POLÍTICA DE MEDIOS TECNOLÓGICOS

1. INFORMACIÓN EMPRESARIAL

- **Nombre:** IT CERTIFICA, INSPECCIONES TÉCNICAS Y CERTIFICACIONES S.A.S.
- **NIT:** 900 576 858-9.
- **Domicilio y dirección:** Calle 17 N° 9ª - 33. Sogamoso - Boyacá.
- **Representante legal:** Leidy Johanna Aguilar Corredor
- **Objeto social:** Planeación y ejecución de inspecciones técnicas en instalaciones de servicios públicos y privados, basadas en normas y reglamentos en los cuales se encuentre habilitada la empresa, en general solo podrá realizar las actividades permitidas para un organismo de inspección tipo A, según la NTC ISO/IEC 17020.
- **Correo electrónico:** contacto@itcertifica.com.
- **Teléfono:** 3115990784; 3112440288.
- **Misión:** Ser una empresa íntegra, que aporte por medio de sus actividades a la seguridad, eficiencia energética y cumplimiento reglamentario de las instalaciones inspeccionadas, brindando un servicio con profesionalismo, imparcialidad e independencia, generando confianza en la prestación de cada uno de los procesos ejecutados y en busca de satisfacer las necesidades técnicas del mercado en el cual podamos incursionar, proporcionando a nuestros clientes un servicio eficiente y con altos estándares de calidad. Entrada en vigencia: 2024-01-26.
- **Visión:** En el 2029 contar con un portafolio de servicios diverso y que se ajuste a las necesidades de nuestros clientes y del mercado, el cual no afecte con la imparcialidad de la organización; igualmente, ser reconocidos en 3 departamentos adicionales a nivel nacional como un Organismo de Inspección sólido, confiable, independiente y objetivo, comprometido con el cuidado del medio ambiente, con la Seguridad y Salud de sus colaboradores, prestando servicios con los mejores estándares de Calidad. Así mismo, contar con profesionales competentes, capacitados, calificados e idóneos; con procesos internos sistematizados y con los recursos adecuados para prestar un servicio en tiempos oportunos, logrando la satisfacción del cliente y contribuyendo a que la sociedad cuente con instalaciones seguras y cuyo cumplimiento sea lo establecido por la normatividad y reglamentación aplicable. Entrada en vigencia: 2024-01-26.

Principios corporativos:

1. Respeto

Trato amable y cortésmente a las personas que me rodean, entendiendo, argumentando y, cuando se requiere, aceptando la diferencia de criterios y conceptos de los clientes, proveedores y compañeros de trabajo.

2. Responsabilidad

Soy responsable de mis labores, actividades, acciones y decisiones entendiento y asumiendo las consecuencias positivas o negativas de mis actos.

3. Honestidad

Realizo las labores con objetividad, obrando coherentemente de acuerdo a mis principios éticos y morales y a los principios y valores del Organismo.

Valores corporativos:

Compromiso

- Cumplo eficientemente con mis deberes y funciones dentro del Organismo.

Tolerancia

- Tengo la capacidad de aceptar y manejar las maneras de actuar, pensar y sentir de los demás.

Justicia

- Actuo de manera razonable, reconociendo los derechos y deberes de toda persona.

Mejora contínua

- Acepto la retroalimentación continua de las actividades desarrolladas y agradezco las oportunidades de mejorar.

Seguridad

- Ejecuto cada una de mis actividades siempre bajo el principio de mi seguridad y la de los que me rodean

2. OBJETIVO

IT CERTIFICA S.A.S, adopta la presente política para el uso de medios tecnológicos, con el propósito de regular el uso de los recursos tecnológicos y de comunicación dentro del Organismo de Inspección, asegurando que los medios tecnológicos sean utilizados de manera eficiente, segura y en cumplimiento con las actividades y valores corporativos definidos por esta empresa.

3. ALCANCE

Esta política aplica a todos los trabajadores, contratistas, proveedores, aprendices y a cualquier otra persona que tenga acceso a los sistemas de información del Organismo de Inspección.

Además, aplica a todos los equipos y sistemas informáticos - servidores, equipos de cómputo, dispositivos móviles, portátiles, sistemas de información y demás dispositivos digitales que son propiedad de la empresa y utilizados para el desarrollo de las actividades de la misma.

4. MARCO JURIDICO

- Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1072 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo

5. DEFINICIONES

- Dato Público: Es el dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados. Ejemplo: Nombres y apellidos, número de cedula de ciudadanía, datos relativos al estado civil de las personas, su profesión u oficio, su calidad de comerciante o servidor público y aquellos que pueden obtenerse sin reserva alguna.
- Dato Semiprivado: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas. Ejemplo: Datos financieros y crediticios, dirección, teléfono, correo electrónico, entre otros.
- Dato Privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información. Ejemplo: Fotografías, videos, datos relacionados con su estilo de vida, entre otros.
- 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.
- Medio tecnológico: Para los efectos de la presente política, se define medios tecnológicos a todas las herramientas, plataformas, dispositivos y sistemas que utilizan la tecnología para facilitar la comunicación, la transmisión de información, el desarrollo de actividades previamente definidas con un fin y la interacción entre personas, organizaciones y máquinas permitiendo además la creación, difusión y recepción de contenidos a través de diversos canales.

- Medio tecnológico intangible: recurso tecnológico que no tiene una forma física, es decir, no se puede tocar, pero que cumple una función específica en la transmisión, procesamiento o almacenamiento de información. Se trata de herramientas o sistemas inmateriales que permiten o facilitan la realización de actividades tecnológicas.
- Medio tecnológico tangible: es un recurso o herramienta tecnológica que tiene una forma física y que puedes ver, tocar y manipular. Estos medios se utilizan para facilitar procesos como la comunicación, el aprendizaje, la producción o el entretenimiento.
- Sistemas de información o sistema informático: conjunto organizado de elementos (personas, datos, procesos, tecnología y recursos) que se encargan de recopilar, procesar, almacenar y distribuir información para apoyar la toma de decisiones, la coordinación, el control, el análisis y la visualización de datos en una organización o entorno específico.

6. SEGURIDAD DE LA INFORMACIÓN

Con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información que se maneja a través de los medios tecnológicos, se establecen las directrices mencionadas en los apartados 9, 10 y 12 de la presente política, las cuales se generalizan a continuación:

- Acceso controlado: Los usuarios deberán utilizar credenciales (usuarios y contraseñas) personales e intransferibles para acceder a sistemas informáticos, redes o plataformas institucionales.
- Uso responsable: No se podrá acceder, modificar o divulgar información que no sea autorizada.
- Protección contra software malicioso: Se debe evitar descargar o instalar programas sin autorización o abrir correos electrónicos, enlaces o archivos sospechosos. Todo equipo deberá contar con antivirus actualizado.
- Copia y respaldo de la información: Los trabajadores deberán permitir y realizar respaldos periódicos (cuando corresponda) de la información importante, según las indicaciones dadas.
- Uso adecuado de dispositivos externos: El uso de discos externos u otros dispositivos de almacenamiento externo deberá ser aprobado por el Organismo de Inspección y revisado por el ingeniero de sistemas.
- Confidencialidad: Toda la información debe ser tratada como confidencial y no debe compartirse fuera del ámbito autorizado. Queda prohibido tomar fotografías, capturas de pantalla o grabaciones de datos sensibles sin permiso expreso.
- Reportes de incidentes: Cualquier anomalía, intento de acceso no autorizado o pérdida de información debe ser reportado inmediatamente al área de Calidad o al ingeniero de Sistemas.

7. CONTROLES DE ACCESO A LA INFORMACIÓN SEGÚN SU CLASIFICACIÓN

Para los efectos de la presente política y teniendo en cuenta la información que se manejará, se define lo siguiente:

Por medio de documento ITC-DO-JL “Contrato de transmisión de tratamiento de datos personales” se define que,

- Para el desarrollo y la prestación de los servicios en la empresa, es necesario que se realice una transmisión de la persona jurídica a la persona natural con el fin de realizar el adecuado tratamiento de los

datos personales que a esta se suministren ya sean aspirantes, trabajadores, ex trabajadores, proveedores y clientes.

- El ENCARGADO DEL TRATAMIENTO debe tener acceso y realizar el tratamiento de datos personales que se han brindado al RESPONSABLE DEL TRATAMIENTO DE LOS DATOS PERSONALES, por lo que de acuerdo con el artículo 25 del decreto 1377 de 2013 el contrato que suscriba el RESPONSABLE con el ENCARGADO para el tratamiento de datos personales bajo su control y responsabilidad señalará los alcances del tratamiento, las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales y las obligaciones del ENCARGADO para con el titular y el responsable.
- Ambas partes, de forma libre y espontánea acuerdan regular este acceso y tratamiento de datos de carácter personal de conformidad con las siguientes estipulaciones:

PRIMERO: OBJETO DEL CONTRATO. Mediante las presentes cláusulas se habilita al ENCARGADO DE TRATAMIENTO, para tratar por cuenta del RESPONSABLE DEL TRATAMIENTO, los datos de carácter personal necesarios en el ejercicio de la prestación de servicios.

SEGUNDO: IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA. Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el RESPONSABLE DEL TRATAMIENTO, pone a disposición del ENCARGADO DEL TRATAMIENTO, la información personal de aspirantes, trabajadores, ex trabajadores, proveedores, clientes y demás personal que brinde libremente información personal a la empresa IT CERTIFICA S.A.S.

TERCERO: DURACIÓN. El acuerdo tiene una duración hasta que el ENCARGADO DEL TRATAMIENTO finalice su contrato laboral con la empresa. Una vez finalice el presente contrato, el ENCARGADO DE TRATAMIENTO debe suprimir/devolver al RESPONSABLE, o devolver a otro ENCARGADO que designe el RESPONSABLE los datos personales y suprimir cualquier copia que esté en su poder.

CUARTO: OBLIGACIONES DEL ENCARGADO DE TRATAMIENTO. El ENCARGADO DEL TRATAMIENTO se obliga a:

a) Dar Tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan.
b) Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
c) Guardar confidencialidad respecto del tratamiento de los datos personales.
   Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:
d) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
e) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
f) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;
g) Actualizar la información reportada por los responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;
h) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;
i) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares;

j) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley;
k) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal; i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;
l) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;
m) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;
n) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

QUINTO: OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO. Corresponde al RESPONSABLE DEL TRATAMIENTO los deberes citados en el artículo 17 de la ley 1581 de 2012.
SEXTO: RESPONSABILIDAD DEL ENCARGADO DE TRATAMIENTO.

a) El ENCARGADO DEL TRATAMIENTO será considerado responsable del tratamiento en el caso de que destine los datos a otra finalidad, los comunique o los utilice incumpliendo el presente contrato. En estos casos, el ENCARGADO DEL TRATAMIENTO responderá de las infracciones en que hubiera incurrido personalmente.
b) El ENCARGADO DEL TRATAMIENTO indemnizará al RESPONSABLE DEL TRATAMIENTO por los daños y perjuicios, de cualquier naturaleza, que pudieran resultar del incumplimiento de las obligaciones contraídas en virtud del presente contrato.
c) A título enunciativo, y no limitativo, dicha indemnización incluirá los daños morales e imagen, costes publicitarios o de cualquier otra índole que pudieran resultar para su reparación. El ENCARGADO DEL TRATAMIENTO, asimismo, deberá responder de cualquier indemnización que a resultas de su incumplimiento tuviera que satisfacer a terceros.
d) La responsabilidad del ENCARGADO DEL TRATAMIENTO incluirá, además, el importe de cualquier sanción administrativa y/o resolución judicial condenatoria que pudiera resultar contra el RESPONSABLE DEL TRATAMIENTO, como resultado del incumplimiento del ENCARGADO DEL TRATAMIENTO de la normativa y de las obligaciones exigidas en el presente contrato. La indemnización comprenderá, además del importe de la sanción y/o resolución judicial, el de los intereses de demora, costas judiciales y el importe de la defensa del RESPONSABLE DEL TRATAMIENTO en cualquier proceso en el que pudiera resultar demandada por cualquiera de las causas anteriormente expuestas.

SÉPTIMO: CONTROLES Y AUDITORÍA. El RESPONSABLE DEL TRATAMIENTO, en su condición, se reserva el derecho de efectuar en cualquier momento los controles y auditorías que estime oportunos para comprobar el correcto cumplimiento por parte del ENCARGADO DEL TRATAMIENTO. Por su parte, el Encargado deberá facilitar al RESPONSABLE DEL TRATAMIENTO los registros que se requieran para el adecuado cumplimiento de dichos controles y auditorías.

Se define a los encargados del tratamiento como personas autorizadas a las siguientes:

Nombre	Cargo	Responsable de
Jessica Yurley León Mojica	Analista administrativo	Los datos de trabajadores y contratistas

8. MEDIOS TECNOLÓGICOS

Los medios tecnológicos de los que dispone el Organismo de Inspección IT CERTIFICA SAS y que serán de aplicación en esta política son:

8.1. Medios tecnológicos tangibles

- Equipos de computo propiedad de la empresa y asignados a un responsable para la ejecución de sus actividades
- Servidores de almacenamiento y procesamiento
- Cámaras digitales propiedad de la empresa y asignados a un responsable para la ejecución de sus actividades
- Celular para uso corporativo
- Impresora y escáner de uso común
- Circuito cerrado de televisión para videovigilancia dentro de las instalaciones de la empresa
- Televisor para videoconferencias
- Discos duros

8.2. Medios tecnológicos intangibles

- Software de servicio de inspección
- Servidor de carpetas compartidas
- Página web
- Redes sociales corporativas
- Contenidos digitales
- Publicidad y maerketing
- Huellero biométrico digital

9. RESPONSABILIDADES DEL ORGANISMO DE INSPECCIÓN IT CERTIFICA SAS CON RESPECTO A LOS MEDIOS TECNOLOGICOS

a) Restringir o prohibir el uso de los medios tecnológicos a cualquier usuario en caso de que se demuestre alguna violación de esta política o de alguna ley.
b) Monitorear cuando así lo vea necesario, cualquiera de los medios tecnológicos dispuestos a través revisiones, informes, indicadores o auditorías para responder a cualquier acción que atente contra la integridad, disponibilidad, seguridad y desempeño correcto de los mismos y de las actividades para los cuales han sido dispuestos, mediante la negación, restricción de acceso a usuarios o sistemas, aislamiento y desconexión de equipos o servicios.

c) Garantizar el respaldo y la restauración de los sistemas de información en caso de fallas eventuales con el objetivo de permitir la continuidad de las actividades de inspección a cada cargo.
d) Garantizar que las versiones de los sistemas operativos usados en la empresa estén actualizados a las últimas versiones con él fin de evitar que alguna vulnerabilidad detectada, pueda ser aprovechada por un virus o atacante.
e) Mantener los antivirus siempre actualizados y tomar las medidas correspondientes cuando se detecte una amenaza de virus.
f) Avalar la contratación de cualquier servicio tecnológico requerido, incluyendo, pero sin limitar, internet, servicios en nube, servidores, equipos de cómputo, Licencias, telefonía, impresión y otros servicios externos.
g) Garantizar el soporte y mantenimiento sobre recursos y servicios informáticos (Software, hardware, equipos, almacenamiento y hosting, entre otros).
h) Utilizar los medios tecnológicos en pro del desarrollo de las actividades diarias para las cuales fue creado el Organismo de Inspección
i) Aplicar los medios tecnológicos que considere apropiados para la mejora de los procesos y la garantía de la seguridad de los trabajadores, contratistas y demás personal que se encuentre dentro de las instalaciones en algún evento desafortunado.
j) Encargarse de las labores de reparación y/o mantenimiento de las impresoras, equipos de cómputo y cualquier otro medio tangible o intangible
k) Velar porque el servicio de impresión sea utilizado para actividades laborales y uso exclusivo del Organismo de Inspección.
l) Asignar a cada usuario un usuario y clave de acceso al software de inspección, servidor de carpetas compartidas y demás servicios informáticos que éste, por la naturaleza de su cargo, requiera.
m) Salvaguardar los datos biométricos digitales obtenidos para el ingreso y salidas de los trabajadores una vez se cuente con la autorización explicita por el titular para su tratamiento y haya sido informado de la finalidad de los mismos, la cual es verificar el cumplimiento de las obligaciones contractuales establecidas como horas de ingreso, descansos, salidas y/o ausentismos laborales.

10. RESPONSABILIDADES DE LOS TRABAJADORES Y CONTRATISTAS CON RESPECTO A LOS MEDIOS TECNOLOGICOS

a) Garantizar el uso de los medios tecnológicos de manera responsable y ética.
b) Informar a su jefe inmediato de los incidentes relacionados con el uso indebido de los sistemas de información.
c) Permitir el acceso a los correos corporativos, celulares y equipos de computo asignados en caso de que se requiera por parte del Organismo de Inspección.
d) Mantener las credenciales tal cual se asignaron y en caso de necesidad de modificar, reportar al responsable del área de Calidad, para que actualice la información. Estas credenciales son para uso estrictamente personal e intransferible. La responsabilidad en su manejo recae exclusivamente en el usuario a quién se le asignen.
e) Utilizar únicamente las credenciales que fueron asignadas; ningún trabajador debe usar las credenciales de otro usuario.

f) Recibir toda la información con respecto a la mejora de medios tecnológicos y aplicarla para el desarrollo de sus actividades a cargo.
g) Propender por el cuidado y preservación de las herramientas informáticas y computadores asignados.
h) Evitar consumir alimentos y tomar bebidas cerca del equipo asignado. Un incidente de este tipo puede afectar su funcionamiento e incluso dañarlo.
i) Informar y entregar al dpto. administrativo los recursos y servicios informáticos que no esté utilizando en su trabajo.
j) Los medios tecnológicos tangibles asignados al empleado están bajo su responsabilidad. En caso de daño, perdida o hurto, el trabajador deberá cumplir con los lineamientos establecidos por el proceso de Gestión de Recursos.
k) En caso de requerir retirar de la empresa cualquier medio tecnológico no asignado al cargo, es deber del trabajador y/o contratista pedir las autorizaciones necesarias.
l) Cualquier trabajador y/o contratista que sea responsable de un contrato en el cual se involucren computadores, servidores, licencias y periféricos, sean propios o de propiedad de un tercero, debe solicitar autorización al dpto. administrativo para el uso y transporte de estos dentro de las instalaciones.
m) Mantener almacenada en su carpeta de “Datos”, la información resultado de las actividades a su cargo para garantizar copias de seguridad. La información que se encuentre almacenada en otra carpeta podrá ser eliminada en el momento de realizar los mantenimientos preventivos o correctivos que sean necesarios.
n) Permitir las copias de seguridad de la información a las que haya lugar en los discos duros dispuestos por el Organismo de Inspección para dicha labor.
o) Solicitar, en caso de que requiera, al área de Calidad, la información correspondiente a copias de seguridad o archivo de documentación en los discos duros para el desarrollo de alguna actividad particular. Por ningún motivo hacer uso de los discos duros sin previa autorización.
p) Usar el servidor de carpetas compartidas para mantener información no confidencial que puede utilizarse o consultarse por mas de una persona y que sea únicamente de uso laboral.
q) Los equipos portátiles son responsabilidad de la persona a quien fueron asignados mientras esté vinculado laboralmente a la organización.
r) Utilizar el servicio de impresión para actividades laborales y uso exclusivo del Organismo de Inspección.
s) Realizar un uso razonable del papel e imprimir siempre y cuando sea estrictamente necesario.
t) Cualquier dispositivo de colaboración asignado a un empleado, como teléfono, cámara, audífonos, diademas, entre otros, quedará bajo su responsabilidad y deberá ser usado para actividades laborales.

11. DECLARACIÓN DE USO DE MEDIOS TECNOLÓGICOS

IT CERTIFICA SAS provee el acceso a todo el personal a fuentes de información y promueve un ambiente digital que fomente la mejora de los procesos, la efectividad, eficiencia y eficacia en la prestación del servicio y la seguridad de los trabajadores contratistas, proveedores, aprendices y a cualquier otra persona que se encuentre dentro de las instalaciones del Organismo de Inspección. En este sentido el trabajador, contratista, proveedor, cliente declara que conocer y acepta las siguientes clausulas:

a) La empresa cuenta con un circuito cerrado de televisión, lo cual implica el uso de imagen del material y datos tomados por este sistema, por lo cual, se debe contar con la autorización por parte de trabajadores, contratistas y

demás personal que por alguna razón permanezca a las instalaciones del Organismo de Inspección para el uso de estos datos siendo su finalidad el monitoreo de las instalaciones por parte del empleador en procura de la seguridad y armonía del establecimiento de tal forma que los videos del mismo gozan de plena autenticidad y valoración probatoria. Igualmente tengo conocimiento de que soy monitoreado y/o grabado incluso en horas de descansos laborales, actividades de recreación o periodos de refrigerio.

a) La empresa debe informar acerca de la zona videovigilada, en caso de que ingrese proveedores, clientes u otro personal a las instalaciones.
b) La empresa cuenta con un sistema de autenticación biométrico como forma de identificación y control de acceso (este registro de la huella digital, se realiza una única vez el día de la contratación o en la implementación de dicha metodología). Por medio de este sistema se valida hora de ingreso, descansos y hora de salida, por lo tanto, la empresa hará uso y lectura de los datos suministrados a través de este medio, para efectos de liquidar horas extras, validación de ausentismos y demás finalidades históricas, estadísticas o científicas.
c) Las líneas telefónicas como celulares corporativos son de propiedad exclusiva de la empresa y están dispuestas únicamente para el uso de las actividades laborales, razón por la cual la empresa se reserva el derecho de grabar y monitorear dichas líneas en aras de propugnar por la mejoría y calidad del servicio.
d) El acceso a correos electrónicos personales y/o redes sociales está prohibido desde las terminales de la empresa, con el fin de prevenir los virus informáticos y proteger las redes internas. La empresa se reserva el derecho de monitoreo de toda la información puesto que es de exclusividad de la misma.
e) El acceso a las redes sociales institucionales es exclusivo para las labores de publicidad previamente autorizado por el empleador y solo a la persona asignada para dicha labor.
f) Está autorizado únicamente el uso del correo institucional que aporta la empresa para el desarrollo y labor encomendada.
g) La empresa puede manejar información y comunicación de carácter empresarial de grupos autorizados por medios digitales como WhatsApp, puesto que al ser un grupo de trabajo la información que allí contiene es de carácter semi- privado por lo tanto en el caso que se requiera el uso de estas conversaciones como prueba no se estará vulnerando ningún derecho a las personas.

12. PROHIBICIONES EN EL USO DE LAS REDES, LAS COMUNICACIONES ELECTRÓNICAS Y SISTEMAS DE INFORMACIÓN

A continuación, se enuncian las acciones prohibidas en el uso de las redes, comunicaciones electrónicas y demás medios tecnológicos que se vean involucrados. Lo cual es meramente enunciativa más no taxativa, de tal manera que cualquier actividad que, aunque no se encuentre en esta lista, cause perjuicio a los sistemas de información, a las personas o a la empresa, se considerará un uso indebido y estará sujeta a las acciones disciplinarias que la empresa estime conveniente:

a) No se permitirá ningún intento de vulnerar o de atentar contra los sistemas de protección o de seguridad de la red. Ante cualquier evento de este tipo el Organismo de Inspección procederá a ejecutar cualquier acción de carácter administrativo, laboral, penal y/o civil que corresponda.

b) No está permitida la operación de software para la descarga y distribución de archivos de música, videos y similares. Cualquier aplicación de este tipo que requiera ser utilizada, deberá ser solicitada previamente para su evaluación.
c) No está permitido almacenar archivos de música, videos y similares de índole personal en el disco duro del equipo asignado ni en el servidor de carpetas compartidas.
d) Usar las comunicaciones electrónicas para acosar o amenazar a compañeros, jefes o externos.
e) Usar las comunicaciones electrónicas para revelar información privada sin la autorización explícita del Organismo de Inspección.
f) Alterar o falsificar de manera fraudulenta los registros del Organismo de Inspección, incluyendo registros computarizados, permisos, documentos de identificación, u otros documentos o propiedades con los medios tecnológicos asignados.
g) Usar las comunicaciones electrónicas para dañar o perjudicar de alguna manera los medios tecnológicos disponibles.
h) Usar las comunicaciones electrónicas para apropiarse de los documentos de otros usuarios.
i) Lanzar cualquier tipo de virus, gusano o programa de computador cuya intención sea hostil, destructiva o intente vulnerar la seguridad de la red informática y sus sistemas de información.
j) Descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando un computador de la Organización.
k) Transportar o almacenar material con derechos de propiedad intelectual o material no permitido usando los equipos o las redes del Organismo de Inspección.
l) Utilizar cualquier sistema de información de la Organización para acceder, descargar, imprimir, almacenar, reenviar, transmitir o distribuir material no permitido o correos electrónicos de tipo “cadenas”.

13. MEDIDAS DISCIPLINARIAS Y CANALES DE CONSULTAS Y RECLAMOS

13.1. Medidas disciplinarias

Cuando se incumpla con alguna de las responsabilidades o no se tenga en cuenta las prohibiciones definidas en la presente política, el Organismo de Inspección IT CERTIFICA SAS, establece:

- Amonestación verbal o escrita: Para faltas leves o primeras veces quedando registrado como advertencia.
- Suspensión del acceso a medios tecnológicos: Temporal o permanente.
- Sanciones laborales: Llamados de atención formales en el trabajo.
- Suspensión temporal: Prohibición de ingresar al sistema o al lugar de trabajo por un tiempo determinado con los respectivos descuentos salariales.
- Terminación del contrato: En casos graves, como hackeos, robo de información, acoso en línea, etc.
- Acciones legales: Si se infringen leyes, por ejemplo, delitos informáticos, uso de datos personales sin consentimiento.

13.2. Canales de consultas y reclamos

El Organismo de Inspección IT CERTIFICA SAS, dispone de los siguientes medios para la recepción y atención de peticiones, consultas, quejas y reclamos atendiendo a lo establecido en el procedimiento interno de peticiones,

quejas, reclamos y sugerencias ITC-PD-MQ, el cual también es posible consultar detalladamente a través de la página web

Las PQRS´s y Aps se pueden radicar por medio de:

- Comunicación escrita dirigida a IT CERTIFICA SAS en puntos de recepción de información: Calle 17 N° 9ª - 33. Sogamoso – Boyacá; Cra 6 N° 47ª-40 Local 028 en Tunja – Boyacá; Carrera 80 No 39-159 Centro ejecutivo Nutibara de la ciudad de Medellín-Antioquia;
- Correos electrónicos contacto@itcertifica.com; calidaditcertifica@gmail.com
- Comunicación telefónica a 310 341 3517, 313 208 7453, 3115990784 y 3112440288 con los responsables del tratamiento de los datos.
- Solicitudes a través de la página web del Organismo de Inspección: http://itcertifica.com/sitio/proteccion-de-datos-2/ o ingresando la pestaña de "PQRS Y APELACIONES" y diligenciando todos los datos que se solicitan.

Las peticiones, quejas, reclamos, sugerencias y apelaciones deben ser realizadas por el propietario de la instalación o cliente quien firma la aceptación de oferta. Es posible recepcionar solicitudes por parte de terceros y realizar el correspondiente análisis de la manera en que se debe dar respuesta de acuerdo a lo establecido en el presente procedimiento.

14. EJERCICIO DE LOS DERECHOS DE LOS TITULARES DE LOS DATOS

De acuerdo con lo contemplado por la normatividad vigente aplicable en materia de protección de datos, los siguientes son los derechos de los titulares de los datos personales:

a. Acceder, conocer, actualizar y rectificar sus datos personales suministrados a IT CERTIFICA S.A.S 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.
b. Solicitar la prueba de la autorización otorgada a la IT CERTIFICA S.A.S para el tratamiento de datos, mediante cualquier medio válido, salvo en los casos en que no es necesaria la autorización.
c. Ser informado por IT CERTIFICA S.A.S, previa solicitud, respecto del uso que les ha dado a sus datos personales.
d. Presentar ante la Superintendencia de Industria y Comercio, o la entidad que hiciere sus veces, quejas por infracciones a lo dispuesto en la ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen, previo trámite de consulta o requerimiento ante IT CERTIFICA S.A.S.
e. 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.
f. Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento, al menos una vez cada mes calendario, y cada vez que existan modificaciones sustanciales de la presente política que motiven nuevas consultas.

Estos derechos podrán ser ejercidos por:

- El titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición IT CERTIFICA S.A.S.
- El representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.
- Otro a favor o para el cual el titular hubiere estipulado.

15. PUBLICACIÓN

2025-04-28

16. VIGENCIA

La presente política de tratamiento de datos personales rige a partir de su firma y complementa las políticas asociadas, con vigencia indefinida.

Cualquier cambio sustancial en la política de medios tecnológicos, se comunicará de forma oportuna a través de los medios habituales de contacto y/o a través de la página web http://itcertifica.com/sitio.

Todos los usuarios deberán actuar de acuerdo con estos lineamientos, al reglamento interno de trabajo, así como a las leyes nacionales o internacionales pertinentes. El incumplimiento de esta política puede resultar en la negación de acceso a los sistemas de información de la Organización o a otras acciones disciplinarias o legales. Es un compromiso de todas las personas a quien aplique esta política, entender y dar cumplimiento a los lineamientos consignados en el presente documento, y acatarlas durante el desarrollo de sus actividades.

LEIDY JOHANNA AGUILAR CORREDOR

Firmado digitalmente por LEIDY JOHANNA AGUILAR CORREDOR
Fecha: 2025.04.28 13:22:21 -05'00'

Ing. LEIDY JOHANNA AGUILAR CORREDOR
Representante Legal

Entrada en vigencia: 2025-04-28