



NUE 16-DDP-2020 (DH)

██████████ contra Martínez Criollo

Resolución Definitiva

INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA: San Salvador, a las quince horas con cincuenta minutos del veinte de octubre de dos mil veintiuno.

**Descripción del caso:**

I. El presente procedimiento sancionador fue promovido por ██████████ ██████████ en contra de la actuación del -ex empleado público- ██████████ ██████████ Técnico de la Unidad de Desarrollo Tecnológico Institucional del Ministerio de Trabajo y Previsión Social (MTPS) por la supuesta comisión de la infracción clasificada como muy grave contenida en el artículo 76 letra “b” de la Ley de Acceso a la Información Pública (LAIP), consistente en: “*entregar o difundir información reservada o confidencial*”.

La denunciante, manifestó que el denunciado en su calidad de Técnico de la Unidad de Desarrollo Tecnológico Institucional del MTPS accedió y posteriormente difundió su información confidencial consistente en: “*imágenes íntimas de su cuerpo las cuales se encontraban en la computadora asignada a su compañero de vida el señor ██████████ ██████████ empleado de la Unidad de Archivo Institucional del MTPS*”. Respecto a ello, señaló que compartió las imágenes de forma voluntaria con su compañero de vida quien le informó que la información iba a ser tratada en su computadora del MTPS, para posteriormente ser trasladada a un disco duro propiedad de ambos. No obstante, tuvo conocimiento que ██████████ ██████████ en la calidad mencionada accedió sin previo aviso y sin el consentimiento del señor ██████████ ██████████ a las imágenes que había compartido con su pareja, a través de una aplicación informática “anydesk” sustrayendo las imágenes y difundiéndolas al señor ██████████ ██████████ Jefe de la Unidad de Desarrollo Tecnológico Institucional del MTPS, sin contar con su consentimiento o el de su pareja para realizar tal divulgación.



Unido a lo anterior, expuso que el equipo informático que resguarda sus imágenes personales se encuentra en posesión de la Unidad de Desarrollo Tecnológico Institucional del MTPS, sin contar -a su criterio- con garantías efectivas de su resguardo u otros fines no autorizados.

En relación a los hechos descritos solicitó se iniciará el procedimiento administrativo sancionador en contra del denunciado y se adoptarán las medidas cautelares siguientes: “i) se requiera al titular de la institución [REDACTED] a la licenciada [REDACTED] [REDACTED] en su calidad de Jefa de la Unidad Jurídica y al señor [REDACTED] [REDACTED] en su calidad de Jefe de la Unidad de Desarrollo Tecnológico Institucional que se adopte medidas especiales de resguardo del equipo informático y de sus imágenes personales en ese ente obligado y ii) se informe de la tramitación de este procedimiento administrativo al titular de MTPS, a la Jefa de la Unidad Jurídica y al Jefe de la Unidad de Desarrollo Tecnológico Institucional”.

En cuanto, a la apariencia de buen derecho y el peligro en la demora, presupuestos básicos para la adopción de medidas cautelares, indicó que de no adoptarse estas medidas podría seguirse vulnerando su integridad personal al compartir sus imágenes con más personal del MTPS sin su autorización, además, de ser evidente que el acceso y divulgación de dicha información fue sin su conocimiento como titular de la misma, en contraposición a las normas establecidas en la LAIP.

Como elemento probatorio de los hechos denunciados incorporó: acta emitida a las doce horas del siete de octubre de este año, suscrita en la Unidad de Gestión Documental y Archivo del MTPS, en donde -adujo- consta la sustracción y posterior difusión de sus imágenes personales y las de su pareja sentimental.

II. Este Instituto admitió la denuncia por el supuesto cometimiento de la infracción antes mencionada, y designó a la comisionada Claudia Liduvina Escobar Campos, para instruir el procedimiento; sin embargo, el caso fue reasignado a la comisionada Daniella Huevo Santos, para continuar con su instrucción y emitir un proyecto de resolución.

En el mismo, conforme a las facultades conferidas a este Instituto en el artículo 85 de la LAIP y a lo establecido artículos 50, 51 y 57 letra “k” Ley Integral para una Vida Libre de

Violencia para las Mujeres (LEIV) se dictaron las medidas cautelares solicitadas por la denunciante en su escrito de solicitud de inicio de procedimiento sancionador, consistentes en: “a) informar al Ministro de Trabajo y Previsión Social de la tramitación de este procedimiento administrativo sancionador, en concordancia a lo dispuesto en el artículo 85 letra “a” de la LAIP y b) que la Unidad de Desarrollo Tecnológico del MTPS adopte las medidas tecnológicas de resguardo adecuadas, suficientes, no excesivas y exactas que tengan como fin prevenir el acceso no autorizado a las imágenes de la denunciante”.

La segunda de las medidas citadas en el párrafo que antecede se tuvo por cumplida mediante auto de las once horas con cuarenta minutos del diecinueve de mayo de este año.

III. En plena observancia y respeto al derecho de defensa que debe imperar en todo procedimiento, de conformidad con el artículo 88 de la LAIP, se corrió traslado al denunciado, para que rindiera su informe de defensa.

En su informe, sobre los hechos que dieron origen a este procedimiento, manifestó que el 28 de septiembre de 2020, se recibió correo electrónico a la dirección electrónica asignada al licenciado [REDACTED] Jefe de la Unidad de Desarrollo Tecnológico Institucional, por parte de la licenciada [REDACTED] Jefa de la UGDA en el cual solicitaba: “...reparación de servicios de internet e intranet para la oficina del archivo...”; detallando dentro del requerimiento el equipo asignado al Colaborador [REDACTED] por lo que, en fecha 7 de octubre de 2020, el soporte del equipo técnico fue asignado a su persona y otro compañero .

En esa línea, agregó que el día 7 de octubre de 2020, se brindó el soporte técnico por medio de la aplicación “Anydesk” la cual funciona como una herramienta que permite desarrollar mantenimiento en los equipo desde la Unidad de Desarrollo Tecnológico Institucional, motivo por el cual, se encontraba en dicha Unidad al momento de brindar revisión a los equipos informáticos y en constante comunicación telefónica con la licenciada [REDACTED] Jefa de la Unidad solicitante para la realización de pruebas y dado que el Colaborador [REDACTED] no se encontraba en la Unidad el día de la revisión del equipo fue la licenciada [REDACTED] quien autorizó la revisión. Al proceder a la revisión del equipo-continuó manifestando-, se habilitó la última carpeta que fue utilizada por el



Colaborador desplegándose en este caso la carpeta “descargas” en donde se encontraron las imágenes sobre la base de las cuales se ha dado apertura a este procedimiento.

Ante ello, expuso que procedió a hacer de conocimiento de su Jefe inmediato el hallazgo, por lo que, se trasladaron a la UGDA del MJSP y se levantó un acta en presencia de la licenciada [REDACTED] Jefa de la UGDA, el licenciado [REDACTED] Jefe de la Unidad de Desarrollo Tecnológico Institucional, [REDACTED] Colaborador de la UGDA y [REDACTED] Colaborador de Recursos Humanos; documento que fue utilizado como base para dar inicio a este procedimiento y que no se encuentra firmado por ninguno de los presentes- la cual adjuntó a su escrito-, en tal documento además, consta que el equipo informático quedó en posesión de la Unidad de Desarrollo Tecnológico Institucional y los archivos tecnológicos quedan resguardados en el mismo, asignándole una contraseña ya que el equipo carecía de esta.

En ese orden, indicó que el 26 de octubre de 2020, se recibió memorando de referencia DSG-RRHH-IF-0529-INT-2020, suscrito por la licenciada [REDACTED] Jefa del Departamento de Recursos Humanos a través del cual, requirió a su persona y el licenciado [REDACTED] un informe técnico de lo sucedido el 7 de octubre de dos 2020, en la UGDA junto el soporte técnico y documental de lo evidenciado. De tal manera, agregó que procedió a enviar lo solicitado a su jefatura inmediata quién emitió respuesta mediante memorando con referencia DE-ITI-WC-139-INT-2020 la cual contenía el informe técnico solicitado, no así, las imágenes físicas y electrónicas solicitadas, indicando que el equipo técnico seguiría en resguardo de la Unidad de Desarrollo Tecnológico Institucional.

Por otra parte, en relación a la comisión de la conducta antijurídica que se le atribuye tipificada en el art. 76 letra “b” del apartado de las infracciones muy graves de la LAIP mencionó que los hechos antes descritos no se encajan con el supuesto típico contenido en la disposición en referencia, en tanto este exige que la persona entregue o difunda información entendiéndose por entrega la acción de poner en poder de alguien, la cual se configura con el hecho de reproducir la información y materialmente entregársela a otra persona; por otro lado, indicó que la difusión debe entenderse como la transmisión de la información dando la posibilidad a que las personas puedan verla por medios de fácil acceso.

En ese sentido, agregó que de los hechos descritos no se puede entender configurada la infracción puesto que las imágenes encontradas en la computadora del señor [REDACTED] no fueron sustraídas ni difundidas, sino que únicamente se limitó a dar aviso a su Jefe inmediato del incumplimiento al artículo 34 de las Políticas y Procedimientos de Controles Generales de los Sistemas de Información emitidas por el MTPS, evidenciado en el equipo del señor [REDACTED]

Por otro lado, mencionó que las imágenes encontradas en la computadora del señor [REDACTED] se les ha dado el tratamiento de información confidencial en respeto al derecho a la intimidad de las personas involucradas. También, reiteró que el ingreso a la computadora que contenía las imágenes confidenciales fue autorizado por su Jefe inmediato el licenciado [REDACTED] quien le encomendó brindar soporte técnico a dicho equipo y la jefa de la UGDA del MTPS quien autorizó el acceso al mismo como jefa del señor [REDACTED]

A efecto de probar lo mencionado en su informe de defensa ofreció como medios probatorios los siguientes: "a) copia de correo electrónico de fecha 28 de septiembre de 2020, enviado por la licenciada [REDACTED] Jefa de Gestión Documental y Archivo dirigido al licenciado [REDACTED] Jefe de la Unidad de Desarrollo Tecnológico institucional, en donde se requiere soporte técnico al equipo de la Unidad de Gestión Documental y Archivo, entre ellas la de [REDACTED] b) copia de correo electrónico de fecha 5 de octubre de 2020, donde se reitera la solicitud de soporte técnico por la licenciada [REDACTED]; c) copia de correo electrónico de fecha 7 de octubre de 2020, donde se le requiere el soporte técnico solicitado; d) Acta de las doce horas del día 7 de octubre de 2020, debidamente firmada; en la cual se establece el hallazgo de las imágenes con contenido pornográfico, su resguardo y custodia; e) copia de correo electrónico de fecha 7 de octubre de 2020, enviado por [REDACTED] colaboradora de la Unidad de Gestión Documental y Archivo en el cual se les remite el Acta del párrafo que antecede debidamente firmada; f) Memorando referencia DSG-RRHH-IF-0529-INT-2020, suscrito por la licenciada [REDACTED] Jefa del Departamento de Recursos Humanos, en la cual se solicitó al licenciado [REDACTED] y a su persona informe técnico de lo sucedido el 7 de octubre de 2020, en la Unidad de Gestión Documental y Archivo,



requiriendo además la remisión en forma documental y electrónica de las imágenes encontradas en el equipo asignado al colaborador [REDACTED] g) copia de correo electrónico de fecha 29 de octubre 2020, en el cual rindió informe técnico de lo encontrado en fecha 7 de octubre de 2020, en el equipo informático de [REDACTED] [REDACTED] el cual dirigió a su jefe, licenciado [REDACTED] h) Memorando referencia DE-UDT-WC-139-INT-2020, en la cual se rindió el informe técnico solicitado, pero, en relación a la solicitud de remisión de los archivos encontrados de forma documental y electrónica, no fue remitida, pero se estableció "...El equipo seguirá en resguardo de esta unidad y a disposición de las autoridades y/o comisión pertinente para que verifiquen la información emitida, si así lo desean y no se eliminará ningún archivo, hasta que haya alguna otra indicación [...]; y i) Políticas y Procedimientos de los Controles Generales de los Sistemas de Información emitidas por el Ministerio de Trabajo, para que se verifique el art. 34 que ampara la realización del acta ya mencionada por incumplimiento a dicha disposición normativa".

IV. La audiencia oral, se desarrolló a través de la plataforma de "google meet", en aplicación de lo establecido en los artículos 3 letra "g" de la LAIP y 18 de la Ley de Procedimientos Administrativos (LPA). En este acto, comparecieron la denunciante [REDACTED] a través de su representante la Licenciada [REDACTED] [REDACTED] calidad acreditada en etapas anteriores del procedimiento y el denunciado [REDACTED]

Previo el inicio de la respectiva audiencia, durante la etapa de incidentes, la representación de la denunciante solicitó la reprogramación de la audiencia en aras a la no comparecencia de los testigos ofertados por su persona en fecha 18 de mayo de los corrientes, agregando que dichos testigos resultan hostiles y es necesaria la intervención de esta Administración para su comparecencia, amparándose en lo dispuesto en el artículo 362 del Código Procesal Civil y Mercantil (CPCM). Acto seguido se corrió traslado al denunciado respecto al incidente planteado, quien no mostró impedimento alguno para la celebración de la referida audiencia.

Ante ello, el Pleno de este Instituto procedió a deliberar respecto al incidente planteado, dando no lugar a dicho incidente en razón de lo dispuesto en los artículos 7 y

360 del CPCM, en los cuales se regula el principio de aportación de prueba y la obligación de la parte que les propuso de asegurar su comparecencia a través del acto de comunicación donde se plasmó el señalamiento de la respectiva audiencia. Respecto de tal decisión, la parte denunciante solicitó la revocatoria, deliberando el Pleno, al respecto como no procedente el respectivo recurso en aras a que esta Administración realizó las labores necesarias para notificar a las partes dentro del presente procedimiento, siendo labor de la denunciante, en este caso, garantizar la comparecencia de sus testigos, culminando con ello la etapa de incidentes.



Posteriormente, se dio lugar a la etapa probatoria donde las partes no agregaron documentación adicional a la que ya se encontraba incorporada dentro del expediente de este procedimiento.

En la etapa de alegatos, la parte denunciante alegó la comisión de la conducta infractora exponiendo que el denunciado puso a disposición de otras personas el contenido consistente en las fotografías íntimas de su representada encontradas en el equipo informático institucional de su compañero de vida.

Por su lado, el denunciado alegó que, de acuerdo a las Políticas y Procedimientos de los Controles de los Sistemas de Información emitidas por el MTPS era su labor informar a su jefatura inmediata del hallazgo, puesto que el preservar contenido pornográfico dentro del equipo institucional se concibe como una prohibición de acuerdo a dichas Políticas.

En etapa de alegatos, finales las partes reiteraron el contenido de sus argumentos iniciales. Por su lado, dentro de la etapa de consultas aclaratorias por parte del Pleno de este Instituto, la comisionada Daniella Huevo preguntó a la apoderada de la denunciante *“Cuando se habla de divulgación del material contenido en la máquina, no me queda claro dónde se divulgó o a quiénes se divulgaron”*, contestándole que los testigos serían quienes manifestarían si habían o no visto las fotografías, dado que se interpreta del Acta de hallazgo de las imágenes que los firmantes tuvieron acceso a las imágenes. Sobre ello, agregó el denunciado que él al haber dado aviso a su jefatura, se reportó a Recursos Humanos la situación, por lo que se optó por el levantamiento de acta sin necesidad de ver las imágenes de la denunciante.



Posteriormente, la comisionada Huezco consultó al denunciado “¿En algún momento se individualizó a la persona dueña de las imágenes dentro de la computadora?”, contestándole de manera negativa, puesto que con el solo hecho de que se tratara de contenido pornográfico se dio el respectivo reporte a la jefatura inmediata del denunciado. Finalizando de esta forma la audiencia oral.

### *Análisis del caso.*

Una vez establecido lo anterior, el orden lógico con el que se estructura esta resolución será el siguiente: **I.** En primer lugar, se hará referencia a la potestad sancionatoria del Estado y del principio de legalidad, como principios que rigen el ejercicio de dicha facultad por parte de este Instituto; **II.** Posteriormente, se expondrán breves consideraciones sobre la infracción muy grave de entregar o difundir información reservada o confidencial; **III.** Luego, se someterán a un test de determinación los datos que a consideración del denunciante son confidenciales para determinar si procede dicha clasificación conforme a la Constitución, la LAIP y Tratados Internacionales; **IV.** Se analizarán los medios de prueba ofrecidos por las partes en este procedimiento; **V.** Determinados estos aspectos, se examinará si la actuación del denunciado se encontraba amparada en los supuestos establecidos en la LAIP y la normativa aplicable al caso; y **VI.** Con dichos elementos, se concluirá si las actuaciones del denunciado encajan al cometimiento de la infracción objeto de la causa conforme a los hechos probados.

**I. A.** La potestad sancionadora del Estado, conocida como *ius puniendi*, y concebida como la capacidad estatal de ejercer un control social coercitivo sobre actos ilícitos. Esta potestad se despliega, por una parte, en la rama del Derecho Penal —potestad penal judicial— y, por otra, en la Administración Pública. Esta materialización del *ius puniendi* en el campo administrativo se denomina potestad sancionadora de la Administración.

La principal justificación de la potestad sancionadora, ejercida por entes administrativos, atiende a razones pragmáticas, pues es necesaria para el cumplimiento de la finalidad última de la administración: “garantizar el mantenimiento del propio orden jurídico, el de la sociedad en conjunto, y el de la misma administración mediante la represión de todas

aquellas conductas contrarias al mismo”. (Fallo: Sala de lo Contencioso Administrativo: 149-M-99, 19/12/2000).

Asimismo, la actividad de los administrados es controlada y seguida por la Administración Pública, por medio de técnicas permitidas, justificadas por la posibilidad de tutelar los intereses sociales, de ahí que pueda imponer sanciones administrativas, poniendo actitudes lesivas —acciones u omisiones— a la esfera jurídica de los administrados.

Es dable resaltar el efecto disuasivo que la sanción, al igual que la pena en el ámbito penal, trae aparejada para el infractor de una norma. En ese sentido, a través de la corrección de conductas al margen de la ley —que pueden ocasionar consecuencias perniciosas a los beneficiados por ésta— se pretende reorientar actitudes que desde un inicio se perfilaban arbitrarias, a caminos iluminados por la legalidad, como el restablecimiento de la seguridad jurídica.

Así, sobre la base de los artículos 14 de la Constitución con relación al 58 letra “e” de la LAIP, este Instituto puede intervenir punitivamente en la esfera jurídica de los servidores públicos que provoquen una lesión o daño a los derechos que garantiza la mencionada ley, considerados estos como derechos fundamentales de los administrados, siempre que tales comportamientos se encuentren tipificados en el referido cuerpo normativo como infracciones plausibles acreedoras de una sanción de carácter pecuniario.

Dentro de esta potestad administrativa sancionadora, se encuentran fijados fines y principios que deben regir la valoración de los hechos e interpretación de las normas. Entre estos principios se encuentran: el principio de legalidad, lesividad del bien jurídico, culpabilidad y la prohibición de doble juzgamiento, que en doctrina se han denominado como el programa penal de la Constitución.

**B.** La jurisprudencia constitucional de nuestro país, que en esta ocasión hacemos nuestra, establece que el principio de legalidad en el ámbito sancionador, constituye una exigencia de seguridad jurídica que no sólo requiere el conocimiento previo de los delitos o infracciones y de las penas o sanciones, sino que también constituye una garantía política hacia el individuo de que no puede ser sometido a penas o sanciones que no hayan sido



establecidas previamente, evitando así los abusos de poder. (Fallo: Sala de lo Constitucional, Proceso de Amparo de referencia 117-2003, 15/06/2004).

Es así, que el mencionado principio trae aparejadas implicaciones para la elaboración, interpretación y aplicación de la LAIP, en el sentido de que establece condiciones para la imposición de sanciones por infracciones a la Ley, tales como: i) que una ley describa la infracción y su punición; ii) que la ley no sea anterior al hecho; iii) que la ley sea precisa en su lenguaje descriptivo con relación a la construcción de la infracción y precisa en el lenguaje normativo de las consecuencias que resulten de su cometimiento; y, iv) que se evite comprender supuestos que no se enmarquen dentro de su tenor.

II. En el artículo 76 de la LAIP el legislador prevé los tipos de infracciones que podrían ser cometidas por los servidores públicos, al quebrantar las disposiciones relativas al derecho de acceso a la información pública y a la protección de datos personales, en el ejercicio de sus funciones; y, a la vez, califica dichas infracciones en leves, graves y muy graves. Esta calificación ha sido determinada por el legislador atendiendo a la graduación del daño provocado como consecuencia de la comisión de la conducta tipificada en la citada disposición legal.

En consonancia con lo anterior, la LAIP en el artículo 58 letra “e” confiere expresamente, a este Instituto, la potestad de “conocer y resolver del procedimiento administrativo sancionatorio y dictar sanciones administrativas”.

El artículo 76, letra “b” de la LAIP, contempla como infracción muy grave el **“entregar o difundir información reservada o confidencial”**.

En ese sentido, es importante señalar que el acceso y la cesión de la información reservada y confidencial, se encuentra limitada a las personas o autoridades legitimadas para solicitarla y recibirla. Estas son: a) los titulares de los datos personales o sus representantes de acuerdo al artículo 31 de la LAIP; b) el ente obligado o las personas que cuente con el consentimiento expreso y libre, por escrito o por un medio equivalente del titular de los datos para difundir, distribuir o comercializarlos, de conformidad al artículo 33 de la LAIP; c) las autoridades competentes en el marco de sus atribuciones de acuerdo al artículo 26 de la Ley;

d) aquellas situaciones que se encajan en las causales de difusión sin consentimiento del titular de datos, enmarcadas en el artículo 34 de la LAIP; y, e) las personas o instancias del ente obligado autorizadas para acceder a la información reservada, conforme al artículo 21 de la LAIP, en el apartado del contenido de la resolución donde se declara la reserva.

Por tanto, la difusión, distribución o comercialización de los datos personales, fuera de estos parámetros, podría encajar en lo previsto en la infracción antes referida, pues la utilización indebida de los datos personales, puede causar un grave perjuicio a sus titulares, desde el robo de identidad, decisiones automatizadas discriminatorias y la lesión a los derechos de intimidad y privacidad de los mismos.

III. En ese contexto, por dato personal de acuerdo al Instituto Nacional de Transparencia, Acceso a la Información y Protección de los Datos Personales de los Estados Unidos Mexicanos (INAI), en su resolución de fecha 1 de febrero de 2017, de referencia RRA 3995/16, y que ahora hacemos nuestra, se entiende toda aquella información relativa a un individuo identificado o identificable que, entre otras cosas, le dan identidad, lo describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional. Asimismo, señalan aspectos sensibles o delicados sobre tal individuo, como es el caso de su domicilio, teléfono, sus características físicas, ideología o vida sexual, entre otros.

Por otro lado, el artículo 31 de la LAIP establece que: *“Toda persona, directamente o a través de su representante, tendrá derecho a saber si se están procesando sus datos personales; a conseguir una reproducción inteligible de ella sin demora; a obtener las rectificaciones o supresiones que correspondan cuando los registros sean injustificados o inexactos y a conocer los destinatarios cuando la información sea transmitida, permitiéndole conocer las razones que motivaron su petición, en los términos de esta ley. El acceso a los datos personales es **exclusivo de su titular o su representante**”* (la negrita es nuestra).

También el artículo 32 de la referida Ley establece que: *“Los entes obligados serán responsables de proteger los datos personales y en relación con éstos, deberán: [...] e. Adoptar medidas que protejan la seguridad de los datos personales y eviten alteración, pérdida, **transmisión y acceso no autorizado**”* (la negrita es nuestra).



Asimismo, la Sala de lo Constitucional en la Sentencia Definitiva de Amparo del día cuatro de marzo de 2012 de referencia 934-2007, reconoció que la protección de los datos es el medio por el cual se salvaguarda los objetivos de la faceta material del derecho a la autodeterminación informativa, teniendo este su fundamento en la seguridad jurídica artículo 2 inc. 1 de la Constitución de la República; asimismo, estableció que la protección de este derecho, pretende satisfacer la necesidad de las personas de preservar su identidad ante la revelación y el uso de los datos que les conciernen, y que este no puede limitarse a determinado tipo de datos —sensibles o íntimos—; lo decisivo es la utilidad y el tipo de procesamiento que de los mismos se haga, pues se requiere conocer el contexto en que se utiliza o se pretenda utilizar.

Por ello, el grado de sensibilidad o intimidad del dato personal ya no depende si afecta o no la esfera íntima o privada de la persona; hace falta, conocer la relación de utilización de un dato para poder determinar sus implicaciones con el individuo; es decir, determinar la verdadera finalidad, y qué posibilidades de interconexión y de utilización existen, solo así se podrá descifrar la licitud de las restricciones al derecho a la autodeterminación informativa o protección de datos personales.

Este derecho también se encuentra reconocido en los tratados de derechos humanos que forman parte del orden jurídico salvadoreño, como la Declaración Universal de los Derechos Humanos (artículo 12), el Pacto Internacional de Derechos Civiles y Políticos (artículo 17), la Convención Americana sobre Derechos Humanos (artículo 11) y la Convención sobre los Derechos del Niño (artículo 16), al interpretar estas disposiciones, los Organismos Internacionales han destacado la noción de las garantías respecto de los registros personales y corporales, las relacionadas con la recopilación y registro de información personal en bancos de datos y otros dispositivos.

En ese sentido, la LAIP en su artículo 24, ha determinado que es información confidencial: *c. los datos personales que requieran el consentimiento de los individuos para la difusión*; asimismo, que requieren el consentimiento expreso y libre del titular de los mismo, conforme al artículo 25 de la Ley.

Conforme a lo antes mencionado, se establece como una limitante al derecho de acceso a la información aquella documentación que se considere confidencial; sin embargo para que determinada información se clasifique con ese carácter, conforme al artículo 24 letra “c”, a consideración de este Instituto debe cumplirse los siguientes requisitos:

1. Que se trate de datos personales:

- Información concerniente a una persona, y
- Que ésta sea identificada o identificable, se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas<sup>1</sup>.

2. Que para la difusión de los datos se requiera el consentimiento del titular.

Esto último, no se requerirá en los casos que la Ley lo determine, y los supuestos del artículo 34 de la LAIP.

Por ello, previo a determinar conforme a los elementos probatorios incorporados por las partes, si el denunciado ha incurrido en la comisión de la infracción que se le atribuye, debe analizarse la información que a consideración del denunciante titular de información presuntamente difundida, es de naturaleza confidencial en su dimensión datos personales, para determinar si procede dicha clasificación.

Al respecto, la denunciante manifestó que se divulgaron: “*imágenes íntimas de su cuerpo*”; de conformidad a lo establecido en el artículo 6 letra “b” son datos personales sensibles los que corresponden a una persona en lo referente al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física y mental, situación moral familiar, y otras informaciones íntimas de similar naturaleza o que pudieren afectar el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

---

<sup>1</sup>Art. 2 “Definiciones” de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, aprobados el 20 de junio de 2017, en Santiago de Chile.



Al hablar de datos personales sensibles, existen según algunos autores diferentes bloques. En primer lugar, los datos que revelan la ideología, afiliación sindical, religión y creencias. Cuando se proceda a su recogida será necesario que se advierta sobre el derecho que se tiene a no facilitar este tipo de datos y además, solo será posible con el consentimiento expreso del afectado. En un segundo bloque, están los datos que refieren al origen racial, salud y *vida sexual*. En el mismo sentido, estos datos sólo podrán ser recogidos tratados y cedidos cuando exista una finalidad de interés general lo disponga una ley o lo consienta el protagonista de forma expresa. También, existen excepciones por ejemplo cuando exista una razón de prevención, prestación de asistencia sanitaria o tratamiento médico [...]. Por último, se sitúa a los datos relativos a las infracciones penales o administrativas. Aunque estos datos solo pueden ser incluidos en ficheros que poseen las Administraciones Públicas<sup>2</sup>. (Las negritas son nuestras).

Partiendo de la anterior premisa, así como, de la definición de datos personales que contiene la LAIP, es evidente que las imágenes íntimas, tal cual, han sido descritas por las partes en este procedimiento y en el acta de las doce horas del siete de octubre de dos mil veinte, en donde se estableció: “[...], al momento de verificar el equipo informático remotamente desde las oficinas centrales al usuario [REDACTED] del señor [REDACTED] [REDACTED] quien posee asignada computadora de escritorio con código 001.002795.02, se le encontró en la carpeta de descargas materia del contenido pornográfico, el cual se procedió a signarle contraseña [...]”, constituyen datos personales sensibles, siendo la titular de los mismos, la denunciante [REDACTED] [REDACTED]

IV. En su sentido procesal, la prueba es un medio de verificación de las proposiciones otorgadas por las partes, es decir, constituye una actividad a instancia de parte que tiene como finalidad la comprobación de los hechos controvertidos en el litigio; y es contemplada en el derecho común como un derecho y a la vez como una carga.

---

<sup>2</sup> Cristea Nicole, La Protección de Datos de Carácter Sensible en el Ámbito Europeo: Historia Clínica Digital y Big Data en Salud, Universitat Abad Oliba CEU. (2017).

La prueba, se encuentra regida por los principios de pertinencia, idoneidad, o contundencia y utilidad. Estos principios representan una limitación al principio de libertad de la prueba; sin embargo son sumamente necesarios, pues ello significa que no se debe focalizar recursos en la práctica o reproducción de medios que por sí mismos o por su contenido, no sirvan, en absoluto para los fines propuestos y aparezcan claramente impertinentes.

En ese contexto, el Código Procesal Civil y Mercantil (CPCM), de aplicación supletoria en el presente procedimiento conforme a los arts. 106 de la LPA y 102 de la LAIP, contempla dos extremos que deben cumplirse para la admisión de la prueba presentada por las partes: la pertinencia y utilidad. En cuanto a la pertinencia el art. 318 del CPCM, establece que no debe admitirse ninguna prueba que no guarde relación con el objeto del proceso; por otro lado, en lo relativo a la utilidad, el art. 319 del mismo cuerpo normativo, contempla que no deberá admitirse aquella prueba que según las reglas y criterios razonables, no sea idónea o resulte superflua para comprobar los hechos controvertidos.

1. La denunciante ofreció como prueba en su escrito de denuncia: *“Acta emitida a las doce horas del siete de octubre de dos mil veinte, suscrita en la Unidad de Gestión Documental y Archivo del MTPS”*. Respecto de la pertinencia y utilidad de este documento señaló que en el mismo, consta la sustracción y posterior difusión de sus imágenes personales y las de su pareja sentimental.

2. Por su parte, el denunciado en su informe de defensa ofreció como prueba documental: *“a) copia de correo electrónico de fecha 28 de septiembre de dos mil veinte e la licenciada [REDACTED] Jefa de Gestión Documental y Archivo dirigido al licenciado [REDACTED] Jefe de la Unidad de Desarrollo Tecnológico institucional, donde se requiere soporte técnico al equipo de la Unidad de Gestión Documental y Archivo, entre ellas la de [REDACTED] b) Correo electrónico de fecha cinco de octubre de dos mil veinte donde se reitera la solicitud de soporte técnico por la licenciada [REDACTED] c) Correo electrónico de fecha siete de octubre de dos mil veinte, donde se me requiere el soporte técnico solicitado; d) Acta de las doce horas del día siete de octubre de dos mil veinte, debidamente firmada; en la cual se establece el hallazgo de las imágenes con contenido pornográfico, su resguardo y custodia; e) Correo Electrónico*



de fecha siete de octubre de dos mil veinte, de Laura Parada, colaboradora de la Unidad de Gestión Documental y Archivo en el cual se nos remite el acta del párrafo que antecede debidamente firmada; f) Memorando referencia DSG-RRHH-IF-0529-INT-2020, suscrito por la licenciada [REDACTED] Jefa del Departamento de Recursos Humanos, en la cual se solicitó al licenciado [REDACTED], mi persona informe técnico de lo sucedido el siete de octubre en la Unidad de Gestión Documental y Archivo, requiriendo además la remisión en forma documental y electrónica de las imágenes encontradas en el equipo asignado al colaborador [REDACTED]; g) Correo electrónico de fecha veintinueve de octubre en la cual rendí informe técnico de lo encontrado en fecha 7 de octubre en el equipo informático de [REDACTED] el cual dirigí a mi jefe, licenciado [REDACTED]; h) Memorando referencia DE-UDT-WC-139-INT-2020, en la cual se rindió el informe técnico solicitando, pero, en relación a la solicitud de remisión de los archivos encontrados de forma documental y electrónica, no fue remitida, pero se estableció "...El equipo seguirá en resguardo de esta unidad y a disposición de las autoridades y/o comisión pertinente para que verifiquen la información emitida, si así lo desean y no se eliminará ningún archivo, hasta que haya alguna otra indicación [...]; y i) Políticas y Procedimientos de los Controles Generales de los Sistemas de Información emitidas por el Ministerio de Trabajo, para que se verifique el art. 34 que ampara la realización del acta ya mencionada por incumplimiento a dicha disposición normativa".

Los documentos antes descritos con la finalidad de probar los argumentos vertidos en su informe de defensa.

Al respecto, este Instituto considera oportuno admitir los documentos ofrecidos por las partes como prueba debido a que son útiles y pertinentes, constituyen instrumentos públicos y privados, conforme a lo dispuesto en los arts. 331 y 332 del CPCM, y las mismas guardan una relación directa con el objeto de la controversia.

En ese sentido, los insumos probatorios que obran en este procedimiento administrativo sancionador, se constituyen como prueba documental reconocida por el CPCM, que regula lo referido al ámbito probatorio en los procedimientos que tramita la Administración Pública, de acuerdo al artículo 106 de la LPA. Dicho esto, y habiendo enunciado cada uno de los medios probatorios que obran en este procedimiento, este Instituto,

para valorar cada insumo probatorio que consta en el presente, se auxilia de los artículos 341 y 416 del CPCM, que establecen, de forma categórica el valor probatorio que merecen los medios que consten en el procedimiento. Siendo el caso de los documentos públicos y privados que constituyen prueba fehaciente de los hechos, siempre y cuando su contenido no haya sido controvertido.

3. Con base a los elementos de prueba presentados, valorados conjuntamente, y conforme a la sana crítica, se tienen por establecidos los siguientes hechos: (i) que [REDACTED] se desempeñó en el cargo de Técnico Informático- en el momento que ocurrieron los hechos objeto de este procedimiento- en el MTPS; (ii) que el Licenciado Luis Guzmán se desempeña como Técnico de la Unidad de Gestión Documental del MTPS; (iii) que el 28 de septiembre de 2020, la [REDACTED] oficial de gestión documental y archivo requirió a la Unidad de Desarrollo Tecnológico reparación de servicios de internet e intranet para la oficina de archivo, especificando: [REDACTED] (no tiene internet, ni intranet y al enviar correo electrónico a direcciones de Gmail por ejemplo no llegan); [REDACTED] no tiene correo institucional); [REDACTED] (sin servicio de intranet y al enviar correo electrónicos a direcciones de Gmail por ejemplo no llegan); (iv) que dicho requerimiento fue asignado por el Jefe de la Unidad de Desarrollo Tecnológico a los Técnicos [REDACTED] (v) que el 5 de octubre de 2020, la Licenciada [REDACTED] reiteró el requerimiento de revisión de equipo informático; (vi) que el 7 de octubre de 2020, [REDACTED] oficial de gestión documental y archivo, [REDACTED] Jefe de la Unidad de Desarrollo Tecnológico Institucional; [REDACTED] Técnico de la Unidad de Desarrollo Tecnológico Institucional; [REDACTED] Colaborador de la Unidad I y [REDACTED] Colaborador Jurídico de la Unidad de Recursos Humanos-todos empleados del MTPS-, suscribieron, Acta en la cual hicieron constar: “[...] hallazgo de contenido pornográfico en el equipo informático del Colaborador de la Unidad de Gestión Documental y Archivo; [REDACTED] prohibición que regula las Políticas y Procedimientos de Controles Generales de Sistemas de Información en su Capítulo VIII en su art. 34 el cual establece: queda prohibida la utilización de cualquier recurso informático de red para almacenar o portar material ilegal, pornográfico que haga apología del crimen o violencia, ofensivo al buen nombre y honor de otros, propagandas comerciales, cadenas, difusión de actividades lucrativas en general o



utilización en actividades no relacionadas con las funciones de su cargo, una vez explicada la presencia el motivo de la reunión por parte del licenciado [REDACTED] el licenciado [REDACTED] manifiesta: que ese es contenido de su pareja sentimental, que es material personal, que ese material es algo que se envía con su pareja, es algo personal que no lo trae externamente. El hallazgo fue descubierto por el Técnico [REDACTED] quien manifiesta que por un soporte técnico brindado de forma remota con la herramienta "anydesk" y solicitado por la Jefatura de la Unidad de Gestión Documental y Archivo al momento de verificar el equipo informático remotamente desde las oficinas centrales"; (vii) que ante tal situación, el 26 de octubre de 2020, la Jefa del Departamento de Recursos Humanos requirió al Licenciado [REDACTED] informe técnico mediante el cual se determinará el hallazgo y el tipo de material encontrado en la máquina del señor [REDACTED] para ser remitido a la Unidad Jurídica; (viii) que el 29 de octubre de 2020, el Licenciado [REDACTED] emitió informe técnico sobre el hallazgo en equipo informático del señor [REDACTED], (ix) que en el informe suscrito por el Licenciado [REDACTED] se hizo constar entre otras cosas, que en la revisión detallada del contenido del perfil [REDACTED] se encontró en la carpeta descargas un total de 131 elementos, de los cuales 101 eran imágenes en su mayoría de contenido sexual, además de un video de naturaleza similar; asimismo, informó que el equipo sería resguardado por la Unidad a su cargo y estaría a la disposición de las autoridades y/o comisión pertinentes para que verifiquen la información; y (x) que el uso de los recursos informáticos y servicios de red en el MTPS se encuentra regulado en la normativa denominada: Política y Procedimientos de los Controles Generales de los Sistemas de Información, dictada en el mes de abril de 2019.

V. Establecidos los hechos acreditados en este procedimiento y habiéndose determinado que los datos consistentes en las imágenes de la denunciante resguardados dentro del equipo informático confiscado por personal del MTPS constituyen datos personales conforme a lo establecido en el artículo 6 de la LAIP, y solo pueden ser divulgados de forma proporcional con la finalidad que se ha mencionado, corresponde en este apartado examinar si la actuación del denunciado se encontraba amparada en los supuestos establecidos en la LAIP y la normativa aplicable al caso.

En este entendido, la supuesta difusión del dato y la habilitación legal para ello, se analizará con base a lo señalado en la normativa positiva vigente a nivel general y especial.

Al respecto, los artículos 33 y 34 de la LAIP se desprende que todo tratamiento de datos personales que realicen los entes obligados a su cumplimiento debe ser legítimo, en otras palabras, debe mediar el consentimiento de su titular o existir una disposición legal habilite dicho tratamiento. entendiéndose este último como: *“cualquier operación o conjunto de estas efectuadas mediante procedimientos físicos o automatizados, realizadas sobre datos personales relacionados de manera enunciativa más no limitativa, con la obtención, el acceso, registro, organización, estructuración, adaptación, consulta, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales”*<sup>3</sup>.

Para el caso concreto, el tratamiento realizado por parte del denunciado en su calidad de ex técnico de la Unidad de Desarrollo Institucional del MTPS, consistió presuntamente en una difusión de los datos de la denunciante a través de la puesta a disposición de fotografías íntimas a personal del MTPS consignado en el Acta de las doce horas del 7 de octubre de 2020.

Lo antes mencionado, debido a que dentro del equipo informático del compañero de vida de la denunciante –quien ejerce labores dentro del MTPS como colaborador de la Unidad de Gestión Documental y Archivo- se evidenció el hallazgo de contenido pornográfico por parte del ahora denunciado, lo cual fue trasladado al superior jerárquico y se le dio el resguardo debido –según ha sido manifestado durante todo el desarrollo de este procedimiento- y tal cual, consta en el informe emitido por el Licenciado [REDACTED] Jefe de la Unidad de Desarrollo Tecnológico del MTPS.

En ese sentido, es preciso indicar que por regla general la difusión de datos personales se encuentra prohibida, por lo que, las excepciones a la misma deben estar reguladas por la ley. Así, el artículo 34 de la LAIP dispone que los entes obligados deberán proporcionar o divulgar datos personales sin el consentimiento de su titular en los supuestos ahí normados, interesa en este caso hacer referencia a uno de ellos alegados por el denunciado como la

<sup>3</sup> Estándares de Protección de Datos Personales para los Estados Iberoamericanos.



habilitación legal para la suscripción de la nota este es el establecido en la letra “c” de la citada disposición.

Al respecto sobre dicha disposición este Instituto considera que para que una situación encaje en ese supuesto, se requiere de tres condiciones indispensables: 1. Que exista una investigación de delitos o de infracciones administrativas abierta en contra del titular del dato o que esté relacionado directamente; 2. Que la entidad pública esté habilitada por ley para dirigir ese tipo de investigaciones; y, 3. Que exista un procedimiento especial para requerir ese tipo de información al ente obligado que los tenga en su poder. La entidad requirente deberá solicitarlo por resolución u orden fundada.

En ese orden, es evidente que el tratamiento de las imágenes íntimas de la denunciada dió inicio con la verificación de estas por el denunciado en la computadora asignada por el MTPS al señor [REDACTED] hallazgo que fue comunicado a su Jefe inmediato, conforme a lo dispuesto en el artículo 34 de las Políticas y Procedimientos de los Controles Generales de los Sistemas de Información del MTPS. El cual, fue documentado en el Acta de las doce horas del 7 de octubre de 2020, suscrita por la Jefa de la Unidad de Gestión Documental y Archivo, Jefe de la Unidad de Desarrollo Tecnológico Institucional, el denunciado en su calidad de Técnico de la Unidad de Desarrollo Tecnológico Institucional, el señor [REDACTED] un Colaborador Jurídico de la Unidad de Recursos Humanos.

Precisado lo anterior, de los argumentos expuestos dentro de la referida audiencia oral así como de la prueba consistente en: *“Memorando referencia DSG-RRHH-IF-0529-INT-2020, suscrito por la licenciada [REDACTED] Jefa del Departamento de Recursos Humanos, en la cual se solicitó al licenciado [REDACTED] y al denunciado un informe técnico de lo sucedido el siete de octubre en la Unidad de Gestión Documental y Archivo, requiriendo además la remisión en forma documental y electrónica de las imágenes encontradas en el equipo asignado al colaborador [REDACTED]”* ha quedado en evidencia la facultad del MTPS para dar inicio a un procedimiento disciplinario en contra de las actuaciones del señor [REDACTED] Tal facultad se encuentra prevista por el legislador en la Ley del Servicio Civil.

Y es que, de conformidad a lo señalado en el artículo 34 de las Políticas y Procedimientos de los Controles Generales de los Sistemas de Información el cual señala que *“Queda prohibida la utilización de cualquier recurso informático de la Red para almacenar o portar material ilegal, pornográfico, que haga apología del crimen o violencia, ofensivo al buen nombre y honor de otros, propagandas comerciales, cadenas, difusión de actividades lucrativas en general, o su utilización en actividades no relacionadas con las funciones propias del cargo”* existe una prohibición legal respecto de la conducta realizada por el señor [REDACTED] compañero de vida de la denunciante. Acompañado del hecho que de acuerdo al art. 32 literal k), así como del régimen disciplinario consignado en Capítulo VII de la Ley del Servicio Civil (LSC) le corresponde a la Comisión del Servicio Civil o a los Jefes del Servicio la imposición de sanciones conforme a la legislación pertinente.



De ese modo, el aviso realizado por el denunciado a su jefe inmediato se encontraba amparado en las Políticas y Procedimientos de los Controles Generales de los Sistemas de Información del MTPS que a su vez, se encuentran respaldadas en la Ley de Servicio Civil, como un mecanismo que regula la utilización del equipo informático en las instalaciones del MTPS y la conducta de los empleados.

VI. En este orden, conforme a lo dilucidado en el romano que antecede, debe analizarse si, conforme a los argumentos esgrimidos dentro del presente procedimiento se ha evidenciado la comisión de la conducta muy grave señalada en el art. 76 letra “b” de la LAIP por parte del denunciado.

De acuerdo al escrito de denuncia, a los alegatos plasmados dentro de la respectiva audiencia oral y a la documentación aportada como prueba por las partes, no ha quedado comprobada de manera indudable la comisión de tal conducta, en el sentido que, si de la documentación vertida dentro del procedimiento pudiera suponerse una entrega material y verdadera de las fotografías íntimas de la denunciante, se estaría realizando una acusación carente de fundamentos, en el sentido que, si bien se ha comprobado la puesta en resguardo del equipo informático asignado al compañero de vida de la denunciante, no se ha logrado delimitar los sujetos a los cuales fueron entregadas las imágenes, en el sentido que no se comprobó que aquellas personas presentes al momento de levantarse el Acta de las doce horas del 7 de octubre de 2020, tuvieron acceso a las fotografías íntimas de la denunciante.



puesto que su comparecencia resultó únicamente para hacer fe del hallazgo del personal de la Unidad de Desarrollo Tecnológico Institucional del MTPS y no para evidenciar el acceso ilegítimo a dicha información.

Por lo tanto, y acompañado del argumento que la entrega del equipo informático realizada por el denunciado fue realizada como parte del protocolo interno para la posterior investigación de una infracción administrativa cometida por [REDACTED] es que se colige que su actuar se vio revestido por la excepción dispuesta por la LAIP en su art. 34 letra "c", en el sentido que, como parte del aparataje normativo y los procedimientos internos, no existía otra forma de actuar por parte del presunto responsable, concediéndole su actuar como parte de las obligaciones propias del cargo que desempeñó al momento de reportar el hallazgo.

En esa línea, es preciso indicar, que conforme a lo establecido en los artículos 26, 27 y 28 de la LAIP, las autoridades públicas que tengan acceso a información confidencial y reservada en el marco de sus atribuciones legales tienen el deber de custodia y resguardo de esta, de lo contrario incurrirán en responsabilidades previstas en la LAIP. En ese sentido, durante de la tramitación del procedimiento disciplinario al señor [REDACTED] se deberá tener un debido resguardo de estas imágenes y garantizar que solo personas autorizadas tengan acceso a la mismas, en razón del cargo que desempeñan y amparadas en una ley en sentido formal, entiéndase las personas que por ley deben dar trámite al referido procedimiento disciplinario en contra del señor [REDACTED]

Por último, es necesario hacer saber a la denunciante que, una vez finalizado el procedimiento disciplinario en contra de [REDACTED], le queda expedito el derecho de realizar una solicitud de supresión de datos personales a la UAIP del MTPS de conformidad a lo dispuesto en el Art. 36 letra "d" de la LAIP.

### 3. Decisión del caso

Por lo tanto, de conformidad con las razones antes expuestas y disposiciones legales citadas, y con base en los artículos 6 y 18 de la Cn., 52 inciso 3º, 58 letra "e", 76 letra "b" de las infracciones muy graves, 96 y 102 de la LAIP; 78, 79 y 80 del Reglamento de la LAIP;

y, 217 del Código Procesal Civil y Mercantil, a nombre de la República de El Salvador, este Instituto **resuelve:**

a) **Declarar** que [REDACTED], ex Técnico de la Unidad de Desarrollo Tecnológico Institucional del Ministerio de Trabajo y Previsión Social (MTPS) no incurrió en la infracción contenida en el artículo 76 de la Ley de Acceso a la Información Pública "LAIP", consistente en: "entregar o difundir información reservada o confidencial", contenida en la letra "b" de las infracciones muy graves a la LAIP.

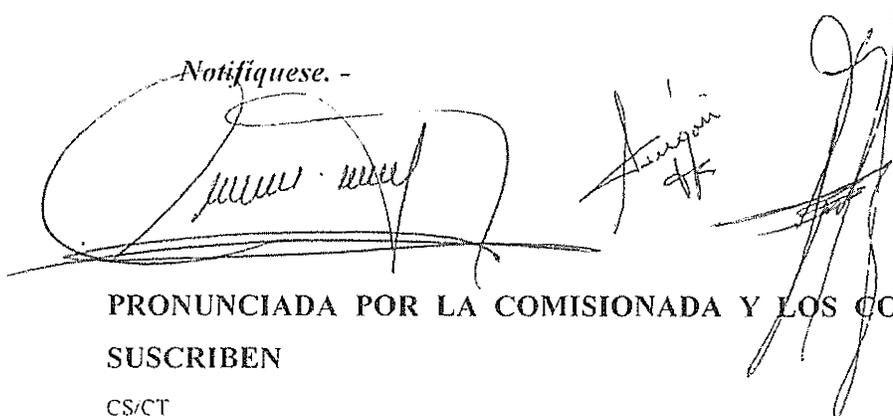
b) **Absolver** a [REDACTED], ex Técnico de la Unidad de Desarrollo Tecnológico Institucional del Ministerio de Trabajo y Previsión Social (MTPS), por las razones señaladas en esta resolución.

c) **Hacer saber** a las partes que en contra de este acto administrativo cabe el recurso de reconsideración; sin embargo, puede directamente acudir a la Jurisdicción Contenciosa Administrativa si así considera necesario. De presentar el recurso de reconsideración este no suspende el plazo establecido en el artículo 25 literal "a" de la Ley de la Jurisdicción Contenciosa Administrativa.

d) **Publíquese** esta resolución, oportunamente.

e) **Archivar** definitivamente este expediente una vez esta resolución adquiriera estado de firmeza.

*Notifíquese. -*



PRONUNCIADA POR LA COMISIONADA Y LOS COMISIONADOS QUE LA SUSCRIBEN

CS/CT

...conforme a su original, con la cual se confrontó y para que lo proveído por este Instituto tenga su debido cumplimiento, se extiende la presente, a los veintisiete días del mes de octubre de dos mil veintiuno.

  
Josselin Elizabeth Callejas Alvarado  
NOTIFICADORA INTERINA  
IAIP

