidades, el envío de comunicaciones comerciales y el tratamiento de datos sensibles.

La Compañía conservará los soportes de autorización de manera segura y vinculada al registro del titular. Cuando cambien las finalidades de forma que requiera nueva autorización, esta se obtendrá antes de iniciar el nuevo tratamiento.

9. DERECHOS DE LOS TITULARES

El titular podrá ejercer, en los términos legales, los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales, incluidos los datos parciales, inexactos, incompletos, fraccionados o que induzcan a error.
- Solicitar prueba de la autorización, cuando sea exigible, e información sobre el uso dado a sus datos.
- Presentar consultas y reclamos ante la Compañía.
- Solicitar revocatoria de la autorización y/o supresión cuando proceda legalmente.
- Acceder gratuitamente a sus datos personales objeto de tratamiento, en los términos legales.
- Ser informado sobre el carácter facultativo de las respuestas a preguntas sobre datos sensibles o de niños, niñas y adolescentes.
- Presentar queja ante la Superintendencia de Industria y Comercio, una vez agotado el trámite previo ante el Responsable o Encargado cuando la ley lo exija.

Estos derechos podrán ser ejercidos por el titular, sus causahabientes, representante o apoderado debidamente acreditado, y por las demás personas legitimadas conforme a la ley. La revocatoria y la supresión no procederán cuando exista un deber legal o contractual de permanencia, una obligación de conservación o una excepción legal aplicable. La Compañía explicará de manera concreta la razón de cualquier limitación.

10. CANALES Y PROCEDIMIENTO PARA CONSULTAS Y RECLAMOS

Canal principal informado: chall@3hsascorp.com. Teléfono informado: +57 315 326 6949. Domicilio informado: Bogotá D. C., Colombia. Antes de publicar, 3HSASCORP deberá confirmar que el correo esté activo, sea administrado por personal autorizado y tenga un procedimiento de escalamiento. Se recomienda habilitar un canal alternativo y publicar dirección física completa para notificaciones.

Las solicitudes deberán permitir identificar al titular y, cuando corresponda, a su representante; describir los hechos y la petición; indicar un medio de respuesta; y adjuntar soportes de identidad o representación cuando sean necesarios y proporcionales. No se solicitarán documentos excesivos para validar la identidad.

10.1. Consultas

Las consultas se atenderán dentro de diez (10) días hábiles contados desde su recepción. Cuando no sea posible responder dentro de ese término, se informarán los motivos y la fecha de respuesta, que no podrá superar cinco (5) días hábiles adicionales al vencimiento del término inicial.

10.2. Reclamos

Si el reclamo está incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a su recepción para que subsane. Transcurridos dos (2) meses desde el requerimiento sin recibir la información solicitada, se entenderá que ha desistido, conforme a la ley. Si quien recibe el reclamo no es competente, lo trasladará a quien corresponda dentro del término legal e informará al interesado.

Una vez recibido el reclamo completo, se incorporará en la base de datos la leyenda “reclamo en trámite” en los términos legales. El reclamo se atenderá dentro de quince (15) días hábiles contados desde el día siguiente a su recepción. Cuando no sea posible, se informarán los motivos y la fecha de respuesta, que no podrá superar ocho (8) días hábiles adicionales al vencimiento del término inicial.

10.3. Registro y trazabilidad

Toda consulta o reclamo deberá registrarse con fecha de recepción, titular, tipo de solicitud, responsable asignado, vencimiento, actuaciones, respuesta y evidencia de envío. Se conservará un expediente de atención con acceso restringido. Antes de acudir a la SIC, el titular agotará el trámite previo ante la Compañía cuando así lo exija la normativa.

11. ROLES DE 3HSASCORP Y RELACIÓN CON CLIENTES

En los servicios de selección, búsqueda y consultoría, el rol de cada parte se determinará operación por operación:

- 3HSASCORP será Responsable cuando construya y administre su propia base de talento, defina finalidades propias de identificación y contacto, conserve perfiles para futuras búsquedas bajo su propia decisión o determine los medios esenciales del tratamiento.
- 3HSASCORP podrá ser Encargado cuando procese información exclusivamente por cuenta de un cliente Responsable, bajo instrucciones documentadas y sin utilizarla para finalidades propias incompatibles.
- El cliente será Responsable de los datos que reciba y trate para sus propias decisiones de selección, contratación, vinculación y administración laboral, salvo que las circunstancias reales indiquen otra distribución de roles.
- Cuando ambas partes determinen conjuntamente finalidades y medios, deberán documentar con precisión sus responsabilidades, canales de atención, instrucciones, seguridad, conservación, incidentes y gestión de derechos.

Los contratos de prestación de servicios y acuerdos de tratamiento deberán identificar las bases de datos, categorías de titulares, finalidades, instrucciones, duración, operaciones autorizadas, medidas de seguridad, subencargados, transferencias internacionales, atención de derechos, incidentes, devolución o supresión de información y mecanismos de auditoría.

12. DIVULGACIÓN, TRANSMISIÓN Y TRANSFERENCIA

La Compañía podrá comunicar datos a clientes contratantes, proveedores tecnológicos, asesores, auditores, aliados y prestadores que necesiten conocerlos para una finalidad legítima y autorizada o jurídicamente habilitada. El acceso será limitado a lo necesario y sujeto a deberes de confidencialidad y seguridad.

Cuando un tercero trate datos por cuenta de 3HSASCORP, se formalizará el contrato de transmisión o las cláusulas correspondientes, con instrucciones documentadas y obligaciones de uso limitado, seguridad, confidencialidad, asistencia en derechos, gestión de incidentes y eliminación o devolución al finalizar el servicio.

Las transferencias de datos a otro Responsable y las transmisiones a Encargados, dentro o fuera de Colombia, se realizarán conforme a las reglas legales aplicables. Antes de habilitar almacenamiento o acceso desde el exterior, la Compañía identificará país, proveedor, rol, ubicación, subencargados, garantías, mecanismos contractuales y requisitos de transferencia internacional. No se presumirá que una transmisión y una transferencia son equivalentes.

La Compañía no venderá datos personales ni los utilizará para fines ajenos a los informados. La comunicación a clientes de perfiles de candidatos no se considerará una autorización general para que estos los incorporen a cualquier base o los compartan con terceros.

13. SEGURIDAD DE LA INFORMACIÓN Y CONFIDENCIALIDAD

3HSASCORP implementará medidas técnicas, humanas, físicas y administrativas razonables y proporcionales al riesgo. Como mínimo, establecerá y mantendrá:

- Control de acceso por roles, principio de mínimo privilegio, autenticación robusta y revisión periódica de permisos.
- Uso de contraseñas seguras, autenticación multifactor cuando esté disponible y prohibición de compartir credenciales.
- Cifrado de información en tránsito y, cuando sea viable y proporcional, en reposo; uso de canales corporativos aprobados.
- Copias de seguridad, pruebas de restauración, protección contra malware y actualización de sistemas.
- Registro y monitoreo de accesos, descargas, cambios, exportaciones y divulgaciones relevantes.
- Almacenamiento en repositorios corporativos autorizados; prohibición de guardar hojas de vida en dispositivos o cuentas personales no aprobadas.

- Reglas de envío seguro de hojas de vida e informes, verificación de destinatarios, enlaces con permisos restringidos y vencimiento cuando sea posible.
- Acuerdos de confidencialidad y capacitación para empleados, contratistas, consultores y proveedores con acceso.
- Retención y eliminación segura de documentos físicos y digitales; control de impresiones y destrucción confidencial.
- Evaluación de proveedores, plataformas de entrevistas, almacenamiento, correo, IA, analítica y otros servicios que puedan acceder a datos personales.

Toda persona que intervenga en el tratamiento deberá guardar confidencialidad sobre la información no pública, incluso después de terminada su relación con la Compañía. Los incidentes deberán escalarse inmediatamente al responsable interno designado, sin esperar a determinar su impacto definitivo.

14. INCIDENTES DE SEGURIDAD Y GESTIÓN DE BRECHAS

Se considera incidente, entre otros, la pérdida, robo, destrucción, alteración, adulteración, consulta, uso, acceso, divulgación o circulación no autorizada o fraudulenta de datos personales, así como la vulneración de controles de seguridad.

La Compañía mantendrá un procedimiento de respuesta que incluya: detección y reporte interno inmediato; contención; preservación de evidencias; evaluación del tipo y volumen de datos, titulares afectados, consecuencias y riesgo; recuperación; documentación; medidas correctivas; comunicación a clientes y titulares cuando corresponda; y reportes ante la SIC y demás autoridades dentro de los términos aplicables.

Cuando resulte exigible, los incidentes se reportarán a la SIC dentro de los quince (15) días hábiles siguientes al momento en que sean detectados y puestos en conocimiento de la persona o área encargada de atenderlos, utilizando el canal correspondiente según la obligación de inscripción en el RNBD. Los Encargados deberán informar sin dilación al Responsable para permitirle cumplir sus deberes y los plazos regulatorios.

La Compañía mantendrá un registro interno de incidentes, incluso de aquellos que no deban reportarse, con fecha, descripción, sistemas y bases afectados, análisis, decisiones, comunicaciones, reportes y acciones de mejora.

15. CONSERVACIÓN, ACTUALIZACIÓN, BLOQUEO Y SUPRESIÓN

Los datos se conservarán durante el tiempo razonable y necesario para las finalidades informadas, la relación contractual, las obligaciones legales, los términos de prescripción y la formulación, ejercicio o defensa de reclamaciones. No se conservarán indefinidamente por simple conveniencia.

Cada base deberá tener una matriz de retención que identifique categoría de datos, finalidad, fundamento, fecha de inicio, plazo o evento de terminación, responsable de revisión, destino final y excepciones de conservación. Cuando termine la finalidad, los datos se suprimirán o anonimizarán de forma segura, salvo deber legal o contractual de conservación.

Cuando exista una solicitud de supresión o revocatoria, la Compañía evaluará su procedencia, detendrá los usos no amparados y conservará únicamente lo estrictamente necesario cuando exista fundamento legal. Los datos sujetos a conservación obligatoria deberán bloquearse o restringirse para impedir usos distintos a la finalidad que justifica su permanencia.

La supresión de una base activa deberá contemplar copias, exportaciones, repositorios compartidos y proveedores, dentro de las posibilidades técnicas y contractuales. Las copias de respaldo se gestionarán de modo que los datos suprimidos no sean reintroducidos en producción al restaurarlas.

16. COOKIES, SITIO WEB Y HERRAMIENTAS DIGITALES

Si el sitio web o las plataformas de la Compañía utilizan cookies, píxeles, analítica, formularios, herramientas de chat, videoconferencia u otras tecnologías que recolecten datos personales, 3HSASCORP informará su uso, finalidades, terceros involucrados y opciones disponibles mediante avisos y configuraciones adecuados. Esta cláusula deberá ajustarse a las tecnologías efectivamente implementadas; no debe publicarse como afirmación de uso de herramientas que no existan.

17. USO DE INTELIGENCIA ARTIFICIAL Y HERRAMIENTAS DE EVALUACIÓN

Cuando la Compañía utilice herramientas de inteligencia artificial, automatización, transcripción, análisis de texto, clasificación, evaluación o generación de informes que involucren datos personales, deberá:

- Definir y documentar la finalidad, necesidad, proporcionalidad, proveedor, ubicación del procesamiento, datos enviados y tiempo de conservación.
- Informar al titular cuando el uso de la herramienta sea relevante para el tratamiento y cumplir los deberes de información y autorización aplicables.
- Evitar introducir hojas de vida, entrevistas, pruebas o datos identificables en herramientas no aprobadas o cuyos términos permitan usos incompatibles, entrenamiento no autorizado o divulgación a terceros.
- Aplicar minimización, anonimización o seudonimización cuando sea viable.
- Mantener supervisión humana significativa sobre análisis y recomendaciones que puedan afectar oportunidades laborales.
- Revisar precisión, sesgos, explicabilidad, pertinencia y riesgos discriminatorios; permitir corrección de datos y revisión de resultados.
- Formalizar compromisos de confidencialidad, seguridad, eliminación y restricciones de uso con proveedores.

La IA no sustituye la valoración profesional ni la decisión del empleador. Los resultados automatizados serán tratados como insumos sujetos a validación, no como hechos incontrovertibles.

18. REGISTRO NACIONAL DE BASES DE DATOS (RNBD) Y RESPONSABILIDAD DEMOSTRADA

La Compañía evaluará y documentará si está obligada a inscribir sus bases de datos en el Registro Nacional de Bases de Datos (RNBD), atendiendo a su naturaleza jurídica y al umbral legal de activos aplicable. La obligación de RNBD no debe presumirse ni descartarse sin revisar los estados financieros y la condición jurídica de la entidad.

La eventual no obligación de inscripción en el RNBD no exime del cumplimiento de la Ley 1581 de 2012, sus decretos reglamentarios y las instrucciones de la SIC. La Compañía mantendrá un programa de gestión de datos personales que incluya inventario de bases, finalidades, autorizaciones, matriz de riesgos, contratos, controles, formación, atención de derechos, retención, incidentes y auditorías.

19. CAMBIOS A LA POLÍTICA

La Compañía podrá actualizar esta Política para reflejar cambios legales, tecnológicos, organizacionales o en las prácticas de tratamiento. La versión vigente se publicará en el sitio web o se pondrá a disposición por los canales habituales. Cuando un cambio implique una nueva finalidad o requiera nueva autorización, esta se obtendrá antes de iniciar el tratamiento correspondiente. Se conservará control de versiones y fecha de publicación.

20. VIGENCIA

Esta versión 2.0 entrará en vigor en la fecha de aprobación formal por la Compañía y reemplazará las versiones anteriores desde esa fecha. La publicación no sustituye los avisos de privacidad, autorizaciones, contratos de transmisión, procedimientos internos, matrices de retención, controles de seguridad ni demás documentos que sean exigibles según las operaciones efectivas.

ANEXO A. TEXTO MODELO DE AUTORIZACIÓN PARA CANDIDATOS

Este texto debe adaptarse al formulario, proceso y canales reales. Se recomienda mantener autorizaciones separadas y no premarcadas para finalidades opcionales, especialmente la inclusión en la base de talento para futuras oportunidades.

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES – CANDIDATOS

Yo, [NOMBRE COMPLETO], identificado(a) con [TIPO Y NÚMERO DE DOCUMENTO], manifiesto que he sido informado(a) de que [RAZÓN SOCIAL COMPLETA DE 3HSASCORP], identificada con NIT [NIT VERIFICADO], con domicilio en

[DIRECCIÓN], correo [CANAL DE PRIVACIDAD] (en adelante, “3HSASCORP”), tratará mis datos personales conforme a su Política de Tratamiento de Datos Personales, disponible en [URL].

Autorizo de manera previa, expresa e informada a 3HSASCORP para recolectar, almacenar, consultar, organizar, actualizar, verificar, analizar y utilizar la información que suministre o que sea obtenida legítimamente para gestionar mi participación en procesos de reclutamiento, selección, executive search, headhunting, talent mapping y recruitment intelligence; verificar, dentro de los límites legales, mi experiencia, formación, competencias y referencias; realizar entrevistas y evaluaciones relacionadas con el perfil; y elaborar informes profesionales.

Autorizo que la información estrictamente pertinente sobre mi perfil, hoja de vida, experiencia, formación, competencias, entrevistas y resultados relacionados con una vacante sea comunicada al cliente o potencial empleador que participe en el proceso para el cual he sido considerado(a), con el fin de evaluar mi ajuste al cargo. Entiendo que el cliente que reciba mis datos podrá actuar como Responsable independiente respecto de sus propios procesos y decisiones, y deberá cumplir la normativa aplicable.

AUTORIZACIÓN OPCIONAL – BASE DE TALENTO Y FUTURAS OPORTUNIDADES: [ ] Sí autorizo / [ ] No autorizo que 3HSASCORP conserve mi hoja de vida y perfil en su base de talento para contactarme y considerarme en futuras oportunidades profesionales compatibles con mi experiencia, incluso en procesos de búsqueda para otros clientes, durante el período informado en la Política y sujeto a sus revisiones de vigencia.

AUTORIZACIÓN OPCIONAL – COMUNICACIONES: [ ] Sí autorizo / [ ] No autorizo el envío de información sobre oportunidades, novedades y comunicaciones relacionadas con servicios de talento, a través de correo electrónico, teléfono o mensajería.

Declaro que conozco mis derechos a conocer, actualizar y rectificar mis datos; solicitar prueba de la autorización e información sobre su uso; revocar la autorización y solicitar supresión cuando proceda legalmente; y presentar consultas o reclamos por los canales indicados en la Política. Entiendo que las respuestas sobre datos sensibles son facultativas y que no estoy obligado(a) a autorizar su tratamiento, salvo excepción legal.

Declaro que la información entregada es, según mi leal saber y entender, veraz, completa y actualizada, y me comprometo a informar cambios relevantes. Entiendo que la autorización no garantiza mi participación, avance o contratación en ningún proceso.

Nombre: _____ Documento: _____

Firma o aceptación electrónica: _____ Fecha: _____

Canal de obtención de autorización: _____ Versión del texto: _____

ANEXO B. LISTA DE VERIFICACIÓN PARA REGULARIZAR HOJAS DE VIDA HISTÓRICAS

La Compañía deberá ejecutar y documentar, como mínimo, las siguientes actividades antes de continuar utilizando indiscriminadamente la base histórica:

1. Inventariar todas las fuentes: correo, Drive, hojas de cálculo, ATS, carpetas locales, informes, entrevistas, archivos físicos, copias y respaldos.
2. Clasificar registros por origen, fecha de recepción, proceso, cliente, finalidad, categoría de datos y ubicación.
3. Identificar evidencia de autorización: formulario, correo, casilla, grabación o registro electrónico; conservar el texto y versión aceptados.
4. Verificar si la autorización cubre el proceso específico, futuras oportunidades, contacto directo, verificación de referencias y comunicación a clientes.
5. Identificar hojas de vida obtenidas de terceros, referidos, búsquedas públicas o bases heredadas; documentar el origen y analizar el fundamento de uso.
6. Separar registros con autorización válida, autorización parcial, autorización no demostrable y datos cuyo origen no pueda establecerse.
7. Restringir temporalmente los registros sin soporte suficiente para impedir nuevas comunicaciones o divulgaciones no justificadas.
8. Contactar a los titulares cuando sea procedente para informar el tratamiento y obtener una autorización válida, sin presentar la falta de respuesta como consentimiento.

9. Suprimir o anonimizar registros cuando no exista fundamento para conservarlos y no sea posible regularizarlos.
10. Registrar las decisiones, fechas, responsables, soportes y resultado de cada lote de regularización.

ANEXO C. CONTROLES MÍNIMOS DE OPERACIÓN

Frente	Control esperado
Gobierno	Designar responsable interno de privacidad y suplente; aprobar matriz RACI; mantener inventario de bases y proveedores.
Candidatos	Usar autorización diferenciada; registrar versión y evidencia; limitar acceso; verificar vigencia; establecer canal de actualización y retiro.
Clientes	Firmar cláusulas de tratamiento; determinar roles; compartir solo datos necesarios; usar perfiles anonimizados en etapas tempranas cuando sea viable.
Tecnología	Aprobar herramientas; activar MFA; revisar permisos; controlar exportaciones; cifrar y respaldar; evaluar ubicación y subencargados.
IA y analítica	Prohibir herramientas no aprobadas; minimizar datos; documentar proveedores y finalidades; asegurar revisión humana y controles de sesgo.
Derechos	Registrar solicitudes; asignar responsable; controlar plazos; conservar evidencia de respuesta y ejecución.
Incidentes	Canal de reporte interno inmediato; protocolo de contención; registro; evaluación de notificación a titulares, clientes y SIC.
Retención	Matriz por base; revisiones periódicas; eliminación segura; bloqueo de registros sujetos a deber legal.
Personal	Compromisos de confidencialidad; inducción y capacitación periódica; revocación de accesos al retiro.
Auditoría	Revisión periódica de autorizaciones, permisos, contratos, incidentes, retención y cumplimiento de proveedores.

ANEXO D. DATOS QUE DEBEN VALIDARSE ANTES DE PUBLICACIÓN

- Razón social exacta que actúa como Responsable, NIT completo y dígito de verificación, domicilio y dirección física de notificaciones.
- Confirmar si “3HSAS” y “3HSASCORP” corresponden a la misma persona jurídica y cuál es la denominación legal que debe aparecer en el documento.
- Confirmar que chall@3hsascorp.com es un buzón válido, monitoreado, con acceso restringido y procedimiento de escalamiento; corregirlo si existe error tipográfico.
- Confirmar teléfono, URL, dirección y persona/área responsable de privacidad.
- Determinar si 3HSASCORP está obligada a inscribir bases en el RNBD, revisando naturaleza jurídica y activos totales.
- Levantar inventario de plataformas y proveedores: correo, almacenamiento, videoconferencia, formularios, ATS, firma electrónica, mensajería, IA, transcripción y analítica; identificar países de alojamiento y subencargados.
- Revisar contratos vigentes con clientes para establecer cuándo 3HSASCORP actúa como Responsable, Encargado o participa en tratamientos con roles compartidos.

- Definir plazos reales de conservación por tipo de dato y obligación legal; el plazo operativo de 24 meses para revisión de la base de talento debe aprobarse internamente y comunicarse correctamente.
- Verificar si se recolectan datos sensibles, antecedentes, referencias, grabaciones de entrevistas, fotografías, datos biométricos o información de salud; eliminar categorías que no sean necesarias.
- Aprobar el formato de autorización de candidatos, aviso de privacidad corto, procedimiento de consultas y reclamos, protocolo de incidentes, matriz de retención y cláusulas de transmisión.

ANEXO E. FUENTES NORMATIVAS Y CRITERIOS DE REFERENCIA

La estructura y los controles de esta propuesta se apoyan principalmente en:

- Constitución Política de Colombia, artículo 15.
- Ley Estatutaria 1581 de 2012, régimen general de protección de datos personales.
- Decreto 1074 de 2015, disposiciones reglamentarias sobre autorización, políticas, avisos, transmisión y responsabilidad en el tratamiento.
- Instrucciones de la Superintendencia de Industria y Comercio (SIC), incluyendo las relativas al Registro Nacional de Bases de Datos, incidentes de seguridad y responsabilidad demostrada.

Referencias oficiales consultadas para esta revisión:

- Ley 1581 de 2012 – Gestor Normativo de Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
- SIC – Políticas de tratamiento de datos personales y contenido mínimo: https://sedeelectronica.sic.gov.co/publicaciones/boletin-juridico/concepto/politicas-de-tratamiento-de-datos-personales
- SIC – Obligación de inscripción en el RNBD: https://sedeelectronica.sic.gov.co/publicaciones/boletin-juridico/concepto/cuales-personas-estan-obligadas-realizar-el-registro-de-bases-de-datos-personales-en-el-rnbd
- SIC – Reporte de incidentes de seguridad: https://sedeelectronica.sic.gov.co/publicaciones/boletin-juridico/concepto/cumplimiento-de-la-obligacion-del-reporte-de-incidentes-de-seguridad