INTEGRIDAD Y COMPLIANCE

Protocolo de Datos Personales en Reclutamiento y Selección

Versión: Agosto 2026

Ossandón Auditores Consultores
Miembro independiente de BKR International
Viña del Mar · Santiago · www.oci.cl

Versión	4.0
Fecha	Agosto de 2026
Responsable interno	Jorge Valencia, Supervisor de Recursos Humanos Profesionales área Recursos Humanos
Ámbito	Procesos de reclutamiento y selección para clientes públicos y privados
Clasificación	Uso interno y externo controlado. Sujeto a aprobación por socio Miguel Ossandón C.

Nota: Este protocolo debe revisarse al menos una vez al año y cada vez que exista cambio normativo, tecnológico o contractual relevante.

Contenido

Resumen ejecutivo. Ossandón Auditores Consultores trata datos personales de postulantes y referencias laborales exclusivamente para evaluar idoneidad, gestionar procesos de selección, cumplir obligaciones contractuales y legales, y reportar resultados al cliente mandante. La regla general es recolectar solo lo necesario, limitar el acceso al equipo autorizado, documentar las bases de licitud, resguardar la confidencialidad, evitar usos secundarios no informados, usar IA solo como apoyo no decisorio y conservar la información por plazos proporcionales y trazables.

Presentación empresa

Somos una empresa de profesionales, fundada en la ciudad de Viña del Mar con más de 20 años de experiencia en el mercado. Nuestra presencia a nivel nacional está garantizada por nuestras oficinas en las ciudades de Santiago y Viña del Mar.

Nos preocupamos de proporcionar un servicio de consultoría y asesoría integral, con una visión de trabajo interdisciplinario, otorgando soluciones oportunas a las necesidades más exigentes, tanto para las organizaciones públicas como privadas.

Inscripciones y Asociaciones:

A nivel nacional, estamos inscritos en la Comisión para el Mercado Financiero en el Registro de Empresas de Auditoría Externa (REAE). Además, estamos presente en forma activa en el Portal de Mercado Público. Por otro lado, somos parte de la Cámara de Comercio de Santiago, de la Asociación de Empresas Región de Valparaíso – ASIVA, del Colegio de Contadores de Chile y de ICLASA.

A nivel internacional, desde el año 2011, nuestra Firma es miembro de BKR International, asociación internacional de auditores consultores establecida en el año 1989, como resultado de la fusión de grupo de CPA nacional en Estados Unidos y varios miembros de la Internacional DHR, principalmente europeo. Así también, estamos inscritos en el registro Public Company Accounting Oversight Board (PCAOB) de U.S.A. y además somos parte de International Test Commission (ITC).

1. Propósito y compromiso

Este Protocolo establece las reglas mínimas obligatorias para la recolección, uso, análisis, comunicación, almacenamiento, conservación y eliminación de información personal y sensible tratada por Ossandón Auditores Consultores en procesos de reclutamiento y selección de trabajadores para entidades públicas y privadas.

Su finalidad es entregar una guía práctica a consultores, psicólogos laborales, coordinadores, jefaturas y personal administrativo que participa en procesos de selección, y a la vez informar a clientes sobre el estándar de manejo de datos aplicado por la consultora.

El documento se adecúa a la legislación de nacional chilena y se alinea con las Normas de Orden, el Programa de Integridad y Compliance y el Protocolo de Inteligencia Artificial de Ossandón Auditores Consultores, en cuanto a probidad, confidencialidad, trazabilidad, prevención de conflictos de interés y uso responsable de herramientas tecnológicas.

2. Alcance y roles

Este Protocolo aplica a todos los procesos de búsqueda, reclutamiento, evaluación, entrevista, levantamiento de referencia, elaboración de informes, envío de ternas, acompañamiento de cierre y conservación posterior de antecedentes. Incluye procesos ejecutados por plataformas digitales, correo electrónico, videollamadas, entrevistas presenciales, evaluaciones psicolaborales, revisión curricular, contacto con referencias y comunicación con clientes.

- Responsable interno del proceso: jefatura o profesional designado para administrar el encargo, definir flujos, controlar accesos y validar entregables.
- Profesionales de selección: personas autorizadas para recolectar, analizar y reportar datos de candidatos y candidatas conforme a las finalidades del proceso.
- Equipo de soporte: personal administrativo o tecnológico que accede a datos solo cuando sea estrictamente necesario para el servicio.
- Cliente mandante: entidad pública o privada que solicita el proceso y recibe información de candidatos para adoptar decisiones de contratación.
- Titular de datos: persona postulante, trabajador o trabajadora, ex trabajador o ex trabajadora, referencia laboral u otra persona natural cuyos datos sean tratados.

3. Marco normativo y documentos considerados

El Protocolo se funda en la legislación chilena vigente y en el proceso de adecuación al nuevo estándar de protección de datos personales. La Ley N° 19.628 regula el tratamiento de datos personales en registros o bancos de datos y reconoce categorías como datos personales, datos sensibles, comunicación, almacenamiento, bloqueo y eliminación. La Ley N° 21.719 modifica dicho régimen, regula la protección y tratamiento de datos personales, crea la Agencia de Protección de Datos Personales y contempla plena vigencia desde el 1 de diciembre de 2026. La Ley N° 21.663, Marco de Ciberseguridad, refuerza principios y requisitos para prevención, respuesta y gestión de incidentes de ciberseguridad.

También se consideran, cuando corresponda, el Código del Trabajo, la normativa de contratación pública aplicable al mandante, deberes de confidencialidad contractual, reglas de igualdad de oportunidades y no discriminación, y políticas internas de integridad, orden, compliance y uso de inteligencia artificial de Ossandón Auditores Consultores.

La interpretación operacional de este Protocolo debe favorecer el estándar más protector para el titular cuando existan dudas razonables sobre alcance, proporcionalidad o comunicación de información sensible.

4. Definiciones operativas

Concepto	Uso en este Protocolo
Dato personal	Información vinculada o referida a una persona natural identificada o identificable: nombre, RUN, correo, teléfono, CV, experiencia, referencias, evaluaciones psicolaborales y registros de entrevista.
Dato sensible	Información sobre salud, discapacidad, resultados psicológicos o psicométricos, datos biométricos, afiliaciones, creencias, vida privada u otros antecedentes protegidos por ley.
Tratamiento	Cualquier operación sobre datos: recolectar, registrar, almacenar, consultar, analizar, comunicar, transferir, bloquear, anonimizar o eliminar.
Base de licitud	Fundamento que autoriza el tratamiento: consentimiento, ejecución de contrato, medidas precontractuales, obligación legal, interés legítimo u otra causal prevista en la ley.
Minimización	Regla de recolectar y usar solo datos necesarios, adecuados y pertinentes para el cargo y el encargo.
Informe de selección	Documento que resume antecedentes relevantes para la decisión del cliente, competencias, categorías, evitando datos excesivos, irrelevantes o discriminatorios.

5. Principios de tratamiento

Principio	Aplicación práctica en selección
Licitud y lealtad	Todo dato tratado debe tener una finalidad legítima, informada y compatible con el proceso de selección.
Finalidad	Los datos se usan solo para evaluar idoneidad, gestionar comunicaciones, cumplir obligaciones y reportar al cliente.
Proporcionalidad	No se solicitan antecedentes excesivos ni ajenos al perfil del cargo.
Calidad	Los datos deben ser actuales y verificables; las inferencias deben distinguirse de hechos comprobados.
Responsabilidad	Cada profesional responde por el uso correcto de los datos bajo su custodia.
Seguridad	Se aplican controles técnicos y organizativos para evitar acceso indebido, pérdida o filtración.
Transparencia	El titular debe conocer quién trata sus datos, para qué, por cuánto tiempo y cómo ejercer derechos.
Confidencialidad	La información de candidatos, clientes y referencias es reservada y solo se comparte con personas autorizadas.

6. Ciclo de vida de los datos en selección

1. Apertura del encargo: Recepción del requerimiento, definir cargo, perfil, mandante, bases de licitud, información necesaria, equipo autorizado y herramientas a usar.

2. Atracción y recepción: Recibir CV por canales autorizados; informar finalidad, responsable, destinatarios, plazos y derechos.

3. Evaluación: Aplicar entrevistas y pruebas pertinentes. No efectuar consultas sobre vida privada no vinculadas al cargo.

4. Validación: Solicitar referencias o antecedentes adicionales solo con conocimiento/consentimiento del candidato o candidata cuando corresponda.

5. Reporte al cliente: Entregar informes proporcionales, objetivos y orientados al perfil; excluir datos sensibles innecesarios.

6. Cierre: Comunicar resultados cuando corresponda; archivar evidencia mínima; eliminar o anonimizar según plazo definido con cliente o por contrato. En caso de usar nubes, crear accesos únicos y acotados en tiempo.

7. Auditoría: Mantener trazabilidad de accesos, envíos, versiones de informes y autorizaciones relevantes.

7. Información sensible y reglas de uso

Regla central: la información sensible solo puede recolectarse si es estrictamente necesaria para determinar idoneidad de la persona postulante respecto al cargo, cumplir una exigencia legal o contractual legítima, o aplicar ajustes razonables, y siempre bajo un estándar reforzado de confidencialidad.

Tipo de información	Regla de uso
Salud, discapacidad o aptitud médica	No solicitar salvo exigencia legal, seguridad ocupacional, ajuste razonable o requerimiento del cargo. No incluir diagnóstico en informes si basta una conclusión funcional.
Pruebas psicológicas o psicométricas	Usar instrumentos pertinentes, aplicados por profesionales competentes. Reportar conclusiones laborales, no material bruto sensible.
Antecedentes penales o comerciales	Solicitar solo si la ley o naturaleza del cargo lo permite y exige. Validar pertinencia y proporcionalidad.
Datos familiares, creencias, afiliación, orientación sexual u opinión política	No preguntar ni registrar salvo mandato legal excepcional y justificado. Estos datos no deben incidir en recomendaciones.
Referencias laborales	Registrar información laboral verificable y pertinente; evitar comentarios subjetivos, discriminatorios o sobre vida privada.
Imágenes, videollamadas y grabaciones	No grabar entrevistas salvo necesidad justificada, información previa y autorización; conservar por plazo breve y controlado.

8. Consentimiento, información al titular y relación con clientes

Antes o al inicio del proceso de evaluación, el candidato debe recibir información clara sobre la identidad de Ossandón Auditores Consultores, finalidad del concurso, categorías de datos, destinatarios, eventual comunicación al cliente, plazo de conservación, posibilidad de futuras oportunidades si aplica, uso de herramientas tecnológicas y medio para ejercer derechos.

El consentimiento debe ser libre, específico, informado e inequívoco cuando sea la base de licitud aplicable, especialmente frente a datos sensibles, incorporación a bases para búsquedas futuras, grabaciones o transferencias no necesarias para el proceso principal.

En cada propuesta o contrato con clientes debe definirse el rol de las partes, deberes de confidencialidad, finalidad del tratamiento, datos que serán compartidos, canales seguros, plazos de conservación, manejo de solicitudes de titulares e instrucciones para eliminación o devolución al cierre.

El cliente solo recibirá la información necesaria para decidir la contratación. No debe recibir material bruto de pruebas, notas completas de entrevistas, datos médicos, información familiar o antecedentes no vinculados al perfil, salvo obligación legal o requerimiento estrictamente justificado.

9. Seguridad, acceso y herramientas digitales

- Usar cuentas corporativas, contraseñas robustas y autenticación multifactor cuando esté disponible.
- Guardar documentos en repositorios autorizados; evitar almacenamiento en dispositivos personales, correos personales o servicios no aprobados. Se dispone de plataforma institucional para el alojamiento de datos.
- Aplicar acceso por necesidad de conocer: solo integrantes del equipo asignado y responsables autorizados. Accesos controlados a carpetas con información. Distinción de accesos según nivel de responsabilidad.
- Enviar informes por canales seguros, con destinatarios verificados; evitar adjuntos masivos y usar enlaces con permisos restringidos cuando sea posible.
- Nombrar archivos sin exponer datos sensibles innecesarios y controlar versiones de informes.
- No descargar bases completas salvo necesidad operacional; eliminar copias temporales una vez terminada la tarea.
- Bloquear pantalla, proteger documentos impresos y destruir impresiones mediante medios seguros.
- Reportar de inmediato correos enviados por error, pérdida de dispositivos, accesos indebidos o exposición accidental.

10. Uso de plataformas, IA y decisiones automatizadas

Las herramientas digitales, sistemas de seguimiento de candidatos, evaluaciones en línea y soluciones de inteligencia artificial pueden usarse solo como apoyo operacional o analítico, conforme al Protocolo de IA de Ossandón Auditores Consultores y las instrucciones del cliente.

Queda prohibido ingresar datos personales o sensibles de candidatos en herramientas de IA públicas o no autorizadas. Si se utiliza una herramienta aprobada, debe verificarse su base contractual, confidencialidad, ubicación de datos, retención, seguridad y posibilidad de auditoría.

La IA no sustituye el juicio profesional. Toda recomendación, descarte o decisión relevante debe contar con revisión humana, criterios trazables y posibilidad de explicación. No deben usarse variables discriminatorias ni inferencias sobre salud, ideología, vida privada, orientación sexual, afiliación sindical, origen étnico u otros datos sensibles no pertinentes.

Cuando exista tratamiento automatizado, perfilamiento o apoyo algorítmico significativo, el titular deberá ser informado de forma comprensible sobre su existencia, finalidad y posibilidad de solicitar revisión humana o impugnar una decisión cuando corresponda.

11. Comunicación de datos, reportes y transferencias

La comunicación de datos al cliente se limita a candidatos presentados formalmente o a información agregada de gestión del proceso. Las nóminas preliminares, bases extensas o candidatos descartados no deben compartirse salvo instrucción documentada y proporcional.

Los informes deben enfocarse en competencias, experiencia, motivación, ajuste al perfil, disponibilidad y condiciones objetivas relevantes. Las opiniones deben fundamentarse en evidencia del proceso y redactarse con lenguaje respetuoso, no discriminatorio y verificable.

Los datos pueden ser comunicados a proveedores tecnológicos o evaluadores externos únicamente si actúan bajo instrucciones, confidencialidad, medidas de seguridad, contrato o acuerdo de tratamiento, y reciben solo los datos indispensables para su función.

Las transferencias internacionales o almacenamiento en nubes ubicadas fuera de Chile deben contar con garantías contractuales, medidas de seguridad y evaluación de pertinencia conforme a la normativa aplicable y al estándar contractual del cliente.

12. Conservación, eliminación y cierre del proceso

Categoría	Criterio de conservación
Postulantes no seleccionados	Conservar hasta 24 meses si existe consentimiento para futuras búsquedas; si no, eliminar o anonimizar al cierre del proceso o dentro del plazo contractual. Plazo sujeto a compromisos contractuales.
Seleccionado contratado	Conservar antecedentes necesarios para respaldo del servicio y obligaciones contractuales/legales, conforme al contrato con cliente.
Pruebas y notas internas	Conservar solo resultados o conclusiones necesarias. Evitar guardar material bruto por más tiempo del necesario. Plazo 24 meses.
Comunicaciones con referencias	Conservar registro resumido, pertinente y laboral. Eliminar antecedentes irrelevantes o de vida privada.
Copias temporales	Eliminar al terminar la tarea que las justificó.
Solicitudes de supresión	Bloquear o suspender tratamiento mientras se evalúa, responder en plazo y ejecutar eliminación si procede.

Los plazos anteriores son criterios operativos y pueden ajustarse por contrato, exigencia legal, auditoría, reclamación pendiente o instrucción del cliente, siempre respetando minimización y trazabilidad.

13. Derechos de titulares y gestión de solicitudes

Los titulares podrán solicitar información y acceso, rectificación, supresión, oposición, bloqueo, portabilidad y revisión humana frente a decisiones automatizadas cuando corresponda. Toda solicitud debe canalizarse al responsable interno designado y registrarse con fecha de recepción, identidad del solicitante, derecho invocado, proceso asociado, respuesta y medidas adoptadas.

El equipo no debe responder informalmente solicitudes complejas ni comprometer eliminación, entrega de informes o modificación de antecedentes sin validación interna. Si la solicitud afecta información entregada al cliente, Ossandón Auditores Consultores deberá coordinar la respuesta con el mandante según el contrato y la ley.

El plazo operativo de respuesta será de hasta 30 días corridos desde la recepción válida de la solicitud, salvo norma, contrato o procedimiento interno más exigente. Cuando se requiera verificar identidad, el plazo se contará desde que dicha verificación quede razonablemente satisfecha.

14. Incidentes, brechas y escalamiento

Constituye incidente cualquier pérdida, envío erróneo, acceso no autorizado, publicación indebida, robo, alteración, destrucción, malware, credenciales comprometidas o tratamiento no autorizado de datos personales o sensibles.

Frente a un incidente, el profesional debe: (1) contener el evento si es posible sin borrar evidencia; (2) avisar de inmediato a su jefatura, Compliance y soporte TI; (3) identificar datos y titulares afectados; (4) preservar registros; (5) evitar comunicaciones externas no autorizadas; y (6) colaborar en la evaluación de notificación al cliente, titulares y autoridad competente cuando corresponda.

La respuesta debe ser documentada, proporcional y orientada a reducir daño, recuperar control, corregir causas raíz y prevenir recurrencia.

15. Controles operativos y anexos

Checklist mínimo por proceso

Control	Sí/No	Observación
Encargo y perfil documentados		
Base de licitud identificada		
Aviso/consentimiento aplicado		
Equipo autorizado definido		
Canales de recepción y almacenamiento aprobados		
Pruebas e instrumentos justificados		
Informe revisado por proporcionalidad y no discriminación		
Envío al cliente por canal seguro		
Cierre y conservación/eliminación registrados		
Solicitudes o incidentes documentados		

16. Potenciales multas, sanciones y consecuencias por incumplimiento

Las infracciones a este Protocolo pueden generar consecuencias en tres planos: sanciones administrativas para la organización por incumplimientos a la normativa de protección de datos; medidas contractuales o reputacionales frente a clientes, candidatos o autoridades; y medidas disciplinarias internas para trabajadores o colaboradores que vulneren obligaciones de confidencialidad, seguridad, probidad o uso adecuado de tecnologías.

Los montos en UTM se informan como referencia normativa y deben calcularse al valor vigente de la UTM al momento de una eventual sanción. La aplicación concreta dependerá de la autoridad competente, gravedad del hecho, cantidad de titulares afectados, naturaleza de los datos, intencionalidad, reincidencia, medidas correctivas y antecedentes de cumplimiento.

16.1. Riesgo de multas administrativas en protección de datos personales

Tipo	Multa potencial	Ejemplos aplicables a selección	Respuesta esperada
Leve	Hasta 5.000 UTM	Incumplimientos formales o procedimentales: aviso de privacidad incompleto, registro interno insuficiente, falta de documentación de bases de licitud o conservación deficiente de evidencias.	Corregir documentación, reforzar checklist, capacitar al equipo y dejar trazabilidad de mejora.
Grave	Hasta 10.000 UTM	Tratamiento sin base de licitud suficiente, uso de datos para fines distintos al proceso, no responder derechos de titulares en plazo o no comunicar adecuadamente una brecha cuando proceda.	Activar revisión de Compliance, suspender tratamiento cuestionado, corregir flujos, notificar según corresponda y documentar medidas.
Gravísima	Hasta 20.000 UTM	Tratamiento de datos sensibles sin justificación legal; comunicación indebida de informes psicolaborales; filtración de CV, evaluaciones o antecedentes sensibles; transferencia internacional sin garantías; reincidencia en conductas graves.	Contención inmediata, investigación interna, comunicación al cliente, evaluación de notificación a autoridad/titulares, medidas disciplinarias y remediación.

Nota. Reincidencia y agravantes. Cuando exista reincidencia, daño relevante, afectación de datos sensibles, falta de cooperación, ausencia de medidas de seguridad, beneficio económico indebido o incumplimiento de medidas correctivas, la exposición sancionatoria puede aumentar dentro de los rangos legales. Todo evento relevante debe escalarse a Dirección y Compliance.

16.2. Medidas disciplinarias internas conforme a Normas de Orden y legislación laboral

Nivel interno	Ejemplos de conducta	Medidas posibles
Falta leve	Incumplimiento aislado sin afectación real de datos: error menor de clasificación, omisión de checklist o uso de formato no actualizado.	Retroalimentación, refuerzo de capacitación, amonestación verbal o medida correctiva documentada.
Falta grave	Enviar información a destinatario equivocado, almacenar CV en medios no autorizados, compartir informes fuera del equipo o usar IA no autorizada sin datos sensibles.	Amonestación escrita, restricción temporal de acceso, capacitación obligatoria, evaluación de multa interna conforme al Reglamento Interno y Código del Trabajo.
Falta muy grave	Divulgar datos sensibles, usar información de candidatos para fines personales, ocultar una brecha, alterar evaluaciones, usar datos para discriminar o ingresar información confidencial/sensible en plataformas no autorizadas.	Investigación interna, medidas de resguardo, denuncia por canales internos, posible multa laboral dentro del límite legal, término de contrato si la gravedad y la ley lo permiten, y acciones legales o contractuales pertinentes.

Nota. Límite legal de multas laborales. Cuando una infracción de un trabajador a las normas internas sea sancionada con multa, esta no podrá exceder de la cuarta parte de la remuneración diaria del infractor. Además, el trabajador podrá reclamar ante la Dirección del Trabajo que corresponda. La aplicación de sanciones debe respetar proporcionalidad, debido proceso interno, derecho a ser oído y registro de antecedentes, de acuerdo con las Normas de Orden de Ossandón Auditores Consultores.

16.3. Consecuencias contractuales, reputacionales y operativas

- Requerimientos de explicación, auditoría o plan de remediación por parte de clientes públicos o privados.
- Suspensión o término anticipado de servicios si el contrato o bases de licitación lo contemplan.
- Obligación de notificar a clientes, titulares o autoridad competente, según la naturaleza del incidente.
- Pérdida de confianza comercial, afectación reputacional, exclusión de futuras licitaciones o exigencia de controles reforzados.
- Eventuales acciones civiles, laborales, administrativas o penales si además existen daños, incumplimientos contractuales, falsificación, ocultamiento o uso indebido doloso de información.

Enfoque preventivo. La finalidad de esta sección no es punitiva, sino preventiva: fortalecer la cultura de integridad, confidencialidad, seguridad, diligencia profesional y mejora continua. La aplicación de sanciones internas debe ser proporcional, documentada y coherente con el Programa de Integridad y Compliance, las Normas de Orden y el Protocolo de IA de la Firma.

Fuentes normativas, bibliográficas y documentos de referencia

- Ley N° 19.628 sobre Protección de la Vida Privada / Protección de Datos de Carácter Personal.
- Ley N° 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.
- Ley N° 21.663, Ley Marco de Ciberseguridad.
- Código del Trabajo, artículo 157, sobre límites de multas laborales contenidas en reglamentos internos.
- Documentos internos considerados: Normas de Orden, Programa de Integridad y Compliance y Protocolo de Inteligencia Artificial de Ossandón Auditores Consultores. Disponibles para revisión y descarga en **www.oci.cl**

Protocolo de uso y resguardo de información sensible para procesos de reclutamiento y selección. 2026.