Lineamientos de Protección de Datos Personales
GRUPO STT PERU S.A.C.

1. ANTECEDENTES

GRUPO STT PERU S.A.C. (en adelante, la "Sociedad") es una sociedad dedicada a prestar servicios de actividades de consultoría de gestión y otras actividades profesionales, científicas y técnicas relacionadas principalmente al servicio de reclutamiento, administración de recursos humanos, manejo de planillas y otros. Nuestra Sociedad está comprometida con el cumplimiento de las normas peruanas y la protección de los derechos de todos los peruanos. En tal sentido, mediante la presente política, manifestamos nuestro compromiso con la protección de los datos personales a los que damos tratamiento, de conformidad con lo establecido en la Ley de Protección de Datos Personales, Ley Nº29733 y su Reglamento aprobado por D.S. Nº003-2013-JUS, modificada por el Decreto Legislativo Nº1353 y su Reglamento aprobado por el Decreto Supremo N° 019-2017-JUS (todo junto, así como las normas que de tiempo en tiempo las complementen, adicionen, modifiquen o supriman, en adelante "Ley"). En virtud de lo anterior, presentamos nuestros Lineamientos de Protección de Datos Personales.

2. ALCANCE

Los presentes Lineamientos de Protección de Datos Personales son aplicables a toda actividad que involucre el tratamiento de datos personales realizada por cualquiera de las áreas de GRUPO STT PERU S.A.C.

Estos Lineamientos son también aplicables a todas aquellas personas o empresas a las que GRUPO STT PERU S.A.C. por encargo requiera el tratamiento de datos personales de los cuales sea responsable.

3. OBJETO

Estos Lineamientos de Protección de Datos Personales, incluidos sus anexos, establecen las reglas para el tratamiento de datos personales que tienden a asegurar las condiciones de operación de los sistemas de información de la Sociedad en función de los principios rectores, a efectos de cumplir la Ley y, más allá de ello, ofrecer el nivel más adecuado de protección para los datos personales que tratamos.

Estos Lineamientos son de obligatorio cumplimiento para todos los miembros de la Sociedad, trabajadores, representantes, accionistas, etc., así como, para los proveedores de la Sociedad a los que se les encargue el tratamiento de los datos personales (Encargados de Tratamiento de Datos Personales).

4. DEFINICIONES

Autoridad Nacional de Protección de Datos Personales o Dirección General de Protección de Datos Personales, de manera indistinta. Es el órgano encargado de realizar todas las gestiones necesarias para el cumplimiento de la Ley. Se encuentra adscrita a la Dirección Nacional de Justicia del Ministerio de Justicia.

Banco de datos personales. Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

Datos personales. Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

Datos sensibles. Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

Encargado de tratamiento de datos personales. Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales.

Encargo de tratamiento. Entrega por parte del titular del banco de datos personales a un encargado de tratamiento de datos personales en virtud de una relación jurídica que los vincula. Dicha relación jurídica delimita el ámbito de actuación del encargado del tratamiento de los datos personales.

Flujo transfronterizo de datos personales. Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.

Nivel suficiente de protección para los datos personales. Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.

Procedimiento de anonimización. Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.

Procedimiento de disociación. Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible.

Titular de datos personales. Persona natural a quien corresponde los datos personales.

Titular del banco de datos personales. Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

Transferencia de datos personales. Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho

privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

Tratamiento de datos personales. Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

5. TITULAR DE LOS BANCOS DE DATOS PERSONALES

El titular de los bancos de datos personales que se detallan en el Anexo A, es:

GRUPO STT PERU S.A.C.
RUC Nº 20549951482.
Domicilio: Calle Alameda del Arco Iris, Tienda 7, Sotano N°118, Urb. La Alborada (Centro Comercial La Alborada), distrito de Santiago de Surco, provincia y departamento de Lima.
Responsable: Claudia Victoria Quiroz Condori
Teléfono: 00 506 72042822
Correo Electrónico: privacidadinformacion@grupostt.com

6. PRINCIPIOS RECTORES

La actuación de la Sociedad y de los eventuales encargados de tratamiento de datos personales y, en general, de todos los que intervengan con relación a los datos personales, debe ajustarse a los principios rectores que se listan a continuación:

Principio de legalidad. El tratamiento de los datos personales se hace conforme a lo establecido en la Ley. La Sociedad está prohibida de recopilar datos personales por medios fraudulentos, desleales o ilícitos.

Principio de consentimiento. Para poder tratar sus datos personales debemos tener su consentimiento libre, previo, expreso, informado e inequívoco.

Principio de finalidad. Los datos personales serán recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

Principio de proporcionalidad. Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

Principio de calidad. Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento. Se presume que los datos directamente facilitados por el titular de los mismos son exactos.

Principio de seguridad. La Sociedad deberá adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate (ver Sección 10).

En el tratamiento de los datos personales deben adoptarse las medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a la Ley, incluyéndose en ellos a la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Principio de disposición de recurso. Todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.

Principio de nivel de protección adecuado. Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por esta Ley o por los estándares internacionales en la materia.

7. DERECHOS DE LOS TITULARES DE DATOS PERSONALES

De acuerdo a Ley, los derechos de los titulares de los datos personales son los siguientes, y la Sociedad está obligada a velar por su cumplimiento:

Derecho a ser informado. A ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del o de los encargados del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello. En el consentimiento informado la Sociedad cumple con brindar esta información (ver sección 8 siguiente).

Si una vez obtenido su consentimiento la Sociedad establece vinculación con un encargado de tratamiento, el accionar del encargado queda bajo responsabilidad de la Sociedad y se le informará de manera oportuna.

Si con posterioridad al consentimiento se produce la transferencia de datos personales por fusión, o supuestos similares, el nuevo titular del banco de datos deberá establecer un mecanismo de información eficaz para el titular de los datos personales sobre dicho nuevo encargado de tratamiento.

Derecho de acceso. A obtener la información que sobre sí mismo sea objeto de tratamiento por la Sociedad, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos.

Derecho de actualización, inclusión, rectificación y supresión. A la actualización, inclusión, rectificación y supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento.

Si sus datos personales hubieran sido transferidos previamente, la Sociedad comunicará la actualización, inclusión, rectificación o supresión a quienes se hayan transferido, en el caso que se mantenga el tratamiento por este último, quien debe también proceder a la actualización, inclusión, rectificación o supresión.

Durante el proceso de actualización, inclusión, rectificación o supresión de datos personales, dispondremos el bloqueo de los datos, impidiendo que terceros accedan a ellos. Dicho bloqueo no es aplicable a las entidades públicas que requieren de tal información para el adecuado ejercicio de sus competencias.

Derecho a impedir el suministro. A impedir que estos sean suministrados, especialmente cuando ello afecte sus derechos fundamentales. El derecho a impedir el suministro no aplica para la relación entre el titular del banco de datos personales y la Sociedad para los efectos del tratamiento de estos.

Derecho de oposición. Siempre que, por ley, no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En caso de oposición justificada la Sociedad procederá a la supresión.

Derecho al tratamiento objetivo. A no verse sometido a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa, sustentada únicamente en un tratamiento de datos personales destinado a evaluar determinados aspectos de su personalidad o conducta, salvo que ello ocurra en el marco de la negociación, celebración o ejecución de un contrato o en los casos de evaluación con fines de incorporación a una entidad pública, de acuerdo a ley, sin perjuicio de la posibilidad de defender su punto de vista, para salvaguardar su legítimo interés.

Derecho a la tutela. En caso de que la Sociedad, a criterio del titular de los datos personales, haya denegado al titular de datos personales, total o parcialmente, el ejercicio de sus derechos, este puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de hábeas data.

Derecho a ser indemnizado. El titular de datos personales que considere que ha sido afectado porque la Sociedad ha incumplido la Ley tiene derecho a solicitar a la autoridad competente la indemnización correspondiente, conforme a ley.

8. CONSENTIMIENTO INFORMADO

La Sociedad obtendrá de manera previa al tratamiento de los datos personales, el consentimiento informado de los titulares de los datos personales, según los formatos contenidos en el Anexo B.

Los consentimientos deberán cumplir los siguientes requisitos:

Libre. Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales.

Previo. Con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron.

Expreso e Inequívoco. Cuando el consentimiento haya sido manifestado en condiciones que no admitan dudas de su otorgamiento.

La condición de expreso no se limita a la manifestación verbal o escrita. Tratándose del entorno digital, también se considera expresa la manifestación consistente en "hacer clic", "cliquear" o "pinchar", "dar un toque", "touch" o "pad" u otros similares.

Podrán otorgarse mediante texto preestablecido, fácilmente visible, legible y en lenguaje sencillo, que el titular pueda hacer suyo, o no, mediante una respuesta escrita, gráfica o mediante clic o pinchado.

Informado. Se debe informar al titular de los datos personales de manera clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos de lo siguiente:

a. La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos.
b. La finalidad o finalidades del tratamiento a las que sus datos serán sometidos.
c. La identidad de los que son o pueden ser sus destinatarios, de ser el caso.
d. La existencia del banco de datos personales en que se almacenarán, cuando corresponda.
e. El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso.
f. Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.
g. En su caso, la transferencia nacional e internacional de datos que se efectúen.

9. TRANSFERENCIA DE DATOS PERSONALES

En caso el titular de los datos personales lo haya autorizado expresamente, GRUPO STT PERU S.A.C. podrá transferir local e internacionalmente datos personales a empresas de su mismo grupo económico para que estos sean utilizados para elaborar estadísticas y/o estudios de comportamiento, evaluar la capacidad de los trabajadores y la productividad de la operación en el Perú. Asimismo, GRUPO STT PERU S.A.C. podrá transferir datos personales a entidades públicas legalmente facultadas dentro del ámbito de sus competencias en cumplimiento de normativa vigente o futura o por requerimiento de estas.

10. MEDIDAS DE SEGURIDAD

La Sociedad ha tomado las medidas de seguridad señaladas por la Ley para lograr el nivel suficiente de protección para los datos personales.

Las medidas de seguridad abarcan tanto aquellos datos que son tratados de manera automatizada como aquellos datos personales que son tratados de manera no automatizada.

En el Anexo C encontrarán detallado el Protocolo de Seguridad.

11. ANEXOS

Anexo A: Bancos de Datos Personales Registrados
Anexo B: Formatos de Consentimientos Informados
Anexo C: Protocolo de Seguridad
Anexo D: Procedimiento para ejercer los derechos del titular de los datos personales.

12. VIGENCIA

Esta Política rige a partir del 20 de diciembre de 2023. Esta Política y sus Anexos podrán ser revisados y actualizados periódicamente para ajustarlo al contexto corporativo de la Sociedad y a la Ley.

Anexo A
Bancos de Datos Personales Registrados

	Nombre	Área Responsable
1	Colaboradores Activos	Recursos Humanos
2	Colaboradores de Proyectos	Operaciones
3	Postulantes	Reclutamiento
4	Proveedores	Administración
5	Clientes	Gerencia
6	Potenciales Clientes	Gerencia

Anexo B
Formatos de Consentimientos Informados

CONSENTIMIENTO DE USO DE DATOS PERSONALES – BANCO DE DATOS DE COLABORADORES ACTIVOS

1	Identidad y domicilio:	GRUPO STT PERU S.A.C.; Calle Alameda del Arco Iris, Tienda 7, Sotano N°118, Urb. La Alborada (Centro Comercial La Alborada), Santiago de Surco; con RUC 20549951482.
2	Finalidad:	Usos obligatorios: cumplir con nuestras obligaciones como empleadores para asignar las labores que se le encarguen como trabajador; para la prevención de riesgos laborales; análisis de perfiles; seguridad y control de acceso a los edificios; actividades asociativas, culturales, recreativas y de deporte; y auditorias laborales, exámenes médicos ocupacionales. Usos opcionales: su imagen podrá ser usada, libre de regalías, para: uso interno en memorias y manuales de GRUPO STT PERU S.A.C. y para la difusión de actividades y eventos de GRUPO STT PERU S.A.C., para publicitar sus servicios, a través de páginas web y redes sociales de GRUPO STT PERU S.A.C. y en documentos y material gráfico (como afiches, folletos u otros). Asimismo, los datos sobre sus hijos(as) podrán ser usados para actividades de bienestar.
3	Datos personales:	Recopilamos los siguientes datos personales: nombre y apellidos, documento de identidad, imagen, dirección, estado civil, tipo de sangre, rango generacional, títulos académicos, teléfono, nombre y edad de los hijos.
4	Consecuencias autorizar o no los usos de sus datos personales:	De no proporcionar esta autorización para los usos obligatorios de sus datos personales, no podrá seguir colaborando con nosotros ya que nos veríamos impedidos de cumplir con nuestras obligaciones legales como empleadores. De no prestar su autorización para los usos opcionales, continuará siendo un valorado trabajador de GRUPO STT PERU S.A.C.
5	Transferencias nacionales:	Cuando el trabajador solicita un crédito o servicio financiero y da como referencia a GRUPO STT PERU S.A.C., GRUPO STT PERU S.A.C. en respuesta al requerimiento de la entidad financiera proporcionará la información solicitada de los datos personales. Para consulta de requisitorias, antecedentes policiales, judiciales, en materia penal, civil, laboral, familiar, fiscalía, INPE, y récord crediticio. Cuando los trabajadores deban viajar en cumplimiento de sus obligaciones laborales GRUPO STT PERU S.A.C. al momento de contratar el transporte y el hospedaje transferirá los datos personales del personal a las empresas proveedoras que se contraten. El trabajador será informado de la empresa en cuestión. GRUPO STT PERU S.A.C. en cumplimiento de sus obligaciones legales, en caso así requerirlo la legislación vigente podrá transferir sus datos personales a la administración tributaria, ONP, AFPs, entidades de salud, seguro social, empresa de seguros, Registros Públicos u otra entidad pública. GRUPO STT PERU S.A.C. También podrá transferir sus datos personales a sus abogados externos (Estudio Aurelio Garcia Sayán – Abogados S.Civ.R.L.) y auditores.

		Se podrá encargar el tratamiento de sus datos personales a empresas que realicen pruebas psicométricas.
6	Transferencias internacionales:	STT GROUP DE CR S.A., STT GROUP CHILE SPA y STT GROUP SUCURSAL COLOMBIA S.A. (SUCURSAL DE STT), empresas del mismo grupo empresarial localizadas en Costa Rica y Colombia respectivamente para fines estadísticos y de reporte. Por el tipo de organización de GRUPO STT PERU S.A.C., el personal reporta a Coordinadora de Recursos Humanos, quien supervisa a la subsidiaria peruana, por lo que ésta podrá tener acceso a la información con la misma finalidad declarada en el punto 2.
7	Banco de Datos:	La información será almacenada en el Banco de Datos de "Colaboradores Activos" inscrito en el Registro Nacional de Protección de Datos Personales con el código RNPDP-PJP N°26913.
8	Tiempo de conservación:	Los datos serán conservados hasta que sea retirado el consentimiento por parte del titular de los datos personales
9	Ejercicio de los derechos ARCO:	Puede ejercer los derechos de acceso, rectificación, cancelación y oposición, así como revocar su consentimiento para las finalidades no necesarias para la ejecución de la relación contractual, a través del correo electrónico privacidadinformacion@grupostt.com o en nuestras oficinas ubicadas en la dirección señalada líneas arriba. De considerar que no ha sido atendido en el ejercicio de sus derechos puede presentar una reclamación ante la Autoridad Nacional de Protección de Datos Personales, dirigiéndose a la Mesa de Partes del Ministerio de Justicia y Derechos Humanos.

Doy mi consentimiento para los usos obligatorios y opcionales: □
Doy mi consentimiento sólo para los usos obligatorios: □

Firma:_____

Nombres y Apellidos: _____
DNI N°_____

CONSENTIMIENTO DE USO DE DATOS PERSONALES – BANCO DE DATOS DE COLABORADORES DE PROYECTOS

1	Identidad y domicilio:	GRUPO STT PERU S.A.C.; Calle Alameda del Arco Iris, Tienda 7, Sotano N°118, Urb. La Alborada (Centro Comercial La Alborada), Santiago de Surco; con RUC 20549951482.
2	Finalidad:	Usos obligatorios: cumplir con nuestras obligaciones como empleadores, para asignar las labores que se le encarguen como trabajador; para la prevención de riesgos laborales; análisis de perfiles; seguridad y control de acceso a los edificios; actividades asociativas, culturales, recreativas y de deporte; y auditorias laborales, exámenes médicos ocupacionales; para gestionar su ingreso a las instalaciones de nuestros clientes; para apertura de cuenta sueldo o cuenta CTS. Usos opcionales: sus imágenes podrán ser usadas, libre de regalías, para: uso interno en memorias y manuales de GRUPO STT PERU S.A.C. y para la difusión de actividades y eventos de GRUPO STT PERU S.A.C., para publicitar sus servicios, a través de páginas web y redes sociales de GRUPO STT PERU S.A.C. y en documentos y material gráfico (como afiches, folletos u otros).
3	Datos personales:	Recopilamos los siguientes datos personales: nombre completo, DNI, fecha de nacimiento, domicilio, datos académicos, número de teléfono, imagen, correo electrónico. De sus hijos: nombre completo, fecha de nacimiento, copia del DNI de los hijos. De su cónyuge o conviviente: nombre completo, fecha de nacimiento, DNI y partida de matrimonio.
4	Consecuencias autorizar o no los usos de sus datos personales:	De no proporcionar esta autorización para los usos obligatorios, no se podrá continuar como colaboradora de GRUPO STT PERÚ S.A.C. De no prestar su autorización para los usos opcionales, podrá ser un colaborador nuestro y se tomará nota de su decisión para futuras solicitudes.
5	Transferencias nacionales:	Cuando el colaborador solicita un crédito o servicio financiero y da como referencia a GRUPO STT PERU S.A.C., GRUPO STT PERU S.A.C. En respuesta al requerimiento de la entidad financiera proporcionará la información solicitada de los datos personales. Para consulta de requisitorias, antecedentes policiales, judiciales, en materia penal, civil, laboral, familiar, fiscalía, INPE, y récord crediticio. Cuando los Colaboradores de Proyectos deban viajar en cumplimiento de sus obligaciones laborales GRUPO STT PERU S.A.C. al momento de contratar el transporte y el hospedaje transferirá los datos personales del personal a las empresas proveedoras que se contraten. El colaborador será informado de la empresa en cuestión. GRUPO STT PERU S.A.C. en cumplimiento de sus obligaciones legales, en caso así requerirlo la legislación vigente podrá transferir sus datos personales a la administración tributaria, ONP, AFPs, entidades de salud, seguro social, empresa de seguros, Registros Públicos u otra entidad pública. GRUPO STT PERU S.A.C. también podrá transferir sus datos personales a sus abogados externos (Estudio Aurelio Garcia Sayán – Abogados S.Civ.R.L.) y auditores.

		GRUPO STT PERU S.A.C. también podrá transferir sus datos personales a aseguradoras (seguros de viaje, seguro de vida ley, seguro SCTR, EPS). GRUPO STT PERU S.A.C. también podrá transferir sus datos personales para apertura de cuenta sueldo o cuenta CTS. Se podrá encargar el tratamiento de sus datos personales a empresas que presten servicios de exámenes médicos ocupacionales, sean pública o privadas. A los clientes de GRUPO STT PERU S.A.C., cuando por obligación contractual con los clientes de GRUPO STT PERU S.A.C. deban compartirse datos personales de los trabajadores de GRUPO STT PERU S.A.C. que ejecutan el servicio, ya sea para un control interno del cliente o por una auditoría propia del servicio.
6	Transferencias internacionales:	STT GROUP DE CR S.A., STT GROUP CHILE SPA y STT GROUP SUCURSAL COLOMBIA S.A. (SUCURSAL DE STT) empresa del mismo grupo empresarial localizada en Colombia para fines estadísticos y de reporte. Por el tipo de organización de GRUPO STT PERU S.A.C., el personal reporta a una gerencia en Colombia por lo que ésta tendrá el mismo acceso a la información y para la finalidad declarada en el punto 2.
7	Banco de Datos:	La información será almacenada en el Banco de Datos de "Colaboradores de Proyectos" inscrito en el Registro Nacional de Protección de Datos Personales con el código RNPDP-PJP N°26915.
8	Tiempo de conservación:	Los datos serán conservados mientras dure la relación contractual, posteriormente a la misma, se conservarán los datos por diez (10) años
9	Ejercicio de los derechos ARCO:	Puede ejercer los derechos de acceso, rectificación, cancelación y oposición, así como revocar su consentimiento para las finalidades no necesarias para la ejecución de la relación contractual, a través del correo electrónico privacidadinformacion@grupostt.com o en nuestras oficinas ubicadas en la dirección señalada líneas arriba. De considerar que no ha sido atendido en el ejercicio de sus derechos puede presentar una reclamación ante la Autoridad Nacional de Protección de Datos Personales, dirigiéndose a la Mesa de Partes del Ministerio de Justicia y Derechos Humanos.

Doy mi consentimiento para los usos obligatorios y opcionales: □
Doy mi consentimiento sólo para los usos obligatorios: □

Firma:_____

Nombres y Apellidos: _____
DNI N°_____

CONSENTIMIENTO DE USO DE DATOS PERSONALES – BANCO DE DATOS DE POSTULANTES

1	Identidad y domicilio:	GRUPO STT PERU S.A.C.; Calle Alameda del Arco Iris, Tienda 7, Sótano N°118, Urb. La Alborada (Centro Comercial La Alborada), Santiago de Surco; con RUC 20549951482.
2	Finalidad:	Usos obligatorios: Los datos que son recopilados a través de su CV o facilitados por usted durante el proceso de selección serán tratados con el fin de valorar su candidatura para vacantes actuales o futuras a cubrir en GRUPO STT PERU S.A.C., subsidiarias y/o sus clientes, en el Perú o en el extranjero Sus datos personales serán usados para implementar, a su solicitud, medidas precontractuales entre usted y GRUPO STT PERU S.A.C. subsidiarias y/o sus clientes en el Perú o en el extranjero, como, por ejemplo, dar inicio y seguimiento al proceso de selección, evaluar su solicitud, negociar su contrato, recolectar y verificar sus antecedentes y referencias, solicitar exámenes psicotécnicos y exámenes médicos pre-ocupacionales para verificar si es apto para el puesto para el que se le está contratando, entre otros. El tratamiento de sus datos personales es necesario para la preparación, y posible celebración y ejecución de una relación contractual en la que usted, titular de datos personales, será parte.
3	Datos personales:	Recopilamos los siguientes datos personales: nombre completo, DNI, número teléfono, correo electrónico, dirección de domicilio, fecha de nacimiento, estado civil, con/sin hijos, y demás información que usted nos envió al estar incluida en su CV.
4	Consecuencias autorizar o no los usos de sus datos personales:	De no proporcionar esta autorización para los usos obligatorios de sus datos personales, no podrá participar en los procesos de selección de GRUPO STT PERU S.A.C.
5	Transferencias nacionales:	Cualquier autoridad peruana según requerimiento cuando las normas legales así lo exijan. Para consulta de requisitorias, antecedentes policiales, judiciales, en materia penal, civil, laboral, familiar, fiscalía, INPE, y récord crediticio. A cualesquiera de nuestros clientes locales que solicitan el servicio de contratación de personal y a clínicas de medicina ocupacional en las cuales el postulante deba rendir el examen preocupacional; el de evaluación de competencias mediante herramientas como Psicoweb, Inglés Futura, Amitai, u otro proveedor que preste servicios similares para que realicen su evaluación de competencias y pruebas psicotécnicas (en adelante, los "Encargados del Tratamiento"). Asimismo, nos autoriza para que una vez realizada su evaluación de competencias los Encargados del Tratamiento nos envíen los resultados a efectos de que podamos verificar su aptitud para el puesto. Su historia médica quedará en custodia del Encargado del Tratamiento que le realice las pruebas. A los clientes de GRUPO STT PERU S.A.C., cuando por obligación contractual con los clientes de GRUPO STT PERU S.A.C. deban compartirse datos personales de los posibles trabajadores de GRUPO STT PERU S.A.C. que ejecutarán el servicio.
6	Transferencias internacionales:	STT GROUP DE CR S.A., STT GROUP CHILE SPA y STT GROUP SUCURSAL COLOMBIA S.A. (SUCURSAL DE STT) empresas del mismo grupo empresarial localizadas en Colombia y Chile, para fines estadísticos y de reporte. Por el tipo de organización de GRUPO STT PERU S.A.C., la información de los postulantes se reporta a un Coordinador de Filial Colombia, quien supervisa a la subsidiaria

		peruana, por lo que ésta podrá hacer el mismo tratamiento declarado den el Punto 2. Finalidad.
7	Banco de Datos:	La información será almacenada en el Banco de Datos de "Postulantes" inscrito en el Registro Nacional de Protección de Datos Personales con el código RNPDP-PJP N°26916.
8	Tiempo de conservación:	Los datos personales serán almacenados hasta que sea retirado el consentimiento por parte del titular de los datos personales, y se le podrá convocar a otro proceso de selección en el que su perfil sea coincidente.
9	Ejercicio de los derechos ARCO:	Puede ejercer los derechos de acceso, rectificación, cancelación y oposición, así como revocar su consentimiento para las finalidades no necesarias para la ejecución de la relación contractual, a través del correo electrónico privacidadinformacion@grupostt.com o en nuestras oficinas ubicadas en la dirección señalada líneas arriba. De considerar que no ha sido atendido en el ejercicio de sus derechos puede presentar una reclamación ante la Autoridad Nacional de Protección de Datos Personales, dirigiéndose a la Mesa de Partes del Ministerio de Justicia y Derechos Humanos.

Doy mi consentimiento sólo para los usos obligatorios: □

Firma:_____

Nombres y Apellidos: _____
DNI N°_____

CONSENTIMIENTO DE USO DE DATOS PERSONALES – BANCO DE DATOS DE PROVEEDORES

1	Identidad y domicilio:	GRUPO STT PERU S.A.C.; Calle Alameda del Arco Iris, Tienda 7, Sotano N°118, Urb. La Alborada (Centro Comercial La Alborada), Santiago de Surco; con RUC 20549951482.
2	Finalidad:	Usos obligatorios: Los datos personales que son recopilados son facilitados por usted durante el proceso de contratación, ya sea por correo electrónico, en entrevistas o en su propuesta de servicios, serán tratados con el fin de cumplir con nuestras obligaciones como comitentes; para asignar los encargos; para la prevención de riesgos; análisis de perfiles; para coordinar su ingreso a las instalaciones de nuestros clientes. El tratamiento de sus datos personales es necesario para la preparación, y ejecución de una relación contractual en la que usted, titular de datos personales, será parte.
3	Datos personales:	Recopilamos los siguientes datos personales: nombre completo, DNI, RUC, cargo en su puesto de trabajo, correo electrónico. dirección.
4	Consecuencias autorizar o no los usos de sus datos personales:	De no proporcionar esta autorización para los usos obligatorios de sus datos personales, no podrá ser un proveedor de GRUPO STT PERU S.A.C.
5	Transferencias nacionales:	A cualquier autoridad peruana según requerimiento cuando las normas legales así lo exijan. En cumplimiento de sus obligaciones legales podrá transferir sus datos personales a la administración tributaria.
6	Transferencias internacionales:	STT GROUP DE CR S.A., empresa del mismo grupo empresarial localizada en Costa Rica para fines estadísticos y de reporte. Por el tipo de organización de GRUPO STT PERU S.A.C., el personal reporta a una Gerencia localizada en Costa Rica por lo que ésta podrá hacer uso de la información con los mismos fines declarados en el Punto 2.
7	Banco de Datos:	La información será almacenada en el Banco de Datos de "Proveedores" inscrito en el Registro Nacional de Protección de Datos Personales con el código RNPDP-PJP N°26917.
8	Tiempo de conservación:	Los datos personales serán conservados mientras dure la relación contractual, posteriormente a la misma, se conservarán los datos personales hasta que revoque su consentimiento para posibles futuros encargos.
9	Ejercicio de los derechos ARCO:	Puede ejercer los derechos de acceso, rectificación, cancelación y oposición, así como revocar su consentimiento para las finalidades no necesarias para la ejecución de la relación contractual, a través del correo electrónico privacidadinformacion@grupostt.com o en nuestras oficinas ubicadas en la dirección señalada líneas arriba. De considerar que no ha sido atendido en el ejercicio de sus derechos puede presentar una reclamación ante la Autoridad Nacional de Protección de Datos Personales, dirigiéndose a la Mesa de Partes del Ministerio de Justicia y Derechos Humanos.

Doy mi consentimiento solo para los usos obligatorios: □

Firma:_____

Nombres y Apellidos: _____
DNI N°_____

CONSENTIMIENTO DE USO DE DATOS PERSONALES – BANCO DE DATOS DE CLIENTES

1	Identidad y domicilio:	GRUPO STT PERU S.A.C.; Calle Alameda del Arco Iris, Tienda 7, Sótano N°118, Urb. La Alborada (Centro Comercial La Alborada), Santiago de Surco; con RUC 20549951482.
2	Finalidad	Usos obligatorios: Gestionar y ejecutar sus pedidos o encargos como cliente nuestro. Usos opcionales: Perfilamiento para ofrecerle otros servicios que ofrece GRUPO STT PERU S.A.C.; y envío de información comercial respecto de servicios de GRUPO STT PERU S.A.C., subsidiarias y afiliadas.
3	Datos personales:	Recopilamos los siguientes datos personales: nombre y apellidos, DNI, correo electrónico, teléfono celular, fecha de nacimiento, RUC.
4	Consecuencias autorizar o no los usos de sus datos personales:	De no proporcionar esta autorización para los usos obligatorios, no podremos prestarle los servicios que requiere. De no prestar la autorización para los usos opcionales, continuaremos prestando servicios con la calidad de siempre pero no recibirá información sobre promociones que podrían serle beneficiosas.
5	Transferencias nacionales:	Administración Pública en los casos que así se requiera de acuerdo con la legislación vigente.
6	Transferencias internacionales:	A STT GROUP DE CR S.A., para fines estadísticos y de reporte. Por el tipo de organización de GRUPO STT PERU S.A.C., el personal reporta a un coordinador local y otro regional localizado en Costa Rica, quién supervisa a la subsidiaria peruana, por lo que ésta podrá tener el mismo acceso a los datos personales los cuáles serán utilizados para la misma finalidad declarada en el Punto 2.
7	Banco de Datos:	La información será almacenada en el Banco de Datos de “Clientes” inscrito en el Registro Nacional de Protección de Datos Personales con el código RNPDP-PJP N°26914.
8	Tiempo de conservación:	Los datos personales serán conservados mientras dure la relación contractual, posteriormente a la misma, se conservarán los datos personales para acciones promocionales hasta que revoque su consentimiento.
9	Ejercicio de los derechos ARCO:	Puede ejercer los derechos de acceso, rectificación, cancelación y oposición, así como revocar su consentimiento para las finalidades no necesarias para la ejecución de la relación contractual, a través del correo electrónico privacidadinformacion@grupostt.com o en nuestras oficinas ubicadas en la dirección señalada líneas arriba. De considerar que no ha sido atendido en el ejercicio de sus derechos puede presentar una reclamación ante la Autoridad Nacional de Protección de Datos Personales, dirigiéndose a la Mesa de Partes del Ministerio de Justicia y Derechos Humanos.

Doy mi consentimiento para los usos obligatorios y opcionales: □
Doy mi consentimiento sólo para los usos obligatorios: □

Firma:_____

Nombres y Apellidos: _____
DNI N°_____

CONSENTIMIENTO DE USO DE DATOS PERSONALES – BANCO DE DATOS DE POTENCIALES CLIENTES

1	Identidad y domicilio:	GRUPO STT PERU S.A.C.; Calle Alameda del Arco Iris, Tienda 7, Sotano N°118, Urb. La Alborada (Centro Comercial La Alborada), Santiago de Surco; con RUC 20549951482.
2	Finalidad:	Usos obligatorios: Gestionar las peticiones del potencial cliente a GRUPO STT PERU S.A.C., ya sean solicitar un servicio, información sobre servicios, sugerencias y/o reclamos. Usos opcionales: Perfilamiento para ofrecerle otros servicios de GRUPO STT PERU S.A.C.; y envío de información comercial respecto de los servicios de GRUPO STT PERU S.A.C.
3	Datos personales:	Recopilamos los siguientes datos personales: nombre y apellidos, DNI, correo electrónico, teléfono celular, fecha de nacimiento.
4	Consecuencias autorizar o no los usos de sus datos personales:	De no proporcionar esta autorización para los usos obligatorios, la Sociedad no podrá atender su requerimiento. De no prestar la autorización para los usos opcionales, atenderemos su requerimiento, pero no recibirá información sobre promociones que podrían serle beneficiosas.
5	Transferencias nacionales:	Administración Pública en los casos que así se requiera de acuerdo con la legislación vigente.
6	Transferencias internacionales:	STT GROUP DE CR S.A., STT GROUP CHILE SPA y STT GROUP SUCURSAL COLOMBIA S.A. (SUCURSAL DE STT), empresas del mismo grupo empresarial localizadas en Costa Rica y Colombia respectivamente para fines estadísticos y de reporte. Por el tipo de organización de GRUPO STT PERU S.A.C., el personal reporta a una coordinación local y otra regional, quien supervisa a la subsidiaria peruana, por lo que ésta podrá tener acceso a los datos personales con la misma finalidad que la declarada en el Punto 2.
7	Banco de Datos:	La información será almacenada en el Banco de Datos de "Potenciales Clientes" inscrito en el Registro Nacional de Protección de Datos Personales con el código RNPDP-PJP N°26917.
8	Tiempo de conservación:	Hasta que revoque su consentimiento.
9	Ejercicio de los derechos ARCO:	Puede ejercer los derechos de acceso, rectificación, cancelación y oposición, así como revocar su consentimiento para las finalidades no necesarias para la ejecución de la relación contractual, a través del correo electrónico privacidadinformacion@grupostt.com o en nuestras oficinas ubicadas en la dirección señalada líneas arriba. De considerar que no ha sido atendido en el ejercicio de sus derechos puede presentar una reclamación ante la Autoridad Nacional de Protección de Datos Personales, dirigiéndose a la Mesa de Partes del Ministerio de Justicia y Derechos Humanos.

Doy mi consentimiento para los usos obligatorios y opcionales: □
Doy mi consentimiento sólo para los usos obligatorios: □

Firma:_____

Nombres y Apellidos: _____
DNI N°_____

Anexo C
Protocolo de Seguridad

I. Antecedentes:

El presente documento explica las medidas de seguridad implementadas por GRUPO STT PERU S.A.C. (en adelante, la "Sociedad") para cumplir con la Ley de Protección de Datos Personales, Ley Nº 29733 y su Reglamento aprobado por D.S. Nº 003-2013-JUS, modificada por el Decreto Legislativo N° 1353 y su Reglamento aprobado por el Decreto Supremo N° 019-2017-JUS (todo junto, así como las normas que de tiempo en tiempo las complementen, adicionen, modifiquen o supriman, en adelante "Ley"), que conforman el Protocolo de Seguridad (en adelante, el "Protocolo").

El Protocolo se ajusta a la naturaleza jurídica de la Sociedad, a sus necesidades específicas en relación con su operación y tamaño, a la clase de datos personales objeto de tratamiento, al tipo de tratamiento, y a los riesgos potenciales que pueden derivar del tratamiento para salvaguardar los derechos de los titulares de los datos personales.

Para responder tanto ante la Autoridad Nacional de Protección de Datos Personales (en adelante, la "Autoridad"), como ante los titulares de los datos personales sobre el adecuado tratamiento de los mismos, la Sociedad cuenta con una estructura administrativa proporcional a su estructura empresarial y ha adoptado e implementado las políticas de medidas de seguridad consistentes con la Ley. Asimismo, la Sociedad adoptó los mecanismos internos para la ejecución de las referidas políticas a lo largo de toda su estructura, incluyendo herramientas de implementación, entrenamiento y protocolos de educación para su personal y la adopción de procedimientos para atender y dar respuesta a consultas, peticiones, y reclamos de los titulares de datos personales en relación con el tratamiento de los mismos.

Asimismo, la Sociedad entiende que la protección de datos personales no se limita a formular enunciados, sino que es una actividad que requiere atención constante con el fin de ofrecer y demostrar un adecuado tratamiento de los datos personales tanto al titular de los mismos como a la Autoridad.

Finalmente, el presente Protocolo, que principalmente es una herramienta de consulta interna, detallan de manera específica los protocolos de tratamiento de los datos personales y las medidas de seguridad implementadas por la Sociedad.

II. Asignación de Recursos:

La Sociedad ha implementado las medidas de seguridad para la protección de datos personales, conforme a las necesidades tanto a nivel corporativo como normativo. En tal sentido, la Sociedad ha venido destinando recursos humanos, físicos, tecnológicos, y presupuestarios para facilitar un adecuado tratamiento de los datos personales.

En consecuencia, la Sociedad continuará proporcionando los recursos mencionados en función de sus necesidades, siendo plenamente consciente que desde el punto de vista regulatorio el nivel de exigencias por la Autoridad ha venido evolucionando. Mediante la adopción de este Protocolo, se busca un manejo articulado de todo lo relacionado a la

protección de datos personales, y la Sociedad reafirma su compromiso de destinar los recursos necesarios para cumplir en todo momento con lo establecido en la Ley.

III. Responsable del Tratamiento de los Datos Personales:

La Sociedad nombra como responsable global del tratamiento de los datos personales (en adelante, el Responsable), al: Gerente de Ética y Cumplimiento Regulatorio, Claudia Victoria Quiroz Condori.

El Responsable del tratamiento de los datos personales, asume la responsabilidad en el interior de la Sociedad de velar por el cumplimiento de este Protocolo, así como atender las solicitudes y/o reclamos de los titulares, y establecer responsabilidades con las demás personas y áreas de la Sociedad, dependiendo del grado de manejo que puedan tener sobre los datos personales.

En términos, generales, el Responsable del tratamiento de los datos personales asume las siguientes responsabilidades:

- Estructurar, diseñar y administrar el Protocolo, el cual permite administrar los potenciales riesgos que puedan derivar del tratamiento de los datos personales. Asimismo, mantener el Protocolo actualizado, adoptando los cambios que sean necesarios.

- Realizar las funciones de enlace entre las distintas áreas de la Sociedad y coordinar todas las actividades relativas a la protección de datos personales.

- Mantener el inventario de los bancos de datos personales y velar por su actualización.

- Registrar los bancos de datos personales ante la Autoridad, para lo cual podrá solicitar el apoyo del área especializada.

- Revisar que en los casos de flujo transfronterizo de los datos personales se celebren los contratos necesarios con los encargados no domiciliados en el Perú que reciban tales datos personales.

- Coordinar capacitaciones del personal de la Sociedad en relación a la protección de datos personales. Requerir que, dentro de los análisis de desempeño del personal, los empleados hayan cumplido satisfactoriamente con el entrenamiento sobre protección de datos personales.

- Atender requerimientos y fiscalizaciones de la Autoridad.

- Evaluar y revisar periódicamente el Protocolo y adecuarlo a los cambios que se produzcan al interior de la Sociedad.

- Informar anualmente a los directivos de la Sociedad sobre la situación de la implementación del Protocolo.

- Las demás responsabilidades que por la naturaleza de la función le corresponda asumir.

IV. Gestión de Riesgos:

Las evaluaciones, revisiones y detección de eventuales riesgos en las medidas de seguridad asociados al tratamiento de los datos personales deben ocasionar la actualización del Protocolo, el mismo que debe corresponder y adecuarse a las últimas amenazas y riesgos detectadas en las medidas de seguridad implementadas para los bancos de datos personales.

V. Medidas de Seguridad Implementadas:

V.1. Medidas de Seguridad relacionadas a bancos de datos personales no automatizados:

a. Los bancos de datos personales de la Sociedad estarán protegidos contra acceso físico no autorizado mediante mecanismos de bloqueo físico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados. En tal sentido, los archivadores que están en un cuarto de la oficina de la Sociedad deberán tener una llave la misma que estará bajo custodia del Gerente de la Filial en toda oportunidad. Será su responsabilidad garantizar que solo personal autorizado por la Sociedad con privilegios suficientes tenga acceso a los documentos que contengan datos personales.

b. Todo traslado de datos personales hacia lugares fuera de los ambientes en donde se ubica el banco de datos personales deberá contar con autorización escrita del Gerente de la Filial, pudiendo ser otorgada por e-mail.

c. Al momento del traslado de los datos personales en soporte físico, deben estar en un contenedor que evite su acceso y legibilidad por terceras personas, y el contenedor debe contar con un mecanismo de verificación de no vulneración del mismo, como grapas o pegado. Los documentos originales deberán ser devueltos a su lugar de almacenamiento lo antes posible y se deberá confirmar dicha devolución al Gerente de la Filial.

d. El personal de la Sociedad que por sus funciones maneje base de datos personales, será responsable de generar y/o eliminar las copias o reproducciones de los datos personales de acuerdo con los siguientes lineamientos:

    - Utilizar impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados por la Sociedad.
    - Supervisar el proceso de copia o reproducción de los documentos. No dejar desatendido el equipo.
    - Retirar los documentos originales y las copias del equipo inmediatamente después de finalizada la copia o reproducción.
    - Siempre eliminar los documentos conteniendo los datos personales mediante el uso de la máquina trituradora de papel.

e. Todo banco de datos personales no automatizado deberá mantener los datos personales independizados de forma individual, de modo que pueda referirse

inequívocamente a un titular de datos personales sin exponer la información de otro titular.

f. Se deberá restringir el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales salvo autorización del Gerente de la Filial.

V.2. Medidas de Seguridad relacionadas a bancos de datos personales automatizados:

1. Banco de Datos "Colaboradores Activos":

a. El banco de datos personales se registra usando el software en la nube que almacena base de datos alojada en la nube (Google Drive).

b. El servidor se encuentra en un Data Center que cuenta con sistema de enfriamiento, control de acceso, sistema contra incendios.

c. Se podrá acceder al banco de datos personales en función a los siguientes niveles de privilegio (datos a tratar o tarea a realizar):

- Usuarios tipo 1: personal del área de Reclutamiento y Ética y Cumplimiento Regulatorio.
  Privilegios: solo ingreso de datos y lectura.

- Usuario Administrador: personal del área de Recursos Humanos.
  Privilegios: ingreso de datos, edición, eliminar, grabar, lectura.

- Todos los Usuarios está prohibido de imprimir documentos que contengan datos personales o de grabar los mismos en dispositivo removibles, salvo que sean parte necesario del desarrollo de su trabajo.

d. Anualmente, se revisarán los privilegios de acceso a los bancos de datos personales que correspondan al personal autorizado de la Sociedad. Esta revisión deberá constar en un acta que debidamente firmada será archivada.

e. El personal de la Sociedad autorizado con privilegios suficientes para tener acceso a los bancos de datos personales, contará con una contraseña que le permitirá acceder al banco de datos personales en función a sus privilegios.

f. Medidas de seguridad para el uso de contraseñas:

- El personal autorizado de la Sociedad debe mantener en secreto las contraseñas que les han sido asignadas.
- Cuando se utilice un servidor de autenticación, este debe almacenar las contraseñas de manera cifrada.
- Permitir que el personal autorizado de la Sociedad cambie la contraseña asignada cuando lo considere necesario, debiendo hacerlo cuando mínimo cada tres (3) meses.

- Requerir el uso de contraseñas que contengan al menos ocho (8) dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial.
- El acceso al sistema en entornos públicos (intranet, internet o similares) se bloquea temporalmente luego de seis (6) intentos fallidos de autenticación consecutivos. Es decir, en caso de ingresar la contraseña de manera errónea seis (6) veces consecutivas, el sistema bloqueará el acceso por determinados minutos, luego de los cuales se podrá ingresar nuevamente la contraseña. Posterior a ello, cada vez que se ingrese de modo incorrecto el código, el tiempo de espera para desbloquear el sistema se incrementará consecutivamente.

g. Los softwares y subprocesadores donde se almacenan los datos personales protege el banco de datos personales contra acceso lógico no autorizado mediante algún mecanismo de bloqueo lógico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados por la Sociedad.

h. El sistema/programa/software donde se almacenan los datos personales identifica los accesos realizados a los bancos de datos personales para su tratamiento, considerando al menos, los siguientes campos:

- Fecha y hora del acceso;
- Persona o personas que realiza(n) el acceso;
- Motivo del acceso (acciones relevantes).

i. Los registros de los ingresos a los bancos de datos personales se almacenan en Google Drive y se accede a ellos mediante ingreso de clave. El cargo con acceso a los mismos es el Gerente de Ética y Cumplimiento Regulatorio. Estos datos se registran de manera permanente.

j. Los datos personales contenidos en soporte informático se transportan previa encriptación y su integridad es validada con login vía Autenticación de múltiples factores - MFA.

k. Cuando se requiera eliminar la información de datos personales contenida en un medio informático removible, se deberán utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del medio informático utilizado, de forma tal que, no permitan la recuperación de dichos datos personales.

l. Los equipos utilizados para el tratamiento de los datos personales deberán recibir mantenimiento preventivo y correctivo de acuerdo con las recomendaciones y especificaciones del proveedor de los mismos para asegurar su disponibilidad, integridad y buen funcionamiento. El mantenimiento de los referidos equipos deberá ser realizado por personal técnico previamente autorizado por la Sociedad. Los mencionados equipos utilizados para el tratamiento de los datos personales deberán contar con software de protección contra software malicioso (virus, troyanos, spyware, etc.), para proteger la integridad de los bancos de datos personales almacenados en los mismos. El software de protección deberá ser

actualizado frecuentemente de acuerdo con las recomendaciones y especificaciones del proveedor de los mismos.

m. En relación con las medidas de seguridad en los servicios de tratamiento de datos personales por medios tecnológicos tercerizados, la Sociedad tendrá en cuenta las siguientes medidas de seguridad para la prestación del referido servicio de tratamiento de datos personales:

- Que el proveedor no tenga acceso a la información de los datos personales almacenados en su infraestructura.
- Que el proveedor no brinde acceso a terceros de los datos personales almacenados en su infraestructura.
- La destrucción o la imposibilidad de recuperación de los datos personales almacenados en el servicio tercerizado de tratamiento de datos personales por medios tecnológicos una vez concluida la relación con el proveedor del referido servicio.
- Uso de canales seguros para la transferencia de datos personales.
- Garantizar el cumplimiento de las medidas de seguridad en todos los lugares en donde se encuentre distribuida la infraestructura del proveedor del servicio de tercerización de tratamiento de los datos personales.

n. Se deberán realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción, teniendo en consideración lo siguiente:

- Las copias de respaldo de los datos personales están protegidas mediante técnicas de cifrado y almacenadas en un local seguro y distante al ambiente principal de tratamiento de datos personales.
- La copia de respaldo se realiza con una frecuencia diaria y el periodo de conservación de las referidas copias de respaldo es de un mes.
- Se cuenta con un mecanismo que garantiza la continuidad del tratamiento de datos personales.

o. Toda recuperación de datos personales, desde su copia de respaldo, deberá contar con la autorización por escrito del Gerente de Ética y Cumplimiento Regulatorio.

p. Anualmente se realizarán pruebas de recuperación de los datos personales para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido. Se documentarán los resultados de las pruebas incluyendo:

- Fecha y hora de la prueba de recuperación de los datos personales.
- Nombre de la persona que realizó la prueba de recuperación.
- Banco de datos personales recuperado.
- Archivo recuperado y fecha de los datos personales recuperados.
- Resultado de las pruebas de recuperación de los datos personales.
- Acciones tomadas en caso de pruebas insatisfactorias.

2. <u>Banco de Datos "Colaboradores de proyectos"</u>:

a. El banco de datos personales se registra usando el software en la nube que almacena base de datos alojada en Google Drive.

b. El servidor se encuentra en un Data Center que cuenta con sistema de enfriamiento, control de acceso, sistema contra incendios.

c. Se podrá acceder al banco de datos personales en función a los siguientes niveles de privilegio (datos a tratar o tarea a realizar):

- Usuarios tipo 1: personal del área de Operaciones Regional y el Gerente de País.
  Privilegios: solo ingreso de datos y lectura.

- Usuario Administrador: personal del área de Operaciones.
  Privilegios: ingreso de datos, edición, eliminar, grabar, lectura.

- Todos los Usuarios está prohibido de imprimir documentos que contengan datos personales o de grabar los mismos en dispositivo removibles, salvo que sean parte necesario del desarrollo de su trabajo.

d. Anualmente, se revisará los privilegios de acceso a los bancos de datos personales que correspondan al personal autorizado de la Sociedad. Esta revisión deberá constar en un acta que debidamente firmada será archivada.

e. El personal de la Sociedad autorizado con privilegios suficientes para tener acceso a los bancos de datos personales, contará con una contraseña que le permitirá acceder al banco de datos personales en función a sus privilegios.

f. Medidas de seguridad para el uso de contraseñas:

- El personal autorizado de la Sociedad debe mantener en secreto las contraseñas que les han sido asignadas.
- Cuando se utilice un servidor de autenticación, este debe almacenar las contraseñas de manera cifrada.
- Permitir que el personal autorizado de la Sociedad cambie la contraseña asignada cuando lo considere necesario, debiendo hacerlo cuando mínimo cada tres (3) meses.
- Requerir el uso de contraseñas que contengan al menos ocho (8) dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial.
- El acceso al sistema en entornos públicos (intranet, internet o similares) se bloquea temporalmente luego de tres (3) intentos fallidos de autenticación consecutivos. Es decir, en caso de ingresar la contraseña de manera errónea tres (3) veces consecutivas, el sistema bloqueará el acceso por determinados minutos, luego de los cuales se podrá ingresar nuevamente la contraseña. Posterior a ello, cada vez que se ingrese de modo incorrecto el código, el tiempo de espera para desbloquear el sistema se incrementará consecutivamente.

g. Los softwares y subprocesadores donde se almacenan los datos personales protege el banco de datos personales contra acceso lógico no autorizado mediante algún mecanismo de bloqueo lógico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados por la Sociedad.

h. El sistema/programa/software donde se almacenan los datos personales identifica los accesos realizados a los bancos de datos personales para su tratamiento, considerando al menos, los siguientes campos:

- Fecha y hora del acceso;
- Persona o personas que realiza(n) el acceso;
- Motivo del acceso (acciones relevantes).

i. Los registros de los ingresos a los bancos de datos personales se almacenan en el sistema y se accede a ellos de manera inmediata y/o mediante solicitud al proveedor. Los cargos con acceso a los mismos son la Ejecutiva de Cuenta, el Gerente País y Operaciones Regional. Estos datos se registran de manera permanente.

j. Los datos personales contenidos en soporte informático se transportan previa encriptación y su integridad es validada con login vía Autenticación de múltiples factores - MFA.

k. Cuando se requiera eliminar la información de datos personales contenida en un medio informático removible, se deberán utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del medio informático utilizado, de forma tal que, no permitan la recuperación de dichos datos personales.

l. Los equipos utilizados para el tratamiento de los datos personales deberán recibir mantenimiento preventivo y correctivo de acuerdo con las recomendaciones y especificaciones del proveedor de los mismos para asegurar su disponibilidad, integridad y buen funcionamiento. El mantenimiento de los referidos equipos deberá ser realizado por personal técnico previamente autorizado por la Sociedad. Los mencionados equipos utilizados para el tratamiento de los datos personales deberán contar con software de protección contra software malicioso (virus, troyanos, spyware, etc.), para proteger la integridad de los bancos de datos personales almacenados en los mismos. El software de protección deberá ser actualizado frecuentemente de acuerdo con las recomendaciones y especificaciones del proveedor de los mismos.

m. En relación con las medidas de seguridad en los servicios de tratamiento de datos personales por medios tecnológicos tercerizados, la Sociedad tendrá en cuenta las siguientes medidas de seguridad para la prestación del referido servicio de tratamiento de datos personales:

- Que el proveedor no tenga acceso a la información de los datos personales almacenados en su infraestructura.

- Que el proveedor no brinde acceso a terceros de los datos personales almacenados en su infraestructura.
- La destrucción o la imposibilidad de recuperación de los datos personales almacenados en el servicio tercerizado de tratamiento de datos personales por medios tecnológicos una vez concluida la relación con el proveedor del referido servicio.
- Uso de canales seguros para la transferencia de datos personales.
- Garantizar el cumplimiento de las medidas de seguridad en todos los lugares en donde se encuentre distribuida la infraestructura del proveedor del servicio de tercerización de tratamiento de los datos personales.

n. Se deberán realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción, teniendo en consideración lo siguiente:

- Las copias de respaldo de los datos personales están protegidas mediante técnicas de cifrado y almacenada en un local seguro y distante al ambiente principal de tratamiento de datos personales.
- La copia de respaldo se realiza con una frecuencia diaria y el periodo de conservación de las referidas copias de respaldo es de un mes.
- Se cuenta con un mecanismo que garantiza la continuidad del tratamiento de datos personales.

o. Toda recuperación de datos personales, desde su copia de respaldo, deberá contar con la autorización por escrito del Gerente de Ética y Cumplimiento.

p. Anualmente se realizarán pruebas de recuperación de los datos personales para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido. Se documentarán los resultados de las pruebas incluyendo:

- Fecha y hora de la prueba de recuperación de los datos personales.
- Nombre de la persona que realizó la prueba de recuperación.
- Banco de datos personales recuperado.
- Archivo recuperado y fecha de los datos personales recuperados.
- Resultado de las pruebas de recuperación de los datos personales.
- Acciones tomadas en caso de pruebas insatisfactorias.

3. <u>Banco de Datos "Postulantes"</u>:

a. El banco de datos personales se almacena en Google Drive. Los datos se obtienen a partir del acceso a la plataforma del sub-procesador Hiring Room.

b. El servidor se encuentra en un Data Center que cuenta con sistema de enfriamiento, control de acceso, sistema contra incendios.

c. Se podrá acceder al banco de datos personales en función a los siguientes niveles de privilegio (datos a tratar o tarea a realizar):

- Usuarios tipo 1: personal del área de Operaciones.
  Privilegios: solo ingreso de datos y lectura.

- Usuario Administrador: personal del área Reclutamiento.
  Privilegios: ingreso de datos, edición, eliminar, grabar, lectura.

- Todos los Usuarios está prohibido de imprimir documentos que contengan datos personales o de grabar los mismos en dispositivo removibles, salvo que sean parte necesario del desarrollo de su trabajo.

d. Anualmente, se revisará los privilegios de acceso a los bancos de datos personales que correspondan al personal autorizado de la Sociedad. Esta revisión deberá constar en un acta que debidamente firmada será archivada.

e. El personal de la Sociedad autorizado con privilegios suficientes para tener acceso a los bancos de datos personales, contará con una contraseña que le permitirá acceder al banco de datos personales en función a sus privilegios.

f. Medidas de seguridad para el uso de contraseñas:

- El personal autorizado de la Sociedad debe mantener en secreto las contraseñas que les han sido asignadas.
- Cuando se utilice un servidor de autenticación, este debe almacenar las contraseñas de manera cifrada.
- Permitir que el personal autorizado de la Sociedad cambie la contraseña asignada cuando lo considere necesario, debiendo hacerlo cuando mínimo cada tres (3) meses.
- Requerir el uso de contraseñas que contengan al menos ocho (8) dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial.
- El acceso al sistema en entornos públicos (intranet, internet o similares) se bloquea temporalmente luego de seis (6) intentos fallidos de autenticación consecutivos. Es decir, en caso de ingresar la contraseña de manera errónea seis (6) veces consecutivas, el sistema bloqueará el acceso por determinados minutos, luego de los cuales se podrá ingresar nuevamente la contraseña. Posterior a ello, cada vez que se ingrese de modo incorrecto el código, el tiempo de espera para desbloquear el sistema se incrementará consecutivamente.

g. Los softwares y subprocesadores donde se almacenan los datos personales protege el banco de datos personales contra acceso lógico no autorizado mediante algún mecanismo de bloqueo lógico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados por la Sociedad.

h. El sistema/programa/software donde se almacenan los datos personales identifica los accesos realizados a los bancos de datos personales para su tratamiento, considerando al menos, los siguientes campos:

- Fecha y hora del acceso;
- Persona o personas que realiza(n) el acceso;
- Motivo del acceso (acciones relevantes).

i. Los registros de los ingresos a los bancos de datos personales se almacenan en el sistema/programa/software y se accede a ellos de manera inmediata. Los cargos con acceso a los mismos son el Reclutador regional y Operaciones. Estos datos se registran de manera permanente.

j. Los datos personales contenidos en soporte informático se transportan previa encriptación y su integridad es validada con login vía Autenticación de múltiples factores - MFA.

k. Cuando se requiera eliminar la información de datos personales contenida en un medio informático removible, se deberán utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del medio informático utilizado, de forma tal que, no permitan la recuperación de dichos datos personales.

l. Los equipos utilizados para el tratamiento de los datos personales deberán recibir mantenimiento preventivo y correctivo de acuerdo con las recomendaciones y especificaciones del proveedor de los mismos para asegurar su disponibilidad, integridad y buen funcionamiento. El mantenimiento de los referidos equipos deberá ser realizado por personal técnico previamente autorizado por la Sociedad. Los mencionados equipos utilizados para el tratamiento de los datos personales deberán contar con software de protección contra software malicioso (virus, troyanos, spyware, etc.), para proteger la integridad de los bancos de datos personales almacenados en los mismos. El software de protección deberá ser actualizado frecuentemente de acuerdo con las recomendaciones y especificaciones del proveedor de los mismos.

m. En relación con las medidas de seguridad en los servicios de tratamiento de datos personales por medios tecnológicos tercerizados, la Sociedad tendrá en cuenta las siguientes medidas de seguridad para la prestación del referido servicio de tratamiento de datos personales:

    - Que el proveedor no tenga acceso a la información de los datos personales almacenados en su infraestructura.
    - Que el proveedor no brinde acceso a terceros de los datos personales almacenados en su infraestructura.
    - La destrucción o la imposibilidad de recuperación de los datos personales almacenados en el servicio tercerizado de tratamiento de datos personales por medios tecnológicos una vez concluida la relación con el proveedor del referido servicio.
    - Uso de canales seguros para la transferencia de datos personales.
    - Garantizar el cumplimiento de las medidas de seguridad en todos los lugares en donde se encuentre distribuida la infraestructura del proveedor del servicio de tercerización de tratamiento de los datos personales.

n. Se deberán realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción, teniendo en consideración lo siguiente:

- Las copias de respaldo de los datos personales están protegidas mediante técnicas de cifrado y almacenada en un local seguro y distante al ambiente principal de tratamiento de datos personales.
- La copia de respaldo se realiza con una frecuencia diaria y el periodo de conservación de las referidas copias de respaldo es de un mes.
- Se cuenta con un mecanismo que garantiza la continuidad del tratamiento de datos personales.

o. Toda recuperación de datos personales, desde su copia de respaldo, deberá contar con la autorización por escrito del Gerente de Ética y Cumplimiento Regulatorio.

p. Anualmente se realizarán pruebas de recuperación de los datos personales para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido. Se documentarán los resultados de las pruebas incluyendo:

- Fecha y hora de la prueba de recuperación de los datos personales.
- Nombre de la persona que realizó la prueba de recuperación.
- Banco de datos personales recuperado.
- Archivo recuperado y fecha de los datos personales recuperados.
- Resultado de las pruebas de recuperación de los datos personales.
- Acciones tomadas en caso de pruebas insatisfactorias.

4. <u>Banco de Datos "Proveedores"</u>:

a. El banco de datos personales se registra usando el software en la nube (Google Drive) que almacena base de datos alojada en Google Drive

b. El servidor se encuentra en un Data Center que cuenta con sistema de enfriamiento, control de acceso, sistema contra incendios.

c. Se podrá acceder al banco de datos personales en función a los siguientes niveles de privilegio (datos a tratar o tarea a realizar):

- Usuarios tipo 1: personal del área de Gerencia País.
  Privilegios: solo ingreso de datos y lectura.

- Usuario Administrador: Asistente Administrativa.
  Privilegios: ingreso de datos, edición, eliminar, grabar, lectura.

- Todos los Usuarios está prohibido de imprimir documentos que contengan datos personales o de grabar los mismos en dispositivo removibles, salvo que sean parte necesario del desarrollo de su trabajo.

d. Anualmente, se revisará los privilegios de acceso a los bancos de datos personales que correspondan al personal autorizado de la Sociedad. Esta revisión deberá constar en un acta que debidamente firmada será archivada.

e. El personal de la Sociedad autorizado con privilegios suficientes para tener acceso a los bancos de datos personales, contará con una contraseña que le permitirá acceder al banco de datos personales en función a sus privilegios.

f. Medidas de seguridad para el uso de contraseñas:

- El personal autorizado de la Sociedad debe mantener en secreto las contraseñas que les han sido asignadas.
- Cuando se utilice un servidor de autenticación, este debe almacenar las contraseñas de manera cifrada.
- Permitir que el personal autorizado de la Sociedad cambie la contraseña asignada cuando lo considere necesario, debiendo hacerlo cuando mínimo cada tres (3) meses.
- Requerir el uso de contraseñas que contengan al menos ocho (8) dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial.
- El acceso al sistema en entornos públicos (intranet, internet o similares) se bloquea temporalmente luego de seis (6) intentos fallidos de autenticación consecutivos. Es decir, en caso de ingresar la contraseña de manera errónea seis (6) veces consecutivas, el sistema bloqueará el acceso por determinados minutos, luego de los cuales se podrá ingresar nuevamente la contraseña. Posterior a ello, cada vez que se ingrese de modo incorrecto el código, el tiempo de espera para desbloquear el sistema se incrementará consecutivamente.

g. Los softwares y subprocesadores donde se almacenan los datos personales protege el banco de datos personales contra acceso lógico no autorizado mediante algún mecanismo de bloqueo lógico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados por la Sociedad.

h. El sistema/programa/software donde se almacenan los datos personales identifica los accesos realizados a los bancos de datos personales para su tratamiento, considerando al menos, los siguientes campos:

- Fecha y hora del acceso;
- Persona o personas que realiza(n) el acceso;
- Motivo del acceso (acciones relevantes).

i. Los registros de los ingresos a los bancos de datos personales se almacenan en el sistema/programa/software y se accede a ellos de manera inmediata. Los cargos con acceso a los mismos son la Gerencia País y la Asistente Administrativa Estos datos se registran de manera permanente.

j. Los datos personales contenidos en soporte informático se transportan previa encriptación y su integridad es validada con login vía MFA.

k. Cuando se requiera eliminar la información de datos personales contenida en un medio informático removible, se deberán utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del

medio informático utilizado, de forma tal que, no permitan la recuperación de dichos datos personales.

l. Los equipos utilizados para el tratamiento de los datos personales deberán recibir mantenimiento preventivo y correctivo de acuerdo con las recomendaciones y especificaciones del proveedor de los mismos para asegurar su disponibilidad, integridad y buen funcionamiento. El mantenimiento de los referidos equipos deberá ser realizado por personal técnico previamente autorizado por la Sociedad. Los mencionados equipos utilizados para el tratamiento de los datos personales deberán contar con software de protección contra software malicioso (virus, troyanos, spyware, etc.), para proteger la integridad de los bancos de datos personales almacenados en los mismos. El software de protección deberá ser actualizado frecuentemente de acuerdo con las recomendaciones y especificaciones del proveedor de los mismos.

m. En relación con las medidas de seguridad en los servicios de tratamiento de datos personales por medios tecnológicos tercerizados, la Sociedad tendrá en cuenta las siguientes medidas de seguridad para la prestación del referido servicio de tratamiento de datos personales:

- Que el proveedor no tenga acceso a la información de los datos personales almacenados en su infraestructura.
- Que el proveedor no brinde acceso a terceros de los datos personales almacenados en su infraestructura.
- La destrucción o la imposibilidad de recuperación de los datos personales almacenados en el servicio tercerizado de tratamiento de datos personales por medios tecnológicos una vez concluida la relación con el proveedor del referido servicio.
- Uso de canales seguros para la transferencia de datos personales.
- Garantizar el cumplimiento de las medidas de seguridad en todos los lugares en donde se encuentre distribuida la infraestructura del proveedor del servicio de tercerización de tratamiento de los datos personales.

n. Se deberán realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción, teniendo en consideración lo siguiente:

- Las copias de respaldo de los datos personales están protegidas mediante técnicas de cifrado y almacenada en un local seguro y distante al ambiente principal de tratamiento de datos personales.
- La copia de respaldo se realiza con una frecuencia diaria y el periodo de conservación de las referidas copias de respaldo es de un mes.
- Se cuenta con un mecanismo que garantiza la continuidad del tratamiento de datos personales.

o. Toda recuperación de datos personales, desde su copia de respaldo, deberá contar con la autorización por escrito del Gerente Ética y Cumplimiento.

p. Anualmente se realizarán pruebas de recuperación de los datos personales para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido. Se documentarán los resultados de las pruebas incluyendo:

- Fecha y hora de la prueba de recuperación de los datos personales.
- Nombre de la persona que realizó la prueba de recuperación.
- Banco de datos personales recuperado.
- Archivo recuperado y fecha de los datos personales recuperados.
- Resultado de las pruebas de recuperación de los datos personales.
- Acciones tomadas en caso de pruebas insatisfactorias.

5. <u>Banco de Datos "Clientes"</u>:

a. El banco de datos personales se registra usando el software Google Drive solución en la nube que almacena base de datos alojada en Google Drive

b. El servidor se encuentra en un Data Center que cuenta con sistema de enfriamiento, control de acceso, sistema contra incendios.

c. Se podrá acceder al banco de datos personales en función a los siguientes niveles de privilegio (datos a tratar o tarea a realizar):

- Usuarios tipo 1: personal del área Comercial.
  Privilegios: solo ingreso de datos y lectura.

- Usuario Administrador: Gerente País.
  Privilegios: ingreso de datos, edición, eliminar, grabar, lectura.

- Todos los Usuarios está prohibido de imprimir documentos que contengan datos personales o de grabar los mismos en dispositivo removibles, salvo que sean parte necesario del desarrollo de su trabajo.

d. Anualmente, se revisará los privilegios de acceso a los bancos de datos personales que correspondan al personal autorizado de la Sociedad. Esta revisión deberá constar en un acta que debidamente firmada será archivada.

e. El personal de la Sociedad autorizado con privilegios suficientes para tener acceso a los bancos de datos personales, contará con una contraseña que le permitirá acceder al banco de datos personales en función a sus privilegios.

f. Medidas de seguridad para el uso de contraseñas:

- El personal autorizado de la Sociedad debe mantener en secreto las contraseñas que les han sido asignadas.
- Cuando se utilice un servidor de autenticación, este debe almacenar las contraseñas de manera cifrada.
- Permitir que el personal autorizado de la Sociedad cambie la contraseña asignada cuando lo considere necesario, debiendo hacerlo cuando mínimo cada tres (3) meses.

- Requerir el uso de contraseñas que contengan al menos ocho (8) dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial.
- El acceso al sistema en entornos públicos (intranet, internet o similares) se bloquea temporalmente luego de seis (6) intentos fallidos de autenticación consecutivos. Es decir, en caso de ingresar la contraseña de manera errónea seis (6) veces consecutivas, el sistema bloqueará el acceso por determinados minutos, luego de los cuales se podrá ingresar nuevamente la contraseña. Posterior a ello, cada vez que se ingrese de modo incorrecto el código, el tiempo de espera para desbloquear el sistema se incrementará consecutivamente.

g. Los softwares y subprocesadores donde se almacenan los datos personales protege el banco de datos personales contra acceso lógico no autorizado mediante algún mecanismo de bloqueo lógico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados por la Sociedad.

h. El sistema/programa/software donde se almacenan los datos personales identifica los accesos realizados a los bancos de datos personales para su tratamiento, considerando al menos, los siguientes campos:

- Fecha y hora del acceso;
- Persona o personas que realiza(n) el acceso;
- Motivo del acceso (acciones relevantes).

i. Los registros de los ingresos a los bancos de datos personales se almacenan en el sistema/programa/software y se accede a ellos de manera inmediata. Los cargos con acceso a los mismos es el Gerente País, Líder Comercial, Ejecutiva de Cuenta y Analista Contable. Estos datos se registran de manera permanente.

j. Los datos personales contenidos en soporte informático se transportan previa encriptación y su integridad es validada con login vía MFA.

k. Cuando se requiera eliminar la información de datos personales contenida en un medio informático removible, se deberán utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del medio informático utilizado, de forma tal que, no permitan la recuperación de dichos datos personales.

l. Los equipos utilizados para el tratamiento de los datos personales deberán recibir mantenimiento preventivo y correctivo de acuerdo con las recomendaciones y especificaciones del proveedor de los mismos para asegurar su disponibilidad, integridad y buen funcionamiento. El mantenimiento de los referidos equipos deberá ser realizado por personal técnico previamente autorizado por la Sociedad. Los mencionados equipos utilizados para el tratamiento de los datos personales deberán contar con software de protección contra software malicioso (virus, troyanos, spyware, etc.), para proteger la integridad de los bancos de datos personales almacenados en los mismos. El software de protección deberá ser

actualizado frecuentemente de acuerdo con las recomendaciones y especificaciones del proveedor de los mismos.

m. En relación con las medidas de seguridad en los servicios de tratamiento de datos personales por medios tecnológicos tercerizados, la Sociedad tendrá en cuenta las siguientes medidas de seguridad para la prestación del referido servicio de tratamiento de datos personales:

- Que el proveedor no tenga acceso a la información de los datos personales almacenados en su infraestructura.
- Que el proveedor no brinde acceso a terceros de los datos personales almacenados en su infraestructura.
- La destrucción o la imposibilidad de recuperación de los datos personales almacenados en el servicio tercerizado de tratamiento de datos personales por medios tecnológicos una vez concluida la relación con el proveedor del referido servicio.
- Uso de canales seguros para la transferencia de datos personales.
- Garantizar el cumplimiento de las medidas de seguridad en todos los lugares en donde se encuentre distribuida la infraestructura del proveedor del servicio de tercerización de tratamiento de los datos personales.

n. Se deberán realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción, teniendo en consideración lo siguiente:

- Las copias de respaldo de los datos personales están protegidas mediante técnicas de cifrado y almacenada en un local seguro y distante al ambiente principal de tratamiento de datos personales.
- La copia de respaldo se realiza con una frecuencia diaria y el periodo de conservación de las referidas copias de respaldo es de un mes.
- Se cuenta con un mecanismo que garantiza la continuidad del tratamiento de datos personales.

o. Toda recuperación de datos personales, desde su copia de respaldo, deberá contar con la autorización por escrito del Gerente de Ética y Cumplimiento.

p. Anualmente se realizarán pruebas de recuperación de los datos personales para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido. Se documentarán los resultados de las pruebas incluyendo:

- Fecha y hora de la prueba de recuperación de los datos personales.
- Nombre de la persona que realizó la prueba de recuperación.
- Banco de datos personales recuperado.
- Archivo recuperado y fecha de los datos personales recuperados.
- Resultado de las pruebas de recuperación de los datos personales.
- Acciones tomadas en caso de pruebas insatisfactorias.

6. <u>Banco de Datos "Potenciales Clientes"</u>:

a. El banco de datos personales se registra usando el software Google Drive solución en la nube que almacena base de datos alojada en Google Drive

b. El servidor se encuentra en un Data Center que cuenta con sistema de enfriamiento, control de acceso, sistema contra incendios.

c. Se podrá acceder al banco de datos personales en función a los siguientes niveles de privilegio (datos a tratar o tarea a realizar):

- Usuarios tipo 1: personal del área de Comercial.
  Privilegios: solo ingreso de datos y lectura.

- Usuario Administrador: personal del área Gerente País.
  Privilegios: ingreso de datos, edición, eliminar, grabar, lectura.

- Todos los Usuarios está prohibido de imprimir documentos que contengan datos personales o de grabar los mismos en dispositivo removibles, salvo que sean parte necesario del desarrollo de su trabajo.

d. Anualmente, se revisará los privilegios de acceso a los bancos de datos personales que correspondan al personal autorizado de la Sociedad. Esta revisión deberá constar en un acta que debidamente firmada será archivada.

e. El personal de la Sociedad autorizado con privilegios suficientes para tener acceso a los bancos de datos personales, contará con una contraseña que le permitirá acceder al banco de datos personales en función a sus privilegios.

f. Medidas de seguridad para el uso de contraseñas:

- El personal autorizado de la Sociedad debe mantener en secreto las contraseñas que les han sido asignadas.
- Cuando se utilice un servidor de autenticación, este debe almacenar las contraseñas de manera cifrada.
- Permitir que el personal autorizado de la Sociedad cambie la contraseña asignada cuando lo considere necesario, debiendo hacerlo cuando mínimo cada tres (3) meses.
- Requerir el uso de contraseñas que contengan al menos ocho (8) dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial.
- El acceso al sistema en entornos públicos (intranet, internet o similares) se bloquea temporalmente luego de seis (6) intentos fallidos de autenticación consecutivos. Es decir, en caso de ingresar la contraseña de manera errónea seis (6) veces consecutivas, el sistema bloqueará el acceso por determinados minutos, luego de los cuales se podrá ingresar nuevamente la contraseña. Posterior a ello, cada vez que se ingrese de modo incorrecto el código, el tiempo de espera para desbloquear el sistema se incrementará consecutivamente.

g. Los softwares y subprocesadores donde se almacenan los datos personales protege el banco de datos personales contra acceso lógico no autorizado

mediante algún mecanismo de bloqueo lógico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados por la Sociedad.

h. El sistema/programa/software donde se almacenan los datos personales identifica los accesos realizados a los bancos de datos personales para su tratamiento, considerando al menos, los siguientes campos:

- Fecha y hora del acceso;
- Persona o personas que realiza(n) el acceso;
- Motivo del acceso (acciones relevantes).

i. Los registros de los ingresos a los bancos de datos personales se almacenan en el sistema/programa/software y se accede a ellos de manera inmediata. Los cargos con acceso a los mismos son Gerente País, Líder Comercial, Ejecutiva de Cuenta y Analista Contable . Estos datos se registran de manera permanente.

j. Los datos personales contenidos en soporte informático se transportan previa encriptación y su integridad es validada con login vía Autenticación de múltiples factores - MFA.

k. Cuando se requiera eliminar la información de datos personales contenida en un medio informático removible, se deberán utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del medio informático utilizado, de forma tal que, no permitan la recuperación de dichos datos personales.

l. Los equipos utilizados para el tratamiento de los datos personales deberán recibir mantenimiento preventivo y correctivo de acuerdo con las recomendaciones y especificaciones del proveedor de los mismos para asegurar su disponibilidad, integridad y buen funcionamiento. El mantenimiento de los referidos equipos deberá ser realizado por personal técnico previamente autorizado por la Sociedad. Los mencionados equipos utilizados para el tratamiento de los datos personales deberán contar con software de protección contra software malicioso (virus, troyanos, spyware, etc.), para proteger la integridad de los bancos de datos personales almacenados en los mismos. El software de protección deberá ser actualizado frecuentemente de acuerdo con las recomendaciones y especificaciones del proveedor de los mismos.

m. En relación con las medidas de seguridad en los servicios de tratamiento de datos personales por medios tecnológicos tercerizados, la Sociedad tendrá en cuenta las siguientes medidas de seguridad para la prestación del referido servicio de tratamiento de datos personales:

- Que el proveedor no tenga acceso a la información de los datos personales almacenados en su infraestructura.
- Que el proveedor no brinde acceso a terceros de los datos personales almacenados en su infraestructura.
- La destrucción o la imposibilidad de recuperación de los datos personales almacenados en el servicio tercerizado de tratamiento de datos personales

por medios tecnológicos una vez concluida la relación con el proveedor del referido servicio.
- Uso de canales seguros para la transferencia de datos personales.
- Garantizar el cumplimiento de las medidas de seguridad en todos los lugares en donde se encuentre distribuida la infraestructura del proveedor del servicio de tercerización de tratamiento de los datos personales.

n. Se deberán realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción, teniendo en consideración lo siguiente:

- Las copias de respaldo de los datos personales están protegidas mediante técnicas de cifrado y almacenada en un local seguro y distante al ambiente principal de tratamiento de datos personales.
- La copia de respaldo se realiza con una frecuencia diaria y el periodo de conservación de las referidas copias de respaldo es de un mes.
- Se cuenta con un mecanismo que garantiza la continuidad del tratamiento de datos personales.

o. Toda recuperación de datos personales, desde su copia de respaldo, deberá contar con la autorización por escrito del Gerente de Ética y Cumplimiento.

p. Anualmente se realizarán pruebas de recuperación de los datos personales para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido. Se documentarán los resultados de las pruebas incluyendo:

- Fecha y hora de la prueba de recuperación de los datos personales.
- Nombre de la persona que realizó la prueba de recuperación.
- Banco de datos personales recuperado.
- Archivo recuperado y fecha de los datos personales recuperados.
- Resultado de las pruebas de recuperación de los datos personales.
- Acciones tomadas en caso de pruebas insatisfactorias.

V.3 Tratamiento no autorizado del banco de datos personales:

La Sociedad deberá informar al titular de los datos personales los incidentes que afecten significativamente sus derechos patrimoniales o morales, tan pronto se confirme el hecho del tratamiento no autorizado del banco de los datos personales. La información mínima que se deberá proporcionar al titular de los datos personales incluye:

- Naturaleza del incidente (tratamiento no autorizado del banco de datos personales).
- Datos personales comprometidos.
- Recomendaciones al titular de los datos personales.
- Medidas correctivas implementadas por la Sociedad.

Todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de

seguridad establecidas en este Protocolo, deberá ser reportado inmediatamente a Departamento de IT, Legal y Compliance.

V.4 Formalización De Transferencia De Datos Personales

La Sociedad solo podrá transferir datos personales almacenados en bancos de datos de la Sociedad cuando cuente con el consentimiento previo e informado del titular de los datos personales.

Los contratos que celebre donde su ejecución implique la transferencia de datos personales deben contener una cláusula de protección de datos personales. Ejemplo de cláusula:

"CLÁUSULA DE PROTECCIÓN DE DATOS PERSONALES:

En atención de lo previsto en la normatividad vigente sobre Protección de Datos Personales (Ley N°. 29733 y su Reglamento D.S. N° 003-2013-JUS y las que en el futuro las adicionen, modifiquen o complementen), tanto EL CLIENTE como EL LOCADOR manifiestan que dan pleno cumplimiento a la normatividad citada y que cuentan con políticas de privacidad para el tratamiento de datos personales a las cuales dan pleno cumplimiento.

Tanto EL CLIENTE como EL LOCADOR serán responsables por cualquier perjuicio que se cause a la otra parte como consecuencia directa o indirecta del incumplimiento de cualquiera de las obligaciones que se desprenden de la presente cláusula."

Anexo D
Procedimiento para ejercer los derechos del titular de los datos personales

Cada titular de datos personales tratados por la Sociedad puede revocar su consentimiento o ejercer sus derechos de Ley, mediante la presentación de su DNI u otro documento oficial de identidad y enviando su solicitud y/o consultas a:

- Correo electrónico: privacidadinformacion@grupostt.com
- Oficinas principal atención al Calle Alameda del Arco Iris, Tienda 7, Sotano N°118, Urb. La Alborada (Centro Comercial La Alborada), distrito de Santiago de Surco, provincia y departamento de Lima.

En caso de que el titular del dato personal requiera ejercer sus derechos mediante un representante, este deberá presentar carta poder legalizada por notario público que lo faculte como tal y su documento de identidad.

La Sociedad responderá al requerimiento del titular de los datos personales en los siguientes plazos, según el tipo de requerimiento:

- Derecho de información: será de ocho (08) días calendario.

- Derecho de acceso: veinte (20) días calendario.

- Otros derechos como los de rectificación, cancelación u oposición: diez (10) días calendario.