

POLÍTICA DE PROTECCIÓN DE DATOS	Versión No: 2	PROCESO ASOCIADO	
	Fecha: 01/08/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 1 de 11		

POLÍTICA PARA EL TRATAMIENTO DE DATOS PERSONALES

En cumplimiento a lo dispuesto en la Ley estatutaria 1581 de 2012 y a su Decreto Reglamentario 1377 de 2013, la empresa **E - Security LTDA** adopta la presente política para el tratamiento de datos personales, la cual será informada a todos los titulares de los datos recolectados o que en el futuro se obtengan en el ejercicio de las actividades comerciales o laborales. De esta manera, la **E - SECURITY LTDA** manifiesta que garantiza los derechos de la privacidad, la intimidad, el buen nombre y la autonomía de los titulares, en el tratamiento de los datos personales, y en consecuencia todas sus actuaciones se regirán por los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

Todas las personas que, en desarrollo de diferentes actividades contractuales, comerciales, laborales, entre otras, sean permanentes u ocasionales, llegaran a suministrar a la **E - SECURITY LTDA** cualquier tipo de información o dato personal, podrá conocerla, actualizarla y rectificarla.

I. IDENTIFICACIÓN

NOMBRE DE LA EMPRESA: E – Security Ltda.
DIRECION: Av. Calle 26 N° 69 d-91
CORREO ELECTRÓNICO: gerencia@e-security.com.co
TELEFÓNO DEL RESPONSABLE: +57 310 328 4300

II. MARCO LEGAL

- Constitución Política, artículo 15.
- Ley 1266 de 2008
- Ley 1581 de 2012
- Decretos Reglamentarios 1727 de 2009 y 2952 de 2010
- Decreto Reglamentario parcial 1377 de 2013

III. DEFINICIONES

AUTORIZACIÓN: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

AVISO DE PRIVACIDAD: Comunicación verbal o escrita generada por el responsable dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

BASE DE DATOS: Conjunto organizado de datos personales que sea objeto de tratamiento.

POLÍTICA DE PROTECCIÓN DE DATOS	Versión No: 2	PROCESO ASOCIADO	
	Fecha: 01/08/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 2 de 11		

CAUSA HABIENTE: Persona que ha sucedido a otra por causa del fallecimiento de ésta (heredero).

DATO PERSONAL: cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse a una persona natural o jurídica.

DATO PÚBLICO: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

DATOS SENSIBLES: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

DATOS INDISPENSABLES: Se entienden como aquellos datos personales de los asociados imprescindibles para llevar a cabo la actividad de prestación de servicio de seguridad. Los datos de naturaleza indispensable deberán ser proporcionados por los titulares de estos o los legitimados para el ejercicio de estos derechos.

DATOS OPCIONALES: Son aquellos datos que la compañía requiere para ofrecer servicios adicionales en investigación, ofertas laborales, etc.

ENCARGADO DEL TRATAMIENTO: Persona natural o jurídica, pública o privada que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.

LEY DE PROTECCIÓN DE DATOS: Es la Ley 1581 de 2012 y sus Decretos reglamentarios o las normas que los modifiquen, complementen o sustituyan.

HABEAS DATA: Derecho de cualquier persona a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en el banco de datos y en archivos de entidades públicas y privadas.

RESPONSABLE DEL TRATAMIENTO: Persona natural o jurídica, pública o privada que por sí misma o en asocio con otros, decida sobre la base de datos y/o Tratamiento de los datos.

TITULAR: Persona natural cuyos datos personales sean objeto de Tratamiento.

TRATAMIENTO: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

POLÍTICA DE PROTECCIÓN DE DATOS	Versión No: 2	PROCESO ASOCIADO	
	Fecha: 01/08/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 3 de 11		

TRANSFERENCIA: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

TRANSMISIÓN: Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

IV. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES

Con base a lo establecido y aplicación de la ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales y las normas que la complementan, modifican o adicionan, se aplicarán de manera armónica e integral los siguientes principios rectores:

- a) **PRINCIPIO DE LA LEGALIDAD:** El Tratamiento de datos es una actividad regulada que debe sujetarse a lo establecido en la ley y las demás disposiciones que la desarrollen.
- b) **PRINCIPIO DE FINALIDAD:** El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al titular. En lo correspondiente a la recolección de datos personales, La compañía se limitará a aquellos datos que sean pertinentes y adecuados para la finalidad con la cual fueron recolectados o requeridos; las áreas de Talento Humano, Operaciones, SIG, Comercial y Financiera deberán informar al titular el motivo por el cual se solicita la información y el uso específico que se le dará a la misma.
- c) **PRINCIPIO DE LIBERTAD:** el tratamiento solo puede ejercerse con el consentimiento previo, expreso, e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
- d) **PRINCIPIO DE VERACIDAD O CALIDAD:** La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- e) **PRINCIPIO DE TRANSPARENCIA:** En el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
- f) **PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA:** El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros

POLÍTICA DE PROTECCIÓN DE DATOS	Versión No: 2	PROCESO ASOCIADO	
	Fecha: 01/08/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 4 de 11		

medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares y terceros autorizados conforme a la ley.

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.

g) **PRINCIPIO DE SEGURIDAD:** La información sujeta a tratamiento por la compañía, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

h) **PRINCIPIO DE CONFIDENCIALIDAD:** Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de esta.

V.DATOS SENSIBLES

Teniendo en cuenta que la legislación define los datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Tratamiento de datos sensibles: De acuerdo con la normatividad se prohíbe el Tratamiento de datos sensibles, excepto cuando:

- El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- El Tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.

POLÍTICA DE PROTECCIÓN DE DATOS	Versión No: 2	PROCESO ASOCIADO	
	Fecha: 01/08/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 5 de 11		

d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

VI.DERECHOS QUE LE ASISTEN AL TITULAR DE LA INFORMACIÓN

El titular de los datos personales tendrá los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales frente a la compañía en su condición de responsable del tratamiento. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Solicitar prueba de la autorización otorgada a la compañía salvo cuando expresamente se exceptúe como requisito para el tratamiento (casos en los cuales no es necesaria la autorización).
- Ser informado por la compañía, previa solicitud, respecto del uso que le ha dado a sus datos personales.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

VII. DERECHOS DE LOS NIÑOS, NIÑAS Y ADOLESCENTES

En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

VIII.DEBERES DE LA EMPRESA

POLÍTICA DE PROTECCIÓN DE DATOS	Versión No: 2	PROCESO ASOCIADO	
	Fecha: 01/08/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 6 de 11		

En virtud de la presente política de tratamiento y protección de datos personales son deberes de la compañía los siguientes, sin perjuicio de las disposiciones previstas en la ley.

- a) Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- b) Solicitar y conservar, copia de la respectiva autorización otorgada por el titular.
- c) Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten en virtud de la autorización otorgada.
- d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- e) Garantizar que la información sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- f) Actualizar la información, atendiendo de esta forma todas las novedades respecto de los datos del titular. Adicionalmente, se deberán implementar todas las medidas necesarias para que la información se mantenga actualizada.
- g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente.
- h) Respetar las condiciones de seguridad y privacidad de la información del titular.
- i) Tramitar las consultas y reclamos formulados en los términos señalados por la ley.
- j) Identificar cuando determinada información se encuentra en discusión por parte del titular.
- k) Informar a solicitud del titular sobre el uso dado a sus datos.
- l) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- m) Cumplir los requerimientos e instrucciones que imparta la Superintendencia de Industria y Comercio sobre el tema en particular.
- n) Usar únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la ley 1581 de 2012.
- o) La compañía hará uso de los datos personales del titular solo para aquellas finalidades para las que se encuentre facultada debidamente y respetando en todo caso la normatividad vigente sobre protección de datos personales.

POLÍTICA DE PROTECCIÓN DE DATOS	Versión No: 2	PROCESO ASOCIADO	
	Fecha: 01/08/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 7 de 11		

IX. EL REGISTRO NACIONAL DE BASES DE DATOS

El Registro Nacional de Bases de Datos (RNBD), es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país y será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.

Una vez el Gobierno Nacional reglamente la información mínima que debe contener el Registro, y los términos y condiciones bajo los cuales se deben inscribir en éste, la compañía aportará a la Superintendencia de Industria y Comercio las bases de datos sujetas a tratamiento en el tiempo indicado.

X. AUTORIZACIONES Y CONSENTIMIENTO DEL TITULAR

Sin perjuicio de las excepciones previstas en la Ley, en el tratamiento de datos personales del titular se requiere la autorización previa e informada de éste, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

XI. MEDIO Y MANIFESTACIÓN PARA OTORGAR LA AUTORIZACIÓN DEL TITULAR

La compañía en los términos dispuestos en la Ley generó un aviso en el cual se comunica a los titulares que pueden ejercer su derecho al tratamiento de los datos personales a través de la página <https://www.es.company/> y del correo gerencia@e-security.com.co

XII. EVENTOS EN LOS CUALES NO ES NECESARIA LA AUTORIZACIÓN DEL TÍTULO DE LOS DATOS PERSONALES

La autorización del titular de la información no será necesaria en los siguientes casos:

- a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- b) Datos de naturaleza pública.
- c) Casos de urgencia médica o sanitaria.
- d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos. Datos relacionados con el Registro Civil de las personas.

XIII. LEGITIMACIÓN PARA EL EJERCICIO DEL DERECHO DEL TITULAR

Los derechos de los titulares establecidos en la Ley podrán ejercerse por las siguientes personas:

POLÍTICA DE PROTECCIÓN DE DATOS	Versión No: 2	PROCESO ASOCIADO	
	Fecha: 01/08/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 8 de 11		

- a) Por el titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición la compañía
- b) Por los causahabientes del titular, quienes deberán acreditar tal calidad.
- c) Por el representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.
- d) Por estipulación a favor de otro o para otro. Los derechos de los niños, niñas y adolescentes se ejercerán por las personas que estén facultadas para representarlos.

XIV. TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS Y FINALIDAD DE ESTE

El tratamiento para los datos personales indispensables de asociados y/o contratistas, estará enmarcado en el orden legal y en virtud de la condición de la compañía y serán todos los necesarios para el cumplimiento de la misión de la compañía como prestadora de servicios de seguridad privada.

Para el caso de datos personales sensibles, se podrá hacer uso y tratamiento de ellos cuando:

- a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
- b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;
- c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;
- d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
- e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes parámetros y/o requisitos:

- a) que respondan y respeten el interés superior de los niños, niñas y adolescentes.
- b) que se asegure el respeto de sus derechos fundamentales. Cumplidos los anteriores requisitos, el representante legal de los niños, niñas o adolescentes otorgará la autorización, previo ejercicio del menor de

POLÍTICA DE PROTECCIÓN DE DATOS	Versión No: 2	PROCESO ASOCIADO	
	Fecha: 01/08/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 9 de 11		

su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

La compañía velará por el uso adecuado del tratamiento de los datos personales de los niños, niñas o adolescentes

XV.PERSONAS A QUIENES SE LES PUEDE SUMINISTRAR LA INFORMACIÓN

La información que reúna las condiciones establecidas en la ley podrá suministrarse a las siguientes personas:

- a) A los titulares, sus causahabientes (cuando aquellos falten) o sus representantes legales.
- b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
- c) A los terceros autorizados por el titular o por la ley.

XVI.PERSONA O ÁREA RESPONSABLE DE LA ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS

La compañía ha designado como área responsable de velar por el cumplimiento de esta política al interior de la compañía en cabeza de la Gerencia Administrativa con el apoyo del área Jurídica, áreas Funcionales que manejan los Datos Personales de los Titulares como el Sistema integrado de gestión, Gestión humana, operaciones y el responsable de Seguridad de la Información.

Se atenderán peticiones, consultas y reclamos por parte de los titulares, así como solicitudes de actualización, rectificación o supresión de datos personales, a través del correo electrónico comercial@e-security.com.co

XVII.PROCEDIMIENTO PARA LA ATENCIÓN DE CONSULTAS, RECLAMOS Y PETICIONES

a) Consultas: Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en la compañía quien suministrará toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular. La consulta se formulará a través del correo comercial@e-security.com.co. La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de esta. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

b) Reclamos: El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley, podrán presentar un reclamo ante la compañía el cual será tramitado bajo las siguientes reglas:

1. El reclamo del Titular se formulará mediante solicitud dirigida a la compañía por el correo electrónico correo comercial@e-security.com.co con la identificación del Titular, la descripción de los hechos que dan lugar al

POLÍTICA DE PROTECCIÓN DE DATOS	Versión No: 2	PROCESO ASOCIADO	
	Fecha: 01/08/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 10 de 11		

reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo. En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

2. Una vez recibido el correo con el reclamo completo, éste se catalogará con la etiqueta "reclamo en trámite" y el motivo de este en un término no mayor a dos (2) días hábiles. Dicha etiqueta se mantendrá hasta que el reclamo sea decidido.

3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.

Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término. c) Petición de actualización, rectificación y supresión de datos. La compañía rectificará y actualizará, a solicitud del titular, la información de éste que resulte ser incompleta o inexacta, de conformidad con el procedimiento y los términos antes señalados, para lo cual el titular allegará la solicitud al correo comercial@e-security.com.co indicando la actualización, rectificación y supresión del dato y aportará la documentación que soporte su petición.

Revocatoria de la autorización y/o supresión del dato Los titulares de los datos personales pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal o contractual, para ello la compañía pondrá a disposición del Titular el correo electrónico correo comercial@e-security.com.co. Si vencido el término legal respectivo, la compañía, según fuera el caso, no hubieran eliminado los datos personales, el Titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o la supresión de los datos personales. Para estos efectos se aplicará el procedimiento descrito en el artículo 22 de la Ley 1581 de 2012.

XVIII. TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAISES

La compañía en cumplimiento de la misión de prestador de servicios de vigilancia y seguridad privada respeta la prohibición de transferir datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos, se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios, solo se consideran excepciones para esta prohibición los siguientes casos:

a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.

POLÍTICA DE PROTECCIÓN DE DATOS	Versión No: 2	PROCESO ASOCIADO	
	Fecha: 01/08/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 11 de 11		

- b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública.
- c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable,
- d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

La compañía se rige a lo estipulado por ley por ello los casos no contemplados como excepción en esta política, deben ser consultados a la Superintendencia de Industria y Comercio, quien es la única entidad para proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Esta política esta basada en la Legislación colombiana y está aprobada por la Representación legal de la compañía para su estricto cumplimiento.



HUGO DE JESÚS BEJARANO GARZON
GERENTE GENERAL

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión No: 1	PROCESO ASOCIADO	
	Fecha:06/03/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 1 de 1		

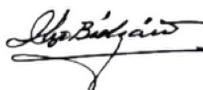
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

E-Security, consiente de las diferentes vulnerabilidades y riesgos que hay en la seguridad de la información, decide establecer directrices necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de la información dentro de la organización, asegurando el cumplimiento de las normativas legales y reguladoras aplicables.

Esta política aplica a todos los empleados, contratistas, proveedores y cualquier otro tercero que tenga acceso a los sistemas, redes o información de la organización.

- **Uso personal de los recursos tecnológicos**
Solo deben ser usados para fines laborales. El producto del uso de dichos recursos será de propiedad de la E – Security.
- **Prohibición de instalación de software y hardware en los computadores de La Empresa**
La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos solo puede ser realizada por los funcionarios de sistemas autorizados por la compañía.
- **Recursos compartidos**
Está terminantemente prohibido compartir los discos duros o las carpetas de los computadores de escritorio, aunque estén protegidos por contraseña. Cuando exista la necesidad de compartir recursos esto se debe hacer con autorización previa y restringir por Dominio
- **Acceso no autorizado a los sistemas de información de la Empresa**
Está totalmente prohibido obtener acceso a sistemas de información a los que no se tiene privilegios y/o dañar o alterar la operación de dichos sistemas. Esto implica la prohibición de capturar contraseñas, llaves de encriptación y otros mecanismos de control de acceso que le puedan permitir obtener ingreso a sistemas no autorizados.
- **Política de Escritorios y pantallas limpios**
Está prohibido almacenar información personal en los equipos de la compañía.
- **Política de uso de licencias de software**
Todos los empleados de la compañía deberán informar en caso del vencimiento de alguna de las diferentes licencias de software Implementados por la compañía para el desarrollo óptimo de sus labores. No podrán falsificar estas licencias bajo ninguna circunstancia
- **Backup**
Todos la información de cada área será respaldada regularmente y almacenada en ubicaciones seguras. La alta Dirección, genera conciencia sobre la presente política a todas las partes interesadas y vela por su adecuado cumplimiento.

Se firma y se aprueba el 6 de marzo de 2025.



HUGO DE JESUS BEJARANO GARZÓN
REPRESENTANTE LEGAL

POLÍTICA INTEGRAL DEL SISTEMA DE GESTIÓN	Versión No: 7	PROCESO ASOCIADO	
	Fecha: 04/06/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 1 de 1		

POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN

En E-Security Ltda., prestamos servicios de vigilancia y seguridad privada con los más altos estándares de calidad, lo que nos permite comprender las necesidades y expectativas de nuestras partes interesadas, brindando un servicio seguro, confiable y responsable. Promovemos la identificación de riesgos y oportunidades, comprometidos con la mejora continua del Sistema Integrado de Gestión (SIG), en cumplimiento de la normatividad legal vigente, los requisitos contractuales y los principios de seguridad y salud laboral, seguridad privada y seguridad vial.

La empresa se compromete a:

- Adoptar estrategias para una mayor satisfacción del cliente mediante procesos eficientes y en mejora continua.
- Promover ambientes de trabajo seguros y saludables con la participación activa y consulta de los trabajadores y del Comité Paritario de Seguridad y Salud en el Trabajo (COPASST), orientados a la prevención de lesiones, enfermedades laborales y daño a la propiedad, mediante la identificación, eliminación y control de peligros y riesgos.
- Integrar medidas que promuevan el respeto de los derechos humanos, garantizando el trato digno a todas las personas durante la operación.
- Evitar, prevenir y reducir la ocurrencia de eventos indeseables y perturbadores en nuestras operaciones de seguridad privada.
- Identificar, evaluar y prevenir los riesgos viales asociados a la movilidad del personal operativo, en cumplimiento del Plan Estratégico de Seguridad Vial (PESV), promoviendo la formación continua, la cultura vial y la adopción de comportamientos seguros para prevenir siniestros en los desplazamientos laborales e in itinere, ya sea como peatón, pasajero o conductor de vehículo automotor o no automotor.
- Definir lineamientos que garanticen el derecho fundamental a la igualdad, la no discriminación y una vida libre de violencias, mediante la adopción de medidas de prevención, protección y atención frente al acoso sexual en el contexto laboral.
- Suministrar los recursos humanos, físicos, técnicos y económicos necesarios para el mantenimiento y mejora del Sistema Integrado de Gestión, incluyendo el desarrollo e implementación efectiva del PESV.

La Alta Dirección genera conciencia sobre la presente política en todos los niveles de la organización y con las partes interesadas pertinentes, asegurando su adecuada aplicación, revisión y actualización periódica.

Se firma y se aprueba el 04 de Junio de 2025.


HUGO DE JESUS BEJARANO GARZÓN
REPRESENTANTE LEGAL

POLÍTICA DE PREVENCIÓN AL CONSUMO DE ALCOHOL, TABACO, DROGAS Y VAPEADORES	Versión No: 4	PROCESO ASOCIADO	
	Fecha: 14/08/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 1 de 1		

POLÍTICA DE PREVENCIÓN AL CONSUMO DE ALCOHOL, TABACO, DROGAS Y VAPEADORES

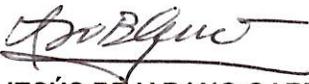
E-SECURITY LTDA., consciente de que el consumo de alcohol, tabaco, drogas, vapeadores o cualquier otro dispositivo electrónico para el consumo de nicotina y sustancias psicoactivas puede tener un impacto negativo en la salud y seguridad en el lugar de trabajo, ya que genera riesgos y enfermedades tanto para los trabajadores como para terceros, establece la siguiente política, de obligatorio cumplimiento para todos los trabajadores, visitantes y contratistas de la empresa:

- ✓ **Se prohíbe** el consumo de alcohol, drogas, tabaco, vapeadores y cualquier dispositivo electrónico para inhalar nicotina o sustancias psicoactivas por parte de los trabajadores, visitantes y contratistas durante la jornada laboral, ya sea dentro o fuera de las instalaciones de la Compañía.
- ✓ **Ninguna persona**, sin importar su rango o posición, podrá encontrarse bajo los efectos del consumo de bebidas alcohólicas, sustancias alucinógenas, vapeadores u otros dispositivos electrónicos de nicotina que alteren la conciencia, el estado de ánimo, la percepción o la capacidad de reacción, durante las horas de trabajo, dentro o fuera de las instalaciones de la Empresa.
- ✓ **No se permitirá** la posesión, consumo y/o comercialización de bebidas alcohólicas, tabaco, vapeadores, sustancias alucinógenas o psicoactivas, tanto en las instalaciones de la Empresa como en la prestación de servicios dentro o fuera de las instalaciones del cliente.
- ✓ **Es obligación** de cada trabajador informar a su jefe inmediato si, por razones médicas, debe utilizar algún tipo de medicamento que pueda afectar la ejecución segura de sus funciones.
- ✓ **Es obligatorio** participar activamente en los programas de sensibilización y capacitación que promuevan el cumplimiento de la presente Política.

Esta política es de obligatorio cumplimiento por parte de todos los colaboradores, contratistas y visitantes. La Empresa se reserva el derecho de realizar, en cualquier momento, inspecciones y pruebas de laboratorio al personal que labore en las instalaciones propias o del cliente.

Asimismo, destinará los recursos financieros, físicos y humanos necesarios para dar cumplimiento a esta política, fomentando la participación de todas las partes interesadas en las actividades que de ella se deriven y buscando prevenir el consumo de las sustancias y dispositivos descritos.

Se firma y se aprueba el 14 de agosto de 2025


HUGO DE JESÚS BEJARANO GARZÓN
 REPRESENTANTE LEGAL

POLÍTICA DESCONEXIÓN LABORAL	Versión No: 1	PROCESO ASOCIADO	
	Fecha: 19/02/2025	SISTEMA INTEGRADO DE GESTIÓN	
	Página: 1 de 1		

POLITICA DESCONEXION LABORAL

E-SECURITY LTDA, consciente de la importancia de facilitar un entorno de bienestar integral, productivo, sano, seguro y adecuado para aquellos que trabajan en la compañía, expresa que todos los trabajadores tienen derecho a la Desconexión Laboral, por cualquier medio o herramienta, bien sea tecnológica o no, para cuestiones relacionadas con su ámbito o actividad laboral, en horarios por fuera de la jornada de trabajo, o convenida, ni en sus vacaciones o descansos, licencias, permisos, construyendo un entorno laboral de bienestar, productivo, favoreciendo la conciliación de la vida laboral y extralaboral. Respetando los Derechos Humanos de todos los trabajadores de la organización y en cumplimiento con la ley 2191 de 2022.

La empresa se compromete a favorecer la productividad en la jornada laboral acordada, retroalimentar el esfuerzo y el desempeño de los trabajadores, permitir la recuperación física y mental del trabajador, aportar al bienestar integral intra y extra laboral, y a la construcción de entornos laborales saludables. Entre dichas actividades estarán:

1. Sensibilización y capacitación sobre la Desconexión Laboral.
2. Capacitación en temas que fortalezcan el aprovechamiento del tiempo laboral y extralaboral, tales como mecanismos y prácticas de Desconexión Laboral.

Serán de excepción la desconexión laboral en las Situaciones que de fuerza mayor o caso fortuito, en los que se requiera cumplir deberes extra de colaboración con la empresa, o cuando sean necesarios para la continuidad del servicio o para solucionar situaciones difíciles o de urgencia en la operación de la empresa, siempre que se justifique la inexistencia de otra alternativa viable.

Esta política será publicada, divulgada y actualizada cada que se estime pertinente.



HUGO DE JESUS BEJARANO GARZÓN

REPRESENTANTE LEGAL