



República de Colombia  
Corte Suprema de Justicia

Sala de Casación Laboral  
Sala de Descongestión N.º 2

**JORGE PRADA SÁNCHEZ**  
**Magistrado ponente**

**SL3942-2022**  
**Radicación n.º 85283**  
**Acta 42**

Bogotá, D. C., dieciséis (16) de noviembre de dos mil veintidós (2022).

La Sala decide el recurso de casación interpuesto por **RUBÉN DARÍO MORERA** contra la sentencia proferida por la Sala Laboral del Tribunal Superior del Distrito Judicial de Bogotá D. C., el 14 de junio de 2018, en el proceso que, junto con **LUZ STELLA AGUDELO OCAMPO, MARÍA FERNANDA** y **JUAN JOSÉ MORERA AGUDELO**, promovió contra el **BANCO BILBAO VIZCAYA ARGENTARIA COLOMBIA S.A.**

## **I. ANTECEDENTES**

Rubén Darío Morera, Luz Stella Agudelo Ocampo, María Fernanda y Juan José Morera Agudelo llamaron a juicio al Banco Bilbao Vizcaya Argentaria Colombia S.A., con el fin de obtener, a favor del primero, el pago indexado de *«los salarios dejados de percibir, bonificaciones y la indemnización de que trata el art. 64 de la Ley 50 de 1990, en concordancia con el*

*pacto colectivo del cual era miembro*, que tasaron en \$78.792.000 por salarios *«y/o ingresos fijos mensuales dejados de percibir»*; \$28.173.143 por bonificaciones causadas *«y las dejadas de recibir, «en razón a las calificaciones y reconocimiento efectuados a mi poderdante»*; y \$538.680.000 a título de indemnización del *«art. 64 de la Ley 50 de 1990»* en concordancia con lo dispuesto en el *«pacto colectivo del cual era miembro»* (fls. 163 a 177 y 182 a 196).

Solicitaron el pago de los perjuicios morales causados con el despido injusto, *«en un mínimo de (100) CIENTO Salarios Mínimos Legales Mensuales Vigentes»* para cada uno, junto con las costas del proceso.

Manifestaron que desde el 15 de julio de 1982 y en ejecución de un contrato de trabajo a término indefinido, Rubén Darío Morera prestó servicios al Banco demandado, hasta el 24 de noviembre de 2014, cuando lo despidió sin justa causa. Precisaron que para ese momento, aquel desempeñaba el cargo de Gerente de Seguridad de la Información, con una asignación fija mensual de \$10.800.000, más \$1.260.000 por auxilio de vivienda.

Señalaron que el motivo del despido radicó en que en su calidad de gerente y responsable de seguridad informática, el trabajador no verificó *«si la herramienta CHECKER estaba en el modo de operación que es efectivo para que no se infecten con software malicioso los cajeros»*; también, incurrió en *«exceso de confianza en los trabajadores que también tenían relación con la operación de la*

*herramienta*», lo cual facilitó que delincuentes informáticos sustrajeran recursos de la entidad a través de los cajeros electrónicos.

Negaron cualquier acto irregular o negligente del trabajador, menos con el carácter de grave. Explicaron que, por el contrario, aquel desplegó varias acciones para proteger los intereses del Banco ante la vulnerabilidad de sus sistemas, como la organización de reuniones con los trabajadores involucrados, a las que también asistieron el Director del Área de Gestión del Fraude y Seguridad de la Información y los especialistas forenses Gabriel Enrique Lasso Ramírez y Carlos Alberto Trilleras Lasso; igualmente, el diseño y puesta en marcha de un *«plan de choque»* para conjurar la fuga de información de la entidad.

Recalaron que Rubén Darío Morera realizó un constante y riguroso seguimiento a dicho plan y solicitó información a los funcionarios responsables acerca del funcionamiento de los programas de seguridad. Adujeron que aquel nunca fue informado de que el producto *checker* estuviera mal configurado, ni de que la implementación de ese software pusiera en peligro la red de cajeros. Destacaron que el trabajador ni siquiera tenía acceso al servidor, porque su equipo de cómputo no se encontraba conectado, ni contaba con usuario y clave de acceso; menos, al aplicativo *checker*, pues esa posibilidad era exclusiva de los especialistas forenses mencionados, por disposición expresa del manual de funciones.

Agregaron que Rubén Darío Morera «era miembro activo del Pacto Colectivo del Banco» y fue desvinculado después de 32 años de servicio a la entidad, lo que generó dolor, tristeza, congoja, vergüenza y discriminación social, además de una crisis económica para él y su familia, pues «lo dejaron como un copartícipe o autor del desfalco sufrido por el banco».

El ente financiero se opuso a la prosperidad de las pretensiones y propuso las excepciones de prescripción, pago, compensación, inexistencia de la obligación, inexistencia de perjuicios morales, cobro de lo no debido y buena fe (fls. 235 a 295).

Negó ser la causante de cualquier perjuicio al ex trabajador y a su grupo familiar, como quiera que la decisión de terminar el contrato de trabajo fue legítima y se ciñó a la realidad. Explicó que aquel actuó en forma «descuidada y negligente» en el cumplimiento de sus funciones, pues el exceso de confianza lo condujo a no verificar los procesos de seguridad de la información, así como a la omisión de acciones que realmente garantizaran el funcionamiento de las herramientas de protección de los sistemas del Banco. Enfatizó en la falta de supervisión sobre la forma en que estaba operando la aplicación *checker* pues, si bien, otros trabajadores tenían a cargo la administración de la herramienta, el demandante era el responsable del área, por manera que debió verificar las condiciones de instalación y operación, lo que habría podido neutralizar la actividad delincencial.

## II. SENTENCIA DE PRIMERA INSTANCIA

El 28 de septiembre de 2016, el Juzgado Veintinueve Laboral del Circuito de Bogotá D.C. (fl. 2526 Cd), resolvió:

**PRIMERO: DECLARAR** que el demandante RUBÉN DARÍO MORERA PEÑA (sic) (...) estuvo vinculado para el BBVA COLOMBIA desde el 15 de julio de 1982 hasta el 24 de noviembre de 2014, devengando como último salario la suma de \$10.800.000.

**SEGUNDO: CONDENAR** al BBVA COLOMBIA a pagar al demandante señor RUBÉN DARÍO MORERA PEÑA la suma de \$467.640.000 por concepto de indemnización por despido sin justa causa.

**TERCERO: CONDENAR** al BBVA COLOMBIA a indexar la suma anterior de conformidad con el IPC certificado por el DANE al momento de su pago.

**CUARTO: CONDENAR** al BBVA COLOMBIA a pagar a título de perjuicios morales las siguientes sumas de dinero:

- a) A favor de RUBÉN DARÍO MORERA PEÑA (sic): 70 SMLMV
- b) A favor de LUZ STELLA AGUDELO OCAMPO: 50 SMLMV
- c) A favor de MARÍA FERNANDA MORERO AGUDELO: 50 SMLMV
- d) A favor de JUAN JOSÉ MORERA PEÑA(sic): 50 SMLMV

**QUINTO: CONDENAR** en costas a la demandada BBVA COLOMBIA incluyendo como agencias en derecho la suma de \$20.000.000.

**SEXTO: ABSOLVER** a la demandada BBVA Colombia de las demás pretensiones incoadas en su contra.

## III. SENTENCIA DE SEGUNDA INSTANCIA

Al resolver los recursos interpuestos por las partes, el Tribunal revocó la sentencia del *a quo* y, en su lugar, absolvió a la demandada, con costas al demandante.

En lo que interesa al recurso extraordinario, centró su competencia en discernir si Rubén Darío Morera incumplió las obligaciones y/o incurrió en las prohibiciones que le eran propias, con la gravedad requerida para justificar el despido. En caso positivo, si había lugar a liquidar la indemnización por despido con arreglo a lo dispuesto en el pacto colectivo vigente en la empresa.

Para comenzar, indicó que esta Corporación ha entendido *«por grave negligencia la que ponga en peligro la seguridad de las personas o de las cosas, pero cuando uno solo no pone en peligro las cosas, sino que efectivamente se genera un daño, como el que representa la pérdida de unos bienes, a fortiori se configura la justa causa del despido»*. Citó las sentencias con *«radicado 37080 de 2010»*, CSJ SL1226-2018 y, CSJ SL, 31 jul. 2006, rad. 28439.

A continuación, relacionó la carta de terminación del contrato de trabajo (f.º 30-41), el manual de funciones del área de medios tecnológicos para la seguridad (f.º 42-77), los cursos y capacitaciones realizadas por el trabajador (f.º 125-130), el manual de instalación del programa checker (f.º 320-416), el reglamento interno de trabajo (f.º 418-454), el código de conducta del BBVA (f.º 456-482), la diligencia de descargos del actor (f.º 18-29), la declaración del representante legal de la demandada y los testimonios de John Ardila Aponte, Gabriel Lasso Ramírez y Álvaro Niño. Concluyó que:

[...] conforme a toda esta prueba que ha analizado la Sala, queda claro que en efecto la persona directamente encargada de la plataforma checker era el señor Trilleros; sin embargo, cabe

resaltar que el trabajador pertenecía al área de medios, tecnologías para la seguridad, en donde fungía en calidad de gerente, siendo el encargado de direccionar, controlar, gestionar y realizar todas las funciones necesarias para prevenir el riesgo de infiltración ilícita a los cajeros del banco BBVA, lo cual en principio deja ver que el cargo desempeñado por el señor Rubén Darío Morera representaba una gran responsabilidad para la entidad, en ese sentido tenía que estar pendiente de todas las gestiones realizadas por sus subalternos para que el área por él encargada funcionara de la manera esperada, por lo que si bien, dentro de su perfil no se indica de manera específica que tuviera el acceso directo a la plataforma checker, lo cierto es que de manera general sí se encontraba al conocimiento de dicha plataforma como se pudo apreciar en el manual de funciones 4.4 accesos adicionales.

Resaltó que los testigos mencionados fueron claros, en tanto señalaron que, en su calidad de gerente, el accionante podía solicitar ingreso al programa y no lo hizo, a pesar de que el trabajador Igor Alexander Gómez había relatado que los delincuentes tenían acceso al sistema, lo que generó alerta dentro de la entidad financiera. Destacó la *reunión en la cual estuvo presente el actor el día 30 de septiembre de 2014, momento en el cual tal y como indicó en la demanda y en la contestación se le encargó la investigación sobre el caso de mayor implementación de los servicios de seguridad de acuerdo a sus responsabilidades*. A partir de allí, asentó que:

[...] el actor no podía quedarse sólo con los informativos dados por el señor Trilleras sin percatarse de que lo dicho fuera cierto, pues las conductas no se dan solo por la acción sino también por omisión, máxime cuando el aplicativo *checker* era el único que podía dar certeza de las irregularidades en el sistema, según lo manifestaron los testigos, situación que quedó clara que el actor no hizo, pues no basta con señalarse que las personas encargadas de manejar el sistema eran profesionales y especializados por lo que no veía la necesidad de verificar su trabajo, y que tan solo le bastaba con el informe dado por ellos ya que como máximo órgano del área era evidente su

responsabilidad en todo su funcionamiento, sin que fuera necesario que se indicara de manera específica dentro de sus funciones las de la revisión de campo, toda vez que el área se encontraba en ese momento frente a una alarma significativa para el banco, lo que conllevaba que el señor Morera debía estar en un todo pendiente de todos sus subalternos para que no se llevara a cabo el fraude. En razón de ello, esta Sala de Decisión considera que contrario a lo dicho por el *a quo* y alegado por la parte demandante, sí hubo negligencia en el cumplimiento de sus funciones por parte del actor, pues no tuvo la atención necesaria como gerente para evitar el problema.

Consideró que las funciones del demandante no eran solo de orden administrativo, sino que, en su mayoría, implicaban gestionar y garantizar la implementación de mecanismos y procedimientos tecnológicos definidos por el Banco, necesarios para minimizar y reducir el riesgo de fraude por esa vía. Añadió que Rubén Darío Morera, en diligencia de descargos y al absolver interrogatorio de parte, corroboró que el aplicativo *checker* debía estar en modo activo, de suerte que como aquella herramienta estaba configurada en modo aprendizaje, facilitó el ilícito. Preciso que el actor solo se percató de ello 3 días después del hurto, *«es decir, que si pudieron acceder al aplicativo sin problema alguno, por lo que si hubiera actuado diligentemente y oportunamente desde el mismo momento en que fue alertado hubiera podido prevenir el robo»*. Remató:

[...] si bien no quedó demostrado que la conducta del actor se encuentra establecida como grave dentro del reglamento interno de trabajo o convención colectiva, a la luz de las citas jurisprudenciales en los eventos del numeral 6º letra a) del artículo 7º del Decreto 2351 de 1965, le compete al juzgador calificar la gravedad de la conducta, tal cómo se indicó por ejemplo en las sentencias 15822 del 19 de septiembre de 2001, 38855 del 28 de agosto de 2012 y 53901 del 14 de febrero de

2014 proferidas por la Corte Suprema de Justicia, Sala Laboral entre muchas otras.

Conforme a ello para la Sala como se dijo anteriormente existió negligencia en el cumplimiento de las funciones del actor que incurrió en violación de sus obligaciones y funciones que fueron tan significativas patrimonialmente para la entidad demandada que en efecto amerita que se catalogue como grave la conducta y se avale la terminación del contrato por justa causa de la que fue objeto; por lo anterior, se revoca la sentencia apelada y en su lugar se absuelve a la demandada de todas y cada una las pretensiones de la demanda, siendo entonces innecesario por este resultado de estudiar la apelación de la parte demandante.

#### **IV. RECURSO DE CASACIÓN**

Interpuesto por Rubén Darío Morera, fue concedido por el Tribunal y admitido por la Corte. Se procede a resolver.

#### **V. ALCANCE DE LA IMPUGNACIÓN**

Mediante un cargo, replicado en tiempo, pide que la Corte case la sentencia impugnada y, en sede de instancia, confirme la proferida por el *a quo*.

#### **VI. CARGO ÚNICO**

Denuncia violación indirecta, por aplicación indebida del artículo 62, literal a), numerales 4 y 6, del Código Sustantivo del Trabajo, en concordancia con los artículos 58, numerales 1 y 5, 60, 64, 115 y 216 *ibídem*.

A título de errores evidentes de hecho, imputa:

1. Dar por demostrado sin estarlo, que el señor RUBÉN DARÍO MORERA era el encargado de direccionar, controlar,

gestionar y realizar todas las funciones necesarias para prevenir el riesgo de filtración ilícita de los cajeros automáticos del Banco demandado.

2. Dar por demostrado, sin estarlo, que el señor RUBÉN DARÍO MORERA, de manera específica tenía la función de revisar en campo, las actividades desarrolladas por sus subalternos, en especial lo referente al aplicativo Checker.
3. Dar por demostrado, sin estarlo, que el señor RUBÉN DARÍO MORERA actuó con grave negligencia en el cumplimiento de sus funciones, al no haber tenido la atención necesaria como Gerente para evitar el problema de seguridad del Banco demandado.
4. No dar por demostrado, estándolo, que el señor RUBÉN DARÍO MORERA fue diligente y estuvo pendiente y atento de sus subalternos en la implementación de los mecanismos de seguridad dispuestos por el Banco, con el fin de evitar fraudes.
5. Dar por demostrado, sin estarlo, que el señor RUBÉN DARÍO MORERA de acuerdo con el Manual de Funciones, tenía la función básica (objetivo de cargo) de gestionar y garantizar que se implementaran los mecanismos, procedimientos y tecnologías corporativas necesarias definidas por el grupo para minimizar y reducir el fraude tecnológico en el BBVA.
6. Dar por demostrado, sin estarlo, que el señor RUBÉN DARÍO MORERA incurrió en violación de sus obligaciones y funciones contractuales, que fue tan significativa que ameritó ser catalogada como una falta grave.
7. Dar por demostrado, sin estarlo, que en la ceremonia de descargos rendida por el señor RUBÉN DARÍO MORERA, dentro del proceso disciplinario, adelantado por el Banco demandado, se hubiere reconocido o confesado algún incumplimiento a sus obligaciones legales, contractuales y/o reglamentarias.
8. No dar por demostrado, estándolo, que el demandante desarrolló su labor de Gerente de Administración de Seguridad de la Información, conforme a las directrices legales, contractuales y reglamentarias.
9. No dar por demostrado, estándolo, que el señor MORERA PEÑA (sic), en sus más de 30 años de servicio, tuvo un desempeño impecable en sus labores, sin ninguna sanción disciplinaria, tornándose la decisión adoptada por el Banco demandado, de terminar su contrato de trabajo con justa causa, como desproporcionada.
10. Dar por demostrado, sin estarlo, que los hechos relacionados en la carta de terminación del contrato de trabajo fueron efectivamente realizados por el demandante.

11. No dar por demostrado, estándolo, que la sociedad demandada no logró probar la justa causa o motivos que invocó para dar por finalizado el contrato de trabajo del demandante.
12. No dar por demostrado, estándolo, que el despido del demandante fue sin justa causa.
13. No dar por demostrado, estándolo, que el demandante, así como su cónyuge e hijos, sufrieron unos perjuicios morales, como consecuencia de la terminación injusta e intempestiva del contrato de trabajo por parte del Banco demandado.

Asevera que tales yerros fueron el resultado de la apreciación errónea de la carta de terminación del contrato de trabajo (f.º 28-39); el manual de funciones del Gerente de Seguridad de la Información (f.º 70-77); las capacitaciones realizadas por el actor (f.º 125-130); el acta de diligencia de descargos (f.º 18-29); la política de seguridad de los sistemas de la información (f.º 320-416); la declaración del representante legal del Banco demandado (CD 1.ª audiencia); el manual de instalación de la herramienta checker (f.º 132-141); el código de conducta del BBVA (f.º 18-29) y los testimonios de John Ardila Aponte y Gabriel Lasso Ramírez.

Además, la preterición de los manuales de funciones del profesional senior (f.º 42 y ss) y del profesional especializado en tecnologías para la seguridad (f.º 52 y ss); los descargos presentados (f.º 22-26) y los correos electrónicos que envió (f.º 236-241).

Asegura que el BBVA Colombia no acreditó en el proceso los motivos del despido; menos, que constituyeran grave negligencia o incumplimiento de sus obligaciones laborales. Explica que, ni siquiera en forma genérica, el

manual de funciones contempla que en su condición de Gerente de Administración de Seguridad de la Información, debía participar directamente en la implementación del aplicativo *checker* en el sistema operativo de los cajeros electrónicos. Refiere que:

- i) El señor MORERA PEÑA (sic) nunca estuvo a cargo de los Cajeros Electrónicos del Banco, pues esta función era ajena al desempeño gerencial emanado del propio Manual de Funciones,
- ii) la prevención del riesgo del Banco estaba diseñada en todos los cargos y estructuras pertenecientes al área de Gestión del Fraude y Seguridad Informática, la cual era desempeñada por personas capacitadas y especializadas y
- iii) las funciones de gestión, control y riesgo también eran desempeñadas por los profesionales senior y especializados. Lo anterior denota una evidente inconsistencia por parte del Tribunal en el señalamiento de las funciones desarrolladas por el demandante, conforme a las directrices emitidas por el Banco.

Agrega que como lo refirió en sus descargos ante la entidad (fls. 22 a 26) y lo corroboran las funciones previstas en el manual de folios 70 a 77, tampoco le concernía desplegar trabajo de campo en cajeros automáticos, porque solo estaba facultado para gestionar, de manera regular y periódica, el seguimiento, control y validación de los diferentes proyectos y productos de seguridad informática, con el objetivo de blindar y asegurar las plataformas de atención y servicios del banco. Que esa actividad se desarrollaba a través de un grupo de especialistas que integraban el área de tecnología para la seguridad, los cuales tenían directamente a su cargo la operación, implementación y manejo del aplicativo *checker*.

Sostiene que en el caso puntual de la herramienta *checker*, gestionaba y ejecutaba el seguimiento mensual a los especialistas a cargo de su implementación, que es lo que correspondía a su ámbito funcional. Para tal fin, les solicitaba informes sobre el estado del producto y el grado de avance en la actualización a la nueva versión. Explica que no solo lo manifestó en sus descargos y en su declaración, sino que así lo corroboraron el representante legal del Banco al momento de absolver interrogatorio de parte, y el testigo John Ardila, que era su jefe inmediato.

Asevera que el *ad quem* no tuvo en cuenta que de las capacitaciones que recibió, nunca hubo una específica sobre el aplicativo *checker*, lo cual se explica porque sus funciones no requerían conocimientos específicos, experiencia, ni acceso al sistema, como sí ocurría en el caso de los profesionales senior y especializado que interactuaban con el programa, tal cual lo contemplan los manuales de funciones aplicables a esos trabajadores.

Sostiene que los correos electrónicos que obran en el informativo dan cuenta de las acciones que adelantó una vez conoció de la denuncia presentada por el trabajador Igor Alexander Gómez, representadas en el inicio e impulso de una investigación exhaustiva y un plan de contingencia con el fin de evitar el fraude. Fue así que pudo analizar la seguridad de los cajeros a través del aplicativo Netopp, exigió y remitió a las áreas involucradas informes diarios sobre la presencia de archivos sospechosos, recolectó y procesó la información de los accesos remotos de aquel trabajador y de

los cajeros automáticos, y colaboró con las autoridades para adelantar las investigaciones correspondientes; es decir, *«coordinó, apoyó, gestionó, implementó y diseñó todas las medidas (sic) de seguridad con el fin de contrarrestar el ilícito que se estaba cometiendo y así continuar garantizando la integridad informática del Banco demandado»*, conforme su marco funcional.

Precisa que, en ese contexto, no puede endilgársele una negligencia grave pues, por el contrario, su gestión evitó mayores perjuicios a la entidad; *«sencillamente»*, afirma, *«realizó lo que funcional, técnica y operativamente estaba a su alcance»*. Es decir, no se trató de un descuido, falta de atención o desinterés en la ejecución de las labores a cargo, pues hizo el seguimiento que correspondía sobre la actividad de los trabajadores encargados de la instalación del producto *checker*, quienes nunca informaron acerca de alguna deficiencia en la implementación del producto.

Cuestiona que el juez colegiado de instancia coligiera que el trabajador incumplió el deber de *«gestionar y garantizar que se implementen los mecanismos, procedimientos y tecnologías corporativas necesarias definidas por el grupo para minimizar y reducir el fraude tecnológico en el BBVA»*, siendo que, según los manuales de funciones incorporados al proceso, *«dicha función corresponde única y exclusivamente para los cargos de profesional especializado y profesional senior»*.

Reprocha que el Tribunal avalara la consideración del empleador sobre la gravedad de la conducta, *«desconociendo que ninguno de los documentos allegados al expediente, en especial los relacionados como erróneamente apreciados (políticas de seguridad, código de conducta de funciones (sic), diligencia de descargos, manual de funciones), endilgaran dicha gravedad»*. Añade que era necesario *«acreditar la gravedad de la falta en algún pacto, convención colectiva de trabajo, fallos arbitrales, contrato individual o reglamento»*, de suerte que al no aparecer acreditado ese supuesto, *«el empleador es el que califica la gravedad de la conducta atendiendo a la naturaleza y circunstancias de la empresa, pero dicha conducta debe estar consagrada de manera clara, expresa y pública en un documento conocido previa y ampliamente por el trabajador»*.

Insiste en que en la diligencia de descargos, jamás aceptó ser el responsable de la implementación y manejo del aplicativo *checker*, pues siempre sostuvo que esas actividades se hallaban a cargo y bajo el conocimiento de los especialistas capacitados en la herramienta, quienes suministraban reportes periódicos en ese sentido.

Para finalizar, resalta que prestó servicios a la empresa por más de 30 años, sin antecedentes disciplinarios, ni objeciones de fondo a su desempeño; enfatiza que, por el contrario, su hoja de vida acredita una *«larga trayectoria marcada por su óptimo rendimiento que lo llevó a trascender al punto de ocupar un cargo gerencial»*.

## VII. RÉPLICA

La entidad demandada glosa la técnica del recurso. Destaca la introducción de planteamientos jurídicos en un cargo orientado por la senda de los hechos, en tanto cuestiona la falta de calificación de la conducta reprochada al trabajador; además, la ausencia de una verdadera demostración de los «supuestos desatinos» endilgados al juez de segunda instancia. Afirma que la censura propone un ataque a la facultad de apreciar libremente la prueba e intenta trasladar a terceros la responsabilidad de lo ocurrido, lo que «no borra la obligación de diligencia y cuidado que le competía al demandante en su función como gerente de seguridad de la información».

Refiere que la ausencia de faltas en 30 años de trabajo «es un argumento pueril», toda vez que no se le despidió por lo que hubiera pasado en ese lapso, sino por lo que aconteció en esa última oportunidad, de suerte que «aceptar el argumento del cargo supondría que hay que esperar que el hurto se repita para que se pueda responsabilizar al demandante, lo cual involucra un claro absurdo».

## VIII. CONSIDERACIONES

Previo a abordar el estudio de la acusación, es necesario precisar que si bien, el recurrente solicita casar la sentencia de segundo grado y confirmar la de primer nivel, esta última impuso condenas a favor de Luz Stella Agudelo Ocampo, María Fernanda y Juan José Morera Agudelo, quienes no

acudieron a sede extraordinaria. Por ende, la Sala entenderá que el alcance de la impugnación está circunscrito al quiebre de la decisión del Tribunal, en cuanto fuera desfavorable al demandante y recurrente en casación.

De otro lado, la Sala no coincide con la réplica en que el cargo incursione en cuestionamientos de orden jurídico, dentro de una discusión eminentemente fáctica. Distinto es que para explicar que el Tribunal se equivocó al hallar demostrada la gravedad de la conducta del trabajador, en los términos del artículo 62, literal a, numeral 6, 1.ª parte, del estatuto laboral, la censura diferenciara que, cuando ha de aplicarse la segunda parte de esa disposición, es imprescindible la consagración del carácter grave de la falta, en pactos o convenciones colectivas, fallos arbitrales, contratos individuales o reglamentos.

Tras aludir a ese supuesto, en que solo es procedente verificar la consagración normativa de la falta grave, el propio recurrente admite que en este caso había lugar a ponderar *«la gravedad de la conducta atendiendo a la naturaleza y circunstancias de la empresa»*, es decir, finalmente coincide con el Tribunal en la regla jurídica de que este se sirvió, consistente en que correspondía al juzgador evaluar la conducta del trabajador y calificar su gravedad.

De ahí que esas anotaciones y comentarios no descalifican, ni desarticulan, el sentido general de los cuestionamientos, que lucen adecuadamente encaminados a demostrar que el juez colegiado de instancia se equivocó en

la valoración de los medios de convicción adosados al expediente.

Dicho lo anterior, la Sala entiende que sin cuestionar la relación laboral entre Rubén Darío Morera y el Banco Bilbao Vizcaya Argentaria Colombia, entre el 15 de julio de 1982 y el 24 de noviembre de 2014, cuando aquel se desempeñaba como Gerente de Seguridad de la Información en la dependencia de Gestión de Fraude y Seguridad de la Información, la censura arremete contra la conclusión central de la decisión absolutoria de segundo grado, consistente en que el empleador acreditó que el despido del trabajador se fundó en una justa causa, representada en un actuar negligente y en una grave *«violación de sus obligaciones y funciones»*.

Importa recordar que para arribar a esa conclusión, el fallador de la alzada dijo apoyarse en el marco funcional establecido por la entidad, de donde dedujo que el actor i) era *«el encargado de direccionar, controlar, gestionar y realizar todas las funciones necesarias para prevenir el riesgo de infiltración ilícita a los cajeros del banco BBVA»*; ii) si bien, dentro de su perfil no se precisó de manera específica que tuviera acceso directo a la plataforma checker, *«lo cierto es que de manera general si se encontraba al conocimiento de dicha plataforma como se pudo apreciar en el manual de funciones 4.4 accesos adicionales»*; y que iii) desarrollaba funciones que no eran solo de orden administrativo, sino que en su mayoría, conllevaban gestionar y garantizar la implementación de mecanismos y procedimientos

tecnológicos definidos por el Banco, necesarios para minimizar y reducir el riesgo de fraude por esa vía.

Así mismo, coligió que en diligencia de descargos, el actor sostuvo que el aplicativo *checker* debía estar configurado en modo activo y no en modo aprendizaje, como en realidad lo estuvo durante los días en que ocurrió el ilícito. Dedujo patente la falta de diligencia y oportunidad del demandante para «prevenir el robo».

Sin más preámbulos, la Sala concentrará su estudio en los medios de convicción denunciados y que, en criterio del recurrente, descartan toda negligencia o incumplimiento grave de sus obligaciones y, por ende, dejan sin piso la decisión censurada.

De entrada, la Sala descarta que la política de seguridad de los sistemas de la información (fls. 320-416 cuaderno anexo), el Código de conducta del Banco (fls. 456-482 cuaderno anexo), y el Manual de instalación de la herramienta *checker* (fls. 132-141 cuaderno anexo), presten utilidad a los propósitos de la acusación. Los dos primeros son documentos que consagran deberes y reglas de conducta del común de los trabajadores de la entidad financiera, mientras que el tercero es una guía del paso a paso para la instalación del programa mencionado; ninguno refiere detalles sobre las funciones específicas del trabajador, que es lo que aquí interesa.

La carta de terminación del contrato de trabajo (fls. 28 a 39), empieza con una alusión a aspectos generales de la vinculación del trabajador y sigue con un compendio de las funciones básicas y específicas de dirección, gestión, control y riesgo propias de su rol gerencial. En cuanto al motivo concreto del despido, se infiere que el empleador reprochó al actor que pese a los riesgos a los que se hallaba expuesta la entidad por la infiltración de software malicioso en sus sistemas operativos, no tomó medidas inmediatas y urgentes para evitar el fraude; en particular, cuestionó que a sabiendas de que el Banco había adquirido la herramienta de seguridad *checker*, no verificó que se mantuviera en modo activo, lo que a la postre facilitó el accionar de los delincuentes informáticos.

Así mismo, le enrostró que sus funciones no eran solo de tipo administrativo, sino de *«dirección, gestión, control y riesgo»* y, pese a ello, *«no hizo ni venía haciendo lo mínimo, que, para este caso, era el control frente al adecuado uso de la herramienta checker»*. En el mismo sentido, le criticó la falta de control sobre la actividad de los profesionales subalternos y que no hubiera hecho *«labor de campo de verificación de la forma de operación de la herramienta»*.

Visto el contenido de dicho documento, en estricto sentido, el Tribunal no desacertó en su valoración; solo que hizo eco de las afirmaciones del empleador acerca del espectro funcional del trabajador, así como de lo que el empresario consideró como un actuar negligente y omisivo, hasta llegar al mismo punto, esto es, la configuración de los

supuestos del artículo 62, literal a), numerales 4 y 6 del Código Sustantivo del Trabajo, para proceder al despido con justa causa.

De cara a la valoración del marco funcional del trabajador, conviene acotar que el Tribunal se refirió al compendio de folios 42 a 77, que contiene no solo el catálogo de actividades y roles asignados al actor en condición de Gerente de Seguridad de la Información, sino el de los profesionales senior y especializado de la misma dependencia.

De ahí, coligió que dentro de sus funciones básicas, el demandante debía *gestionar y garantizar que se implementen los mecanismos, procedimientos y tecnologías corporativas necesarias definidas por el grupo para minimizar y reducir el fraude tecnológico en el BBVA Colombia*; y, dentro de las específicas:

[...] las de gestionar que se cumpla la integridad, confidencialidad, disponibilidad de la información procesada y almacenada en los sistemas de información del Banco, gestionar e implementar los procedimientos concernientes al control de incidentes de seguridad informática, garantizar que se instauren los procedimientos de monitorización en la modalidad 7x24x365 para eventos de seguridad del grupo, investigando posibles intentos de fraude, gestionar y propender por la implementación de las directrices corporativas o en los componentes online y procesos bath, gestionar el cumplimiento de la metodología establecida para el ciclo de vida de aplicativos del capítulo de seguridad informática, entre otras, también apoyar el desarrollo de estudios periódicos de análisis de riesgo de la plataforma tecnológica de internet, red ATMS y servidores que almacenan y procesan información clasificada como confidencial del banco, gestionar y propender por la normal operación y disponibilidad

de las diferentes plataformas de seguridad, información e internet. Igualmente se puede, entre varias, otras, igualmente se puede apreciar de dicho manual de funciones en su numeral 4º información complementaria 4.4 accesos adicionales encontrándose allí servidor checker, en el numeral 5.2 refiere a conocimientos específicos el cual indica el conocimiento está catalogado como experto dada la involucración en el diseño, análisis, instalación, administración, gestión e implementación de estrategias tecnológicas de prevención de fraude, dentro del numeral 5.4 se habla de la experiencia y se encuentra plataforma corporativa checker.

Esta acotación es relevante, como quiera que al revisar la documental acusada, la Sala observa con facilidad que el juez de segunda instancia se remitió a las funciones asignadas al Profesional Especializado (fls. 42 a 55), que claramente no corresponde al cargo desempeñado por el promotor del juicio.

Semejante ligereza o dislate no es de poca monta pues, evidentemente, condujo a extraviar la perspectiva desde la cual debía sopesarse el ámbito de acción del demandante. Es decir, el Tribunal apuntaló sus premisas sobre supuestos equivocados; en particular, la asignación al actor de funciones básicas y específicas propias de un rol operativo, dedicado a la implementación e interacción con las herramientas tecnológicas del Banco, y la posibilidad de acceso a la plataforma *checker*, prevista concretamente para el citado profesional, pero no para el gerente, quien solo registraba acceso a «TSO Producción y Desarrollo, Beta88» y a «office» (fl. 76).

En contraste con lo anterior, los folios 70 a 77 dan cuenta de que el verdadero marco funcional del actor seguía este norte básico:

Garantizar la integridad, confidencialidad y disponibilidad de la información procesada y almacenada en los sistemas de información del Banco, dada por directrices institucionales de México y España, apoyando la implementación y mantenimiento de políticas, estándares y procedimientos de seguridad informática, en la infraestructura de Hardware y Software especializado de seguridad, por la administración y control de incidentes de seguridad informática. Así como el seguimiento y control de la solución de los casos de fraude tecnológico -Call Center e Internet.

Y dentro de las funciones específicas, vale la pena resaltar:

#### **Funciones de Dirección:**

- Apoyar y gestionar la normal operación y disponibilidad (7x24x365) de las diferentes plataformas de seguridad informática en el ambiente de Producción, propendiendo siempre por obtener la mayor eficiencia y rendimiento de ellas.
- Coordinar la ejecución en la definición y mantenimiento de parámetros del ambiente de equipos de seguridad informática.
- Diseñar e implantar controles necesarios para asegurar y proteger la información del BBVA Colombia.
- Definir las estrategias para el cumplimiento de la disponibilidad de los equipos de seguridad del Banco (7x24x365) de las diferentes plataformas de Hardware del Banco.
- Definir las estrategias para la personalización y administración de las herramientas de seguridad de la información.
- Solicitar y controlar los accesos adicionales y/o aplicativos utilizados por los funcionarios de la dependencia y/o grupo a su cargo, corroborando que sean necesarios para ejecución de sus funciones.

### **Funciones de Gestión:**

- Gestionar la garantía de la disponibilidad de los equipos de seguridad del Banco (7x24x365) de las diferentes plataformas de Hardware.
- Implantar controles derivados de las Directrices Corporativas de Seguridad lógica.

### **Funciones de Control:**

- Gestionar y velar por la mejora de los procedimientos operativos y administrativos de la seguridad informática en las plataformas y productos instalados en el BBVA Colombia.
- Coordinar y controlar el mantenimiento preventivo y correctivo de la infraestructura de Hardware y Software de seguridad informática del Banco.
- Definir las estrategias para el monitoreo y funcionamiento de los productos de seguridad, para identificar y tomar acciones correctivas sobre las anomalías que se detecten.

### **Funciones de Riesgo:**

- Definir las estrategias que apoyen la administración y monitoreo de usuarios y perfiles de los diferentes sistemas de información para el cumplimiento de las políticas y estándares de seguridad establecidos.
- Definir las estrategias que apoyen la administración, control y monitoreo a acceso lógico a las plataformas tecnológicas del Banco BBVA Colombia.
- Definir las estrategias para atender las situaciones irregulares detectadas en la red perimetral de seguridad del BBVA Colombia, desarrollando objetivamente los procesos de investigación apoyados con tecnología de punta con el fin de determinar las posibles causas, responsables y proponer soluciones lógicas que minimicen los niveles de riesgo (subraya la Sala).

De las funciones mencionadas, no cabe duda que la administración, manejo, actualización y operatividad del

sistema *checker* no estaba asignada a Rubén Darío Morera, sino al Profesional Especializado del área. Tampoco, le era exigible el desarrollo de «*labores de campo*», propias de trabajadores de nivel profesional de la entidad.

En ese orden, el juez colegiado de instancia desapercibió que desde la perspectiva funcional básica y aún en los ámbitos específicos de dirección, gestión, control y riesgos, el demandante no se desenvolvía dentro de la implementación, interacción y ejecución directa de programas de seguridad como el denominado *checker*. De acuerdo con su nivel de responsabilidad dentro de la organización, su función estaba encaminada a ser garante de procesos, formular políticas y diseñar estrategias, así como a brindar apoyo para su implementación, mantenimiento y mejora.

Es a partir de ese rasero que debió validarse la diligencia y nivel de cumplimiento del actor; de ahí, provino el desacierto evidente del Tribunal, al ubicar al trabajador en un contexto funcional diferente, ajeno al que en realidad le era oponible. Nada más se infiere de que, sin el menor asomo de objetividad, considerara que la conducta de aquel debía ser ponderada a partir de lo que en su criterio *pudo haber hecho*, de espaldas al verdadero alcance de las funciones asignadas y de las que tenían a cargo otros trabajadores de la dependencia.

Ahora bien, la Sala no ignora que el Tribunal también insistió en el actuar negligente u omisivo del trabajador, pese a la inminencia de los riesgos que se cernían sobre la entidad.

No obstante, el cruce de correos electrónicos entre el actor y diferentes áreas del Banco, contradice esa deducción. De folios 236 a 241 del cuaderno anexo, obra registro de las acciones emprendidas por el área de Seguridad de la Información una vez se tuvo conocimiento de la situación que había dado lugar a la exposición de los sistemas del Banco. De esto último, se destaca el análisis a través del aplicativo *Netopp*, que llevó a detectar «en el cajero nro 0011 de la Avda. Chile la presencia de archivos sospechosos», lo que obligó al cambio de su disco duro; así mismo, se llevó a cabo el procesamiento de la información sobre los accesos remotos efectuados por el trabajador que dio pie a la infiltración de software malicioso, así como de los «*Logs de los cajeros mencionados*».

Por ello, también desacertó el Tribunal al colegir que los medios de convicción incorporados al expediente, hicieron evidente un actuar negligente o descuidado del trabajador. Menos aún, que den cuenta de la falta de seguimiento a un evento extraño que, finalmente, se concretó gracias a acciones particulares o individuales que no podían estar bajo su control las 24 horas del día. Por ejemplo, que fueran otros funcionarios de la entidad quienes pudieran acceder, cualquier día y a cualquier hora, al aplicativo *checker* y resolver, en últimas, si este quedaba en modo activo o de aprendizaje.

En consecuencia, según el análisis objetivo de los medios probatorios estudiados, el Tribunal se equivocó en forma manifiesta al concluir que el empleador acreditó que el despido del trabajador se fundó en una justa causa, representada en un actuar negligente y en una grave *«violación de sus obligaciones y funciones»*.

Por lo demás, vale acotar que los descargos presentados por el trabajador y las versiones del representante legal de la demandada y de los testigos citados al proceso, tan solo representan la percepción individual y subjetiva sobre las circunstancias objeto de debate. De esta suerte, en nada influyen sobre el escenario elaborado con base en los medios documentales analizados, que fue ignorado o desapercibido por el fallador de segundo grado.

Sin perder de vista la naturaleza fáctica de la acusación, conviene no olvidar que si bien, en estos casos corresponde al juez laboral calificar con un amplio margen la gravedad de la negligencia o de las conductas endilgadas al trabajador (CSJ SL 10 mar. 2012, rad. 35105, reiterada en la CSJ SL1920-2018), no es menos cierto que ese ejercicio debe fundarse, naturalmente, en la apreciación objetiva y correcta de las pruebas; también, en lo que la jurisprudencia ha acuñado como *«el justiprecio de las circunstancias concurrentes»* (Sentencia del 7 de julio de 1958 del extinto Tribunal Supremo del Trabajo, reiterada en las providencias CSJ SL 14 ago. 2012, rad. 39518 y CSJ SL19449-2017), que no es algo distinto a la búsqueda de un parámetro de ponderación objetivo acerca de los hechos a los que se vio

enfrentado el trabajador y la razonabilidad de su comportamiento.

Desde luego, dichos parámetros jurisprudenciales rifien con lo plasmado en la sentencia de segundo grado, en la que el juez de la alzada pretendió imponer su criterio a partir de lo que, sin prueba ni soporte, estimó que pudo haber hecho el trabajador en un momento dado.

Por tanto, de conformidad con lo discurrido y al haberse acreditado los errores manifiestos de hecho endilgados al Tribunal, el cargo prospera y se casará la sentencia de segundo grado, en cuanto revocó las condenas proferidas por el *a quo* a favor del demandante Rubén Darío Morera.

Sin costas en sede extraordinaria.

#### **IX. SENTENCIA DE INSTANCIA**

Basta lo expuesto en sede extraordinaria para desestimar la impugnación del demandado, en cuanto se centró en la suficiente demostración de los motivos de despido.

La convocada a juicio también cuestiona la condena por los perjuicios morales ocasionados al trabajador por razón del despido; niega que, al motivar el desahucio, le hubiera reprochado comportamientos contrarios a la ética, como para considerar que afectó su dignidad y honor y, con ello, le generó una afectación que deba ser objeto de reparación.

Agrega que la extensión de la relación laboral por varios lustros, tampoco puede ser un factor relevante para conceder dicha indemnización.

Para resolver, cumple recordar que el artículo 64 del Código Sustantivo del Trabajo prevé una indemnización por la terminación unilateral del contrato sin justa causa, que comprende el lucro cesante y el daño emergente. De ahí que, en criterio de esta Sala, *«es posible que se resarza el daño moral cuando quiera que se pruebe que este se configuró ante una actuación reprochable del empleador, que tenía por objeto lesionarlo, o que le originó un grave detrimento no patrimonial»* (CSJ SL14618-2014).

Pues bien, la demandada acierta al advertir que la carta de terminación del contrato de trabajo no contiene señalamientos que afecten la dignidad y el buen nombre del trabajador. Sin perjuicio de que las razones invocadas para el despido quedaran desvirtuadas en el proceso, lo cierto es que se enfocaron en asuntos de orden técnico que, bajo la percepción del empleador, conllevaron incumplimiento de las obligaciones del trabajador, pero nada más.

Así mismo, más allá de la frustración natural por la terminación del vínculo, el demandante no trajo al proceso elementos que ofrezcan certeza del menoscabo de aspectos emocionales de su vida íntima, familiar o social. Por tanto, se revocará la condena por este rubro.

Por lo demás, no hay lugar a revisar el monto de la indemnización por despido sin justa causa a la luz del pacto colectivo vigente en la entidad, como lo pidió el demandante en su apelación, como quiera que en el alcance del recurso extraordinario solicitó la confirmación de la sentencia de primer grado *«en todas y cada una de sus partes»*.

Consecuencia de lo expuesto, se confirmará la decisión del *a quo*, salvo el numeral cuarto, que se revocará.

Sin costas en segunda instancia.

## X. DECISIÓN

En mérito de lo expuesto, la Corte Suprema de Justicia, Sala de Casación Laboral, administrando justicia en nombre de la República y por autoridad de la ley, **CASA** la sentencia proferida el 14 de junio de 2018, por la Sala Laboral del Tribunal Superior del Distrito Judicial de Bogotá DC, dentro del proceso ordinario laboral seguido por **RUBÉN DARÍO MORERA** contra **BANCO BILBAO VIZCAYA ARGENTARIA COLOMBIA**, en cuanto revocó las condenas proferidas por el *a quo* a favor del demandante Rubén Darío Morera.

En sede de instancia, confirma la sentencia proferida el 28 de septiembre de 2016 por el Juzgado Veintinueve Laboral del Circuito de Bogotá D.C., salvo el numeral 4, que se entiende revocado en su integridad.

Sin costas.

Notifíquese, publíquese, cúmplase y devuélvase el expediente al tribunal de origen.

**DONALD JOSÉ DIX PONNEZ**

**JIMENA ISABEL GODOY FAJARDO  
SALVO EL VOTO**

**JORGE PRADA SÁNCHEZ**



República de Colombia  
**Corte Suprema de Justicia**

Sala de Casación Laboral  
Sala de Descongestión N.º 3

**Radicación No. 85283**

**Magistrado Ponente: JORGE PRADA SÁNCHEZ**

**PROCESO DE: RUBÉN DARÍO MORERA, LUZ STELLA AGUDELO OCAMPO, MARÍA FERNANDA y JUAN JOSÉ MORERA AGUDELO** contra el **BANCO BILBAO VIZCAYA ARGENTARIA COLOMBIA SA.**

### **SALVAMENTO DE VOTO**

Con el acostumbrado respeto por las decisiones que toma esta Corporación, a continuación, presento los argumentos que me llevan a disentir de la decisión adoptada en el asunto de la referencia.

Contrario a lo considerado por la mayoría de los integrantes de la Sala, estimo que, no debió prosperar el recurso extraordinario de casación, por las siguientes razones:

Para el Tribunal en las condiciones del *sub lite* no existió duda en cuanto a que Rubén Darío Morera actuó en forma negligente en el cumplimiento de sus funciones, lo que le llevó a incurrir en violación de sus obligaciones y funciones *«que fueron tan significativas patrimonialmente para la entidad demandada que en efecto amerita que se catalogue como grave la conducta y se avale la terminación del contrato por justa causa de la que fue objeto»*.

De las probanzas arrimadas al proceso, coligió:

[...] queda claro que en efecto la persona directamente encargada de la plataforma checker era el señor Trilleros; sin embargo, cabe resaltar que el trabajador pertenecía al área de medios, tecnologías para la seguridad, en dónde fungía en calidad de gerente, siendo el encargado de direccionar, controlar, gestionar y realizar todas las funciones necesarias para prevenir el riesgo de infiltración ilícita a los cajeros del banco BBVA, lo cual en principio deja ver que el cargo desempeñado por el señor Rubén Darío Morera representaba una gran responsabilidad para la entidad, en ese sentido tenía que estar pendiente de todas las gestiones realizadas por sus subalternos para que el área por él encargada funcionara de la manera esperada, por lo que si bien, dentro de su perfil no se indica de manera específica que tuviera el acceso directo a la plataforma checker, lo cierto es que de manera general si se encontraba al conocimiento de dicha plataforma como se pudo apreciar en el manual de funciones 4.4 accesos adicionales.

Aunque el cargo se orientó por la senda indirecta, no se discutió que: Rubén Darío Morera y el Banco Bilbao Vizcaya Argentaria Colombia suscribieron contrato de trabajo a término indefinido que se mantuvo vigente del 15 de julio de 1982 al 24 de noviembre de 2014 y, que para el momento del despido se desempeñaba como Gerente de Seguridad de la Información en la dependencia de Gestión de Fraude y

## Seguridad de la Información.

El asunto que sometió la censura a escrutinio de la Sala se centraba en verificar, si el Tribunal se equivocó, de manera evidente, protuberante ostensible, al considerar que el despido de que fue objeto obedeció a una justa causa.

Del sustento del cargo se extrajo, que no alcanzaba la fuerza suficiente para derruir las conclusiones fácticas a las que llegó el Tribunal, sobre la existencia de los hechos que constituyeron el incumplimiento de las funciones a cargo de Morera, que condujeron a su despido, justificado, como se analizará a continuación.

Contario a lo sostenido por el recurrente, el Tribunal no desconoció que el manejo, actualización, funcionamiento y operatividad del sistema de seguridad informática checker implementado en el banco para repeler fraudes informáticos y hurto de dinero, estaba atribuido al «señor Trilleros»; no obstante, del acervo probatorio endilgó a Rubén Darío Morera, un actuar negligente y omisivo en el desarrollo de sus actividades, pues una vez fue noticiado de las amenazas y acciones de que fue objeto el trabajador Igor Alexander Gómez, el 30 de septiembre de 2014, no desplegó todas las gestiones necesarias para prevenir el riesgo de infiltración ilícita a los cajeros del banco BBVA, que ocurrió días después y que acarreó para la entidad bancaria una pérdida económica superior a los mil millones de pesos.

Tal conclusión encuentra respaldo del análisis objetivo de las pruebas que la censura acusó de indebidamente valoradas, como pasa a analizarse:

- Carta de terminación del contrato de trabajo (f.º 28-39 cuaderno principal):

En este documento, el banco demandado luego de hacer alusión a aspectos generales de la vinculación del trabajador y de rememorar las funciones básicas y específicas de dirección, gestión, control y riesgo propias de su cargo, da a conocer a Rubén Darío Morera las omisiones en las que incurrió en su calidad de Gerente de Seguridad en la Información, una vez fue informado, el 30 de septiembre de 2014, en reunión sostenida con el mismo Igor Alexander Gómez, que este fue coaccionado en tres oportunidades por personas desconocidas para que les permitiera el acceso remoto a la plataforma del banco, con el código de usuario y claves electrónicas, a lo que el accedió en razón a las amenazas de que fue objeto junto con su familia, luego de lo cual, el 1 de octubre de esa anualidad, al revisar en forma aleatoria por parte del área de Gestión de Fraude y Seguridad de la Información, 491 cajeros electrónicos marca Diebold - Atm's, se encontró que 14 de ellos fueron accedidos remotamente a través de la herramienta Netopp, con la información suministrada por Gómez, lo que permitió a los delincuentes instalar un software malicioso -malware- *«para que ejecutara modificaciones lógicas al proceso de dispensación de dinero, alterando así el sistema operativo»*.

No obstante el conocimiento que tuvo el demandante de aquellos hechos en las fechas antes referenciadas, consideró el banco que resultaban evidentes las graves y negligentes conductas en las que incurrió, al no haber tomado medidas inmediatas y urgentes para evitar el fraude, pues a sabiendas de que el trabajador Igor Alexander Gómez había suministrado las claves de acceso a la plataforma Netopp y que el banco había adquirido la herramienta de seguridad checker diseñada específicamente para cajeros ATM's dentro de los que se encuentran los de la marca Diebold, no verificó que esta se mantuviera en modo activo, por lo que, al haberse configurado en modo aprendizaje no se pudo realizar el monitoreo en tiempo real de los cajeros electrónicos lo que conllevó a que no se detectaran las acciones realizadas por los delincuentes para, oportunamente, haberlas repelido.

En aquella misiva recabó la entidad bancaria en la responsabilidad que recaía en el demandante, dado el cargo que desempeñaba y la capacitación recibida, de garantizar la seguridad de todas las plataformas que aquella utiliza y las funciones de dirección, gestión, control y riesgo a su cargo, *«a pesar de lo cual no hizo ni venía haciendo lo mínimo que, para este caso, era el control frente al adecuado uso de la herramienta Checker, esto es que se estuviera operando en debida forma y que se mantuviera en estado ACTIVO».*

Conforme al contenido de dicho documento, no se observa error alguno en la valoración que hiciera el Tribunal, pues de aquel coligió que *«los hechos se enmarcan dentro de las previsiones contempladas en los literales a) numeral 4º*

*segunda parte y sexta primera parte del Decreto 2351 de 1965, numeral 1 y 5 del artículo 58 del CST y la seguridad social, en concordancia con el reglamento interno de trabajo y el código de la conducta del BBVA», tal como lo sostuvo el banco, lo que evidencia que nada distinto a lo que allí se consigna concluyó el juzgador.*

- Manual de funciones del cargo de Gerente de Seguridad de la Información (f.º 70-77 cuaderno principal):

Del contenido de dicha probanza, el Tribunal refiere, luego de analizar el manual de funciones de folios 42-77 que allí se le asignaron al demandante funciones básicas y específicas como Gerente. Dentro de las básicas indicó la de: *"gestionar y garantizar que se implementen los mecanismos, procedimientos y tecnologías corporativas necesarias definidas por el grupo para minimizar y reducir el fraude tecnológico en el BBVA Colombia"* y; dentro de las específicas:

[...] las de gestionar que se cumpla la integridad, confidencialidad, disponibilidad de la información procesada y almacenada en los sistemas de información del Banco, gestionar e implementar los procedimientos concernientes al control de incidentes de seguridad informática, garantizar que se instauren los procedimientos de monitorización en la modalidad 7x24x365 para eventos de seguridad del grupo, investigando posibles intentos de fraude, gestionar y propender por la implementación de las directrices corporativas o en los componentes online y procesos bath, gestionar el cumplimiento de la metodología establecida para el ciclo de vida de aplicativos del capítulo de seguridad informática, entre otras, también apoyar el desarrollo de estudios periódicos de análisis de riesgo de la plataforma tecnológica de internet, red ATMS y servidores que almacenan y procesan información clasificada como confidencial del banco,

gestionar y propender por la normal operación y disponibilidad de las diferentes plataformas de seguridad, información e internet. Igualmente se puede, entre varias, otras, igualmente se puede apreciar de dicho manual de funciones en su numeral 4º información complementaria 4.4 accesos adicionales encontrándose allí servidor checker, en el numeral 5.2 refiere a conocimientos específicos el cual indica el conocimiento está catalogado como experto dada la involucración en el diseño, análisis, instalación, administración, gestión e implementación de estrategias tecnológicas de prevención de fraude, dentro del numeral 5.4 se habla de la experiencia y se encuentra plataforma corporativa checker.

Revisada la documental acusada, encuentra la Sala que el juez de segunda instancia se remitió a las funciones asignadas al cargo de Profesional Especializado cuyo superior inmediato es el Gerente (f.º 43-55), el que no corresponde al desempeñado por el promotor del juicio; no obstante, tal dislate no lleva a variar la decisión del colegiado de instancia, en tanto al revisar las funciones asignadas para el cargo de Gerente del Grupo de Administración de Seguridad de la Información correspondiente a la dependencia de Gestión del Fraude y Seguridad de la Información (f.º 70-77) que ejercía Rubén Darío Morera, ninguna de ellas permite exonerarlo de la responsabilidad que por grave negligencia y omisión le endilgó su empleador.

Como función básica de su cargo allí se lee:

Garantizar la integridad, confidencialidad y disponibilidad de la información procesada y almacenada en los sistemas de información del Banco, dada por directrices institucionales de México y España, apoyando la implementación y mantenimiento de políticas, estándares y procedimientos de seguridad informática, en la infraestructura de Hardware y Software especializado de seguridad, por la administración y control de incidentes de seguridad informática. Así como el seguimiento y

control de la solución de los casos de fraude tecnológico - Call Center e Internet.

Y dentro de las funciones específicas, vale la pena resaltar:

#### Funciones de Dirección:

- Apoyar y gestionar la normal operación y disponibilidad (7x24x365) de las diferentes plataformas de seguridad informática en el ambiente de Producción, propendiendo siempre por obtener la mayor eficiencia y rendimiento de ellas.
- Coordinar la ejecución en la definición y mantenimiento de parámetros del ambiente de equipos de seguridad informática.
- Diseñar e implantar controles necesarios para asegurar y proteger la información del BBVA Colombia.
- Definir las estrategias para el cumplimiento de la disponibilidad de los equipos de seguridad del Banco (7x24x365) de las diferentes plataformas de Hardware del Banco.
- Definir las estrategias para la personalización y administración de las herramientas de seguridad de la información.
- Solicitar y controlar los accesos adicionales y/o aplicativos utilizados por los funcionarios de la dependencia y/o grupo a su cargo, corroborando que sean necesarios para ejecución de sus funciones.

#### Funciones de Gestión:

- Gestionar la garantía de la disponibilidad de los equipos de seguridad del Banco (7x24x365) de las diferentes plataformas de Hardware.
- Implantar controles derivados de las Directrices Corporativas de Seguridad lógica.

#### Funciones de Control:

- Gestionar y velar por la mejora de los procedimientos operativos y administrativos de la seguridad informática en las plataformas y productos instalados en el BBVA Colombia.
- Coordinar y controlar el mantenimiento preventivo y correctivo de la infraestructura de Hardware y Software de seguridad informática del Banco.
- Definir las estrategias para el monitoreo y funcionamiento de los productos de seguridad, para identificar y tomar acciones correctivas sobre las anomalías que se detecten.

#### Funciones de Riesgo:

- Definir las estrategias que apoyen la administración y monitoreo de usuarios y perfiles de los diferentes sistemas de información para el cumplimiento de las políticas y estándares de seguridad establecidos.
- Definir las estrategias que apoyen la administración, control y monitoreo a acceso lógico a las plataformas tecnológicas del Banco BBVA Colombia.
- Definir las estrategias para atender las situaciones irregulares detectadas en la red perimetral de seguridad del BBVA Colombia, desarrollando objetivamente los procesos de investigación apoyados con tecnología de punta con el fin de determinar las posibles causas, responsables y proponer soluciones lógicas que minimicen los niveles de riesgo (subraya la Sala).

De las funciones aquí mencionadas, no cabe duda que la administración, manejo, actualización y operatividad del sistema checker no estaba asignada a Rubén Darío Morera, sino al Profesional Especializado del área, cuestión que jamás desconoció el Tribunal y que tampoco pretendió achacarle al demandante, por el contrario, aseveró que *«queda claro que en efecto la persona directamente encargada de la plataforma checker era el señor Trilleros»*, sin que a pesar de la equivocación al analizar el manual de funciones, resulte errada la conclusión que de aquel derivó, pues como lo afirmó, lo cierto es que en su calidad de Gerente, su

responsabilidad de «*dirigir, controlar, gestionar y realizar todas las funciones necesarias para prevenir el riesgo de infiltración ilícita a los cajeros del banco BBVA*» se acentuaba, pues a su cargo si estaba «*la implementación y mantenimiento de políticas, estándares y procedimientos de seguridad informática, en la infraestructura de Hardware y Software especializado de seguridad*», por lo que, el exceso de confianza y la falta de verificación de la información suministrada por el personal a su cargo no pueden descargarse en Carlos Alberto Trilleras Lasso y Gabriel Enrique Ramírez Lasso, como pretende hacerlo el demandante.

En razón a su cargo, las obligaciones que tenía se encuadran dentro de un espectro amplísimo que comprende no solo las de garantizar la integridad, confidencialidad y disponibilidad de la información procesada y almacenada en los sistemas de información del banco, sino la de «*controlar*» la normal operación y disponibilidad de las diferentes plataformas de seguridad informática, dentro de las que se encuentra la checker, herramienta que de haber estado funcionando en modo activo, como quedó demostrado en el juicio, hubiera evitado el detrimento patrimonial de que fue objeto el banco demandado o por lo menos lo hubiera minimizado, aspecto que no verificó el demandante en su calidad de Gerente a sabiendas que los hechos delictivos que le habían sido puestos en conocimiento el 30 de septiembre de 2014, llevaban a extremar aún más las medidas de seguridad informática adoptadas en el banco con miras a tener un mayor margen de reacción ante un ataque

cibernético que a partir de lo narrado por Igor Alexander Gómez, era inminente que iba a ocurrir en algún momento.

Aunado a lo anterior, el demandante había desempeñado con antelación al cargo de Gerente de Seguridad en la Información, los de Responsable de Plataformas, Administrador de la Base de Datos (DB2) y Coordinador del Área de Desarrollo y Sistemas, es decir, que su conocimiento del manejo de la información y de los sistemas de información y seguridad de la entidad era amplio, lo que le permitía realizar acciones contundentes e inclusive confrontar y verificar la información suministrada por el personal que laboraba en su dependencia y, frente a la cual, su actuar no se ciñó a la diligencia necesaria ante la gravedad de los hechos.

- Capacitaciones dadas al trabajador (f.º 125-130 cuaderno anexo):

De las capacitaciones certificadas por el banco a folios 125 y 126 del cuaderno anexo y de las certificaciones aportadas (f.º 127-130) cierto es que en ninguna se hace alusión a la herramienta checker; no obstante, no puede pasar por alto la Sala la misma confesión vertida por el demandante en el libelo inicial en el hecho 35 en el que sostiene *«Si bien es cierto que mi poderdante estuvo en capacitación de la versión 3 del checker en Madrid en el año 2011, lo más cierto es que no se trataba de una especialización sobre ese producto»* (f.º 188 cuaderno de instancias), es decir, que el demandante si había recibido capacitación sobre el

sistema, no le era ajeno, por lo menos conocía sus generalidades lo que le permitía exigir del personal a cargo de su funcionamiento un informe detallado y verificar su adecuado desempeño, no obstante, como lo sostuvo el Tribunal, faltó diligencia de su parte en la verificación y alistamiento de todas las medidas de seguridad para evitar el fraude del que había sido noticiado antes de su consumación.

- Acta de descargos (f.º 18-29 cuaderno de instancias):

De la citada documental, enfatizó el *ad quem* en las respuestas dadas a las preguntas 10, 15, 16 y 17, de las que resaltó:

[...] en la pregunta 10 consiste en interrogarlo si en la función básica de objetivo del cargo tenía bajo responsabilidad garantizar la integridad, confidencialidad y disponibilidad de la información procesada y almacenada en los sistemas de información del banco, apoyando la implementación y mantenimiento de las políticas estándares, procedimientos de seguridad informática en la infraestructura del hardware y software especializado en seguridad, para lo cual el actor contestó: Si lo conozco, esto lo indica mi manual de funciones.

Se le preguntó en la 15 que indicara si el aplicativo checker tenía definido para su operatividad unas políticas y si él era el responsable del monitoreo de las mismas, a lo que contestó: que no era el responsable de efectuar el monitoreo, que para ello tenía un grupo a su cargo de especialistas definidos para efectuar la administración, la gestión y monitoreo del producto checker y sus políticas instauradas como rectoras para el aseguramiento de los cajeros automáticos.

En la pregunta 16 se le dijo cuáles eran las responsabilidades que tenía a su cargo ante la implementación y funcionamiento del checker en el banco, contestando: "que se instale de manera

adecuada y acorde a lo que ha definido corporativamente, está definido que el checker debe estar en modo activo para repeler cualquier ataque informático sobre los cajeros automáticos, quiero resaltar que antes de que el producto se instale de manera productiva, se efectuaron pruebas en el ambiente de calidad las cuales son certificadas y avaladas por el administrador del producto checker de parte de seguridad e información, que para el caso eran Carlos Alberto Trilleras y Gabriel Lazo Ramírez, conforme a esto quiero aclarar que mi función en el cargo era administrativa, como un técnico que se apoya en los especialistas que conforman parte de la plantilla de seguridad de la información con lo cual la responsabilidad de la implementación y funcionamiento del producto checker recae en la gestión técnica de los especialistas antes mencionados.

En la pregunta 17, se le pregunta que precisara la gestión como gerente para garantizar que las pruebas efectuadas por los administradores del producto cumplieran con las políticas de seguridad definidas por el banco, por lo que contestó que en los seguimientos periódicos que regularmente efectúa en el grupo de especialistas se detallan estos temas relacionados con diferentes productos que se gestionan desde la seguridad de la información y refiriéndonos puntualmente a la garantía de las pruebas, la certificación que se efectuaba en el ambiente de calidad es la prueba contundente de que está efectuado de manera correcta la aplicación de las políticas para desplegarlas luego a producción.

No equivoca el Tribunal lo sostenido por Morera ante su empleador en diligencia de descargos, en la que efectivamente pone de presente que la administración y manejo del checker no estaban a su cargo; sin embargo, si reconoce que dentro de sus responsabilidades como Gerente de Seguridad de la Información, en punto a la implementación y funcionamiento de aquella, estaba la de verificar *«que se instale de manera adecuada y acorde a lo que se ha definido corporativamente y corporativamente se ha definido que el checker debe estar en modo activo para repeler cualquier ataque informático sobre los cajeros automáticos»*, es decir, que si conocía del aplicativo, si sabía cuáles eran las

políticas de uso de la herramienta establecidas por la entidad, tenía claro que la efectividad y seguridad en la ejecución del producto dependía de que estuviera funcionando en modo activo que no, en modo aprendizaje como estaba configurado cuando se cometió el ilícito, situación que a pesar de tener clara, no verificó, se atuvo a lo informado por Carlos Alberto Trilleras Lasso – Profesional Especializado y, Gabriel Lasso Ramírez – Profesional Senior, lo que refleja, ante la severidad de la situación, la grave negligencia y el exceso de confianza que encontró demostrado el Tribunal.

La certificación dada por calidad asegura que el producto resulta útil para la protección de la información, que brinda las seguridades necesarias, no obstante, ello no es suficiente para su efectividad, se requiere de un uso y manejo adecuado que para este caso dependía de que el checker estuviera en modo activo, seguimiento que reconoce en aquella diligencia el demandante no efectuó, pues al responder la pregunta 18, indicó:

**18. PREGUNTADO:** indique por favor cómo era el proceso de seguimiento que usted hacía con los administradores del producto checker para ratificar la aplicación de las políticas?

**CONTESTO:** los seguimientos que yo hago con ellos no van a un detalle tan técnico ni tan de bajo nivel, los procesos que se efectúan en el ambiente de calidad, simplemente se relacionan de manera global. El llegar a este nivel le obligaría a una persona en este cargo a participar en el ambiente de calidad de todas las pruebas y certificarlas para tener la tranquilidad que lo que se está haciendo es real (negrilla del texto).

La situación que le fue reportada al demandante, alusiva a un riesgo inminente de filtración y ataque informático a la red de cajeros electrónicos de la entidad, representaba máxima gravedad y necesitaba acciones y políticas contundentes para repelerla, del demandante se exigía dada la responsabilidad del cargo que ocupaba, no descuidara ningún detalle y extremara medidas de seguridad que no, atenerse a informes genéricos y no verificados, los que en estas particulares circunstancias, exigían la verificación del adecuado funcionamiento de los sistemas informáticos de seguridad instalados en el banco, pues era claro que los delincuentes tenían las claves de acceso a las plataformas de la entidad.

No desconoce la suscrita que el demandante no fue pasivo ante los hechos informados, que inició indagaciones y desplegó acciones como la extracción del disco duro del equipo de cómputo asignado a Igor Alexander Gómez y estuvo presto a colaborar e informar de los avances en la investigación, sin embargo, de la diligencia descargos se observa que no fue diligente en la comprobación que todos los software de seguridad instalados en el banco estuvieran funcionando en óptimas condiciones, especialmente el checker que había sido adquirido por el BBVA atendiendo a su máxima efectividad para la protección de la información, lo que como lo refiere el mismo accionante, ratificó el área de calidad y, por el contrario, trató de justificar su proceder argumentando que la responsabilidad en el manejo de la herramienta estaba a cargo del Profesional Especializado y Profesional Senior; por tal razón, la inferencia que el Tribunal

derivó del análisis de dicha probanza, no se muestra alejada de una lógica razonable, o que transgreda la evidencia procesal, pues contrario a ello, los restantes medios de convicción a los que aludió en su providencia, y en los que la cimentó, ratifican tal conclusión.

- Política de seguridad de los sistemas de la información (f.º 320-416 cuaderno anexo):

De dicha probanza resaltó el juzgador de segunda instancia el numeral 3.3 correspondiente al ámbito de aplicación, que *«dice: el ámbito de la presente política incluye a todas las unidades, áreas, departamentos, empleados y personal subcontratado que accedan a los sistemas de información del grupo BBVA»*, así como el 4.2.1 alusivo a la responsabilidad general.

No contradice el análisis del juzgador lo que la prueba refleja, que no es nada diferente a la responsabilidad que tienen todos los trabajadores del banco, a cualquier nivel, de garantizar la seguridad de la información en razón a su confidencialidad por lo que, en el literal b) del numeral 4.2.1. al que se refiere el Tribunal expresamente se contempla: *«b. Consecuentemente, todos los empleados del Grupo BBVA y aquellos terceros subcontratados, son coparticipes de dicha responsabilidad, debiendo trabajar, desde la posición que ocupen e independientemente de la responsabilidad que explícitamente se les asigne, hacia la consecución de una adecuada seguridad de la información»* (resaltado propio).

La normatividad de seguridad de la información del banco exige un altísimo deber de cuidado y de extremas medidas que inclusive, desborda «*la responsabilidad que explícitamente se les asigne*» a los trabajadores, lo que se traduce en que no solo en la actividad diaria y ordinaria, sino en situaciones de extrema vulnerabilidad de los sistemas de información como ocurrió en el *sub lite*, el personal al servicio de la entidad deba extremar medidas en pro de la seguridad de la información; el mínimo descuido, como aquí se analiza, puede conllevar a ataques cibernéticos de grandes magnitudes como ocurrió en los cajeros de la entidad, que se vieron afectados con el hurto de más de mil millones de pesos, que pudo evitarse o por lo menos reducirse, de haberse efectuado un adecuado control a la operatividad del sistema checker iniciando por aquellas personas responsables de su funcionamiento y administración y, extendiéndose, en todo caso, al demandante, dada su posición gerencial, no solo de mayor rango jerárquico en la entidad, sino de mayor responsabilidad, conocimiento y confianza.

- Manual de instalación herramienta checker (f.º 132-141 cuaderno anexo):

En ninguna equivocación incurrió el Tribunal en la valoración de este manual pues su contenido lo único que ratifica es que para el momento en que se cometió el ilícito y se violó la seguridad informática del banco toda vez que el mismo no se encontraba en modo activo, es decir, la

protección que este suministra no estaba habilitada, lo que facilitó a los delincuentes el éxito de su operación, tal como lo reconoció el mismo promotor del juicio en diligencia de descargos en la que afirmó:

**23. PREGUNTADO:** Sírvase indicar si la condición de tener el aplicativo checker en estado de aprendizaje y no como activo, permitió o facilitó que el sistema operativo de 14 cajeros Diebold para los días 4, 5, y 6 de octubre de 2014 fueran alterados en su funcionamiento operativo y permitieran el fraude ya citado?

**CONTESTO:** si es claro que al tener el checker en modo aprendizaje, permitió de manera contundente que se materializara el fraude (negrilla del texto).

- Código de conducta (f.º 456-482 cuaderno anexo):

El yerro que deriva la censura de esta documental, deviene de la calificación que como grave diera el Tribunal a la conducta del trabajador demandante y que sirvió de justificante para su desvinculación, *«desconociendo que ninguno de los documentos allegados al expediente, en especial los relacionados como erróneamente apreciados (Políticas de seguridad, código de conducta de funciones, diligencia de descargos, manual de funciones), endilgaran dicha gravedad»*; no obstante, dicho reproche antes que corresponder a un asunto de índole fáctico, apareja un juicio de jurídico que resulta ajeno a la senda por la que se orienta el cargo.

- Interrogatorio de parte absuelto por el representante legal de la entidad bancaria demandada:

Sobre el interrogatorio de parte, se ha insistido por esta Corporación en que no es prueba hábil en la casación del trabajo, salvo que contenga confesión, lo que no se deriva de lo relacionado por el recurrente, teniendo en cuenta además que debe cumplir con los requisitos del artículo 191 del CGP, por lo que ningún yerro logra sustentarse de su errada valoración (CSJ SL4706-2021 y CSJ SL2768-2022).

- Manual de funciones Profesional Senior y Profesional Especializado en Tecnologías para la seguridad (f.º 42 y ss y, 52 y ss):

Como quedó visto en apartes que anteceden, mal podría endilgarse al Tribunal, como aquí se hace, falta de valoración del manual de funciones correspondiente al cargo de Profesional Especializado pues de manera errónea el *ad quem* lo consideró para referirse a las responsabilidades asignadas al demandante; sin embargo, como lo dejó sentado esta Sala de su valoración así como de la que se desprende del correspondiente al cargo de Profesional Senior, no se logra el quebrantamiento de la sentencia impugnada, pues antes que acreditar un yerro cometido por el juzgador, ratifican su conclusión en cuanto a que *«queda claro que en efecto la persona directamente encargada de la plataforma checker era el señor Trilleros»*, lo que, como viene de analizarse, no releva al demandante de su responsabilidad en la verificación del adecuado funcionamiento del aplicativo, así como de la veracidad de los informes rendidos por el personal a su cargo.

- Documento de descargos escritos (f.º 22-26 cuaderno anexo):

Nada distinto a lo que expresó el demandante en la diligencia de descargos que rindió ante la entidad demandada, puede extraerse de la documental bajo análisis, en ella, nuevamente pretendió excusar su responsabilidad y su falta de diligencia en los Profesionales Especializado y Senior, lo que, como se analizó en precedencia no es suficiente para considerar que el despido de que fue objeto no tuvo sustento en causa alguna.

- Correos electrónicos (f.º 236-241 cuaderno anexo):

En estos documentos el demandante ratifica que el manejo, administración y adecuado funcionamiento de la herramienta checker *«forma parte de nuestra gestión diaria en la red de Atm's»*, es decir, reconoce que estaba bajo su responsabilidad que la misma prestara toda la seguridad informática para la que estaba diseñada, lo que, como se ha analizado a lo largo de esta decisión, exigía que se verificara por los profesionales a cargo de aquella así como por el demandante, dada su función gerencial, que el mismo se encontraba en modo activo, pues solo así, podía contrarrestarse el actuar delincuencia que desencadenó el hurto de los dineros de propiedad del BBVA.

Ellos reflejan, además, las acciones emprendidas por el área de Seguridad de la Información una vez tuvieron conocimiento de la situación acaecida con Igor Alexander

Gómez, dentro de las que se destacan el análisis a través del aplicativo Netopp que llevó a detectar que «en el cajero nro 0011 de la Avda. Chile la presencia de archivos sospechosos» lo que conllevó al cambio de su disco duro; así mismo se llevó a cabo el procesamiento de la información sobre los accesos remotos efectuados por Gómez así de los «Logs de los cajeros mencionados», pero nótese que a pesar que se inició un plan de acción, jamás se menciona la verificación del adecuado funcionamiento del checker a pesar de que el mismo Morera reconoce que de estar en modo activo, jamás se hubiera consumado el fraude bancario.

- Testimonios de John Ardila Aponte y Gabriel Lasso Ramírez:

Como lo ha sostenido de antaño esta Corporación, los testimonios no son prueba calificada autónoma para sustentar el recurso de casación, sino que dependen de la prosperidad de un medio que tenga tal condición -documento auténtico, confesión judicial o inspección ocular- según la restricción contenida en el artículo 7º de la Ley 16 de 1969, norma que fue declarada exequible por la Corte Constitucional en sentencia C-140 de 29 de marzo de 1995, de manera que la inconformidad con la desacertada valoración probatoria por parte del Tribunal, no puede abordarse ante la ausencia de tal presupuesto (CSJ SL4030-2019).

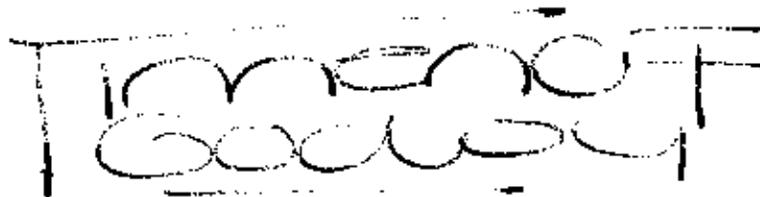
Para finalizar, no está por demás recordar que el hecho de que el sentenciador de alzada le asignara un mayor grado

de convicción a unos medios de prueba respecto de otros, no significa que hubiese incurrido en los desatinos denunciados, pues tal actuar se enmarca dentro de las facultades que le otorga el artículo 61 del Código Procesal del Trabajo y de la Seguridad Social, esto es, en el uso legítimo de la libertad de apreciación probatoria.

En consecuencia, el análisis objetivo de los medios probatorios estudiados con anterioridad, acredita con suficiencia que el demandante incurrió en las faltas endilgadas en la carta de terminación del contrato, de modo que no erró el *ad quem* al valorarlas ni tampoco en la conclusión a la que arribó, que el despido del trabajador fue justificado.

De conformidad con lo aquí discurrido y al no haberse acreditado los errores de hecho endilgados a la sentencia recurrida, el cargo no debía prosperar.

*Fecha ut supra,*



**JIMENA ISABEL GODOY FAJARDO**