RAD: 110014003082-2022-00841-00 / RECURSO DE REPOSICIÓN EN SUBSIDIO DE APELACIÓN CONTRA AUTO DEL 28 de noviembre de 2023 / VERBAL – RESPONSABILIDAD CIVIL

ABOGADOS CG <notificacionabogadoscg@gmail.com>

Lun 04/12/2023 16:57

Para:Juzgado 82 Civil Municipal - Bogotá - Bogotá D.C. <cmpl82bt@cendoj.ramajudicial.gov.co>
CC:cgarrotejuridica@gmail.com <cgarrotejuridica@gmail.com>

1 archivos adjuntos (9 MB)

RECURSO Y ANEXOS.pdf;

Señores
JUZGADO OCHENTA Y DOS CIVIL MUNICIPAL DE BOGOTÁ
Transitoriamente Juzgado 64 de Pequeñas Causas y Competencia Múltiple de Bogotá
E.S.D

PROCESO: **VERBAL – RESPONSABILIDAD CIVIL**
DEMANDANTE: **GRUPO MICROSISTEMAS COLOMBIA S.A.S.**
DEMANDADO: **SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S.**
RADICACIÓN: **110014003082-2022-00841-00**

ASUNTO: **RECURSO DE REPOSICIÓN EN SUBSIDIO DE APELACIÓN**

CAROLINA GARROTE MICOLTA, mayor y vecina de esta ciudad, identificada con la cédula de ciudadanía No. 1.130.664.298, abogada titulada en ejercicio, portadora de la tarjeta profesional No.197771 del Consejo Superior de la Judicatura, en mi calidad de apoderada judicial de la sociedad demandada **SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S. "SOTELCOM SAS",** a través del presente escrito, encontrándome dentro del término que disponen los artículos 110, 318 y 321 del Código General del Proceso, me permito interponer **RECURSO DE REPOSICIÓN EN SUBSIDIO DE APELACIÓN** contra el auto interlocutorio del 28 de noviembre de 2023, en los términos del memorial adjunto.

Cordialmente,

CAROLINA GARROTE MICOLTA
C.C No.1.130.664.298
TP. No.197771 del CS de la J

Señor
JUZGADO OCHENTA Y DOS CIVIL MUNICIPAL DE BOGOTÁ
Transitoriamente Juzgado 64 de Pequeñas Causas y Competencia Múltiple de Bogotá E.S.D

PROCESO: **VERBAL – RESPONSABILDIAD CIVIL**
DEMANDANTE: **GRUPO MICROSISTEMAS COLOMBIA S.A.S.**
DEMANDADO: **SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S.**
RADICACIÓN: **110014003082-2022-00841-00**

ASUNTO: **RECURSO DE REPOSICIÓN EN SUBSIDIO DE APELACIÓN**

CAROLINA GARROTE MICOLTA, mayor y vecina de esta ciudad, identificada con la cedula de ciudadanía No. 1.130.664.298, abogada titulada en ejercicio, portadora de la tarjeta profesional No.197771 del Consejo Superior de la Judicatura, en mi calidad de apoderada judicial de la sociedad demandada **SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S. "SOTELCOM SAS",** a través del presente escrito, encontrándome dentro del término que disponen los artículos 110, 318 y 321 del Código General del Proceso, me permito interponer **RECURSO DE REPOSICIÓN EN SUBSIDIO DE APELACIÓN** contra el auto interlocutorio del 28 de noviembre de 2023, notificado por estado No.133 del 29 de noviembre de 2023, a través del cual se tuvo por no contestada la demanda por parte de mis representadas en los términos que se exponen más adelante.

CONSIDERACIONES PREVIAS AL RECURSO.

El JUZGADO OCHENTA Y DOS CIVIL MUNICIPAL DE BOGOTÁ a través de auto interlocutorio del 28 de noviembre de 2023, dispuso lo siguiente:

> *RIMERO: TENER en cuenta que la sociedad demandada fue notificada del contenido del auto admisorio de la demanda en la forma prevista en el artículo 8° de la Ley 2213 de 2022, quien dentro del término traslado guardó silencio.*
>
> *SEGUNDO: ABRIR a pruebas el presente asunto, para lo cual se decretan las siguientes,*
>
> *2.1. DEMANDANTE:*
>
> *2.1.1. DOCUMENTAL de ser legales y procedentes las aportadas tanto en el líbelo introductor como al momento de descorrer las excepciones, por el valor que la ley les asigne en su oportunidad procésiva, al tenor literal del artículo 176 del C.G.P.*
>
> *2.1.2. INTERROGATORIO DE PARTE. CITAR al representante legal de SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S. "SOTELCOM", con el fin de que RINDA INTERROGATORIO que de este requiere el demandante, decisión que se notifica por estado.*
>
> *2.1.3. OFICIAR: Por secretaría oficiar a la ALCALDIA DE CALI para que en el término de cinco (5) contados a partir de la recepción de la respectiva comunicación, allegue con destino al proceso de la referencia copia de: i) De los requisitos de adjudicación para el contrato suscrito con la unión temporal SOTELCOM SAFEID, ii) Certificación de que indique si dentro de esos requisitos precontractuales o contractuales para el contrato suscrito, se utilizó la factura No.2443 emitida por GMS a SOTELCOM –lo anterior de ser procedente-, iii) Copia del contrato suscrito y modificaciones al mismo.*
>
> *Precisar a la parte demandante que la carga del recaudo de la anterior prueba le es impuesta al tenor de lo previsto en el artículo 167 del C.G.P.*

2.1.4. TESTIMONIALES: De conformidad con lo previsto en el artículo 212 del C.G.P., se niega el decretó del testimonio de la señora MARIA SANDRA GALVES, puesto que, no se enunció concretamente los hechos en particular que se pretenden probar del escrito de la demanda que se allegó

2.2. DEMANDADOS
2.2.1. Guardo silencio frente a la demanda.
2.3. DE OFICIO
2.3.1. CITAR al representante legal de la demandante GRUPO MICROSISTEMAS COLOMBIA S.A.S., con el fin de que RINDA INTERROGATORIO que de este requiere el Despacho, decisión que se notifica por estado.

TERCERO: CONVOCAR AUDIENCIA INICIAL (VIRTUAL) bajo los preceptos del artículo 392 del Código General del Proceso, la que se celebrará a la hora de las 9:30 del día doce (12) del mes de marzo del año dos mil veinticuatro (2024).

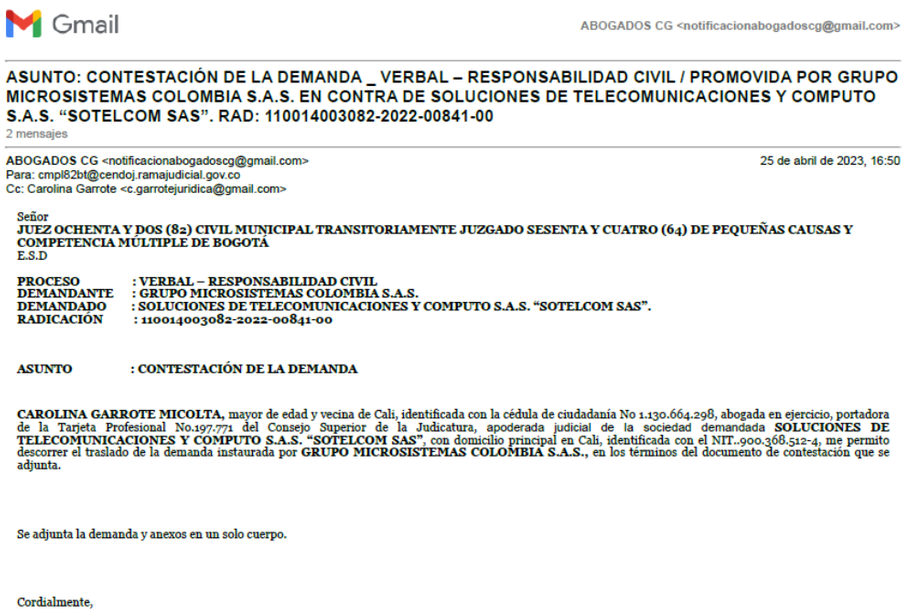
Advertir a las partes que, si en dicha ocasión se llegaré recaudar en integridad las pruebas por principio de concentración, se continuará con el trámite del proceso y se proferirá sentencia.

(…)

Para tomar su decisión el Juzgado adujo que la demanda SOTELCOM SAS fue notificada en los términos del artículo 8vo de la ley 2213 de 2022 y la misma guardó silencio.

SUSTENTANCIÓN DEL RECURSO

Para tomar su decisión el despacho omitió revisar si en efecto la entidad que represento efectivamente omitió descorrer el traslado de la demanda, pues en el expediente digital ni siquiera reposa el escrito de contestación remitido de nuestra parte del pasado 25 de abril de 2023 a la dirección electrónica dispuesta para tal fin por esta sede judicial como se ilustra continuación:



Gmail ABOGADOS CG <notificacionabogadoscg@gmail.com>

ASUNTO: CONTESTACIÓN DE LA DEMANDA _ VERBAL – RESPONSABILIDAD CIVIL / PROMOVIDA POR GRUPO MICROSISTEMAS COLOMBIA S.A.S. EN CONTRA DE SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S. "SOTELCOM SAS". RAD: 110014003082-2022-00841-00

2 mensajes

ABOGADOS CG <notificacionabogadoscg@gmail.com> 25 de abril de 2023, 16:50
Para: cmpl82bt@cendoj.ramajudicial.gov.co
Cc: Carolina Garrote <c.garrotejuridica@gmail.com>

Señor
JUEZ OCHENTA Y DOS (82) CIVIL MUNICIPAL TRANSITORIAMENTE JUZGADO SESENTA Y CUATRO (64) DE PEQUEÑAS CAUSAS Y COMPETENCIA MÚLTIPLE DE BOGOTÁ
E.S.D

PROCESO : VERBAL – RESPONSABILIDAD CIVIL
DEMANDANTE : GRUPO MICROSISTEMAS COLOMBIA S.A.S.
DEMANDADO : SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S. "SOTELCOM SAS".
RADICACIÓN : 110014003082-2022-00841-00

ASUNTO : CONTESTACIÓN DE LA DEMANDA

CAROLINA GARROTE MICOLTA, mayor de edad y vecina de Cali, identificada con la cédula de ciudadanía No 1.130.664.298, abogada en ejercicio, portadora de la Tarjeta Profesional No.197.771 del Consejo Superior de la Judicatura, apoderada judicial de la sociedad demandada **SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S. "SOTELCOM SAS"**, con domicilio principal en Cali, identificada con el NIT..900.368.512-4, me permito descorrer el traslado de la demanda instaurada por **GRUPO MICROSISTEMAS COLOMBIA S.A.S.**, en los términos del documento de contestación que se adjunta.

Se adjunta la demanda y anexos en un solo cuerpo.

Cordialmente,

Inclusive en la referida fecha se remitió un segundo correo con un segundo escrito, ya que por error involuntario se remitió un escrito inicial con 54 folios cuando en realidad debió remitirse uno de 68 folios, sin embargo, en el expediente no reposa ninguno de los escritos, que si en gracia de discusión se hubiese recepcionado de manera extemporánea por el despacho debiera estar glosado en la carpeta digital.

De otra parte, la remisión de la demanda se realizó de manera electrónica el pasado 28 de marzo de 2023, pero se allegó con los anexos casi totalmente ilegibles, lo que conllevó a solicitar a la apoderada de la parte actora que remitiera de nuevo la

demanda con los respectivos anexos pero legibles, lo cual fua atendido por la Doctora DORIS BEATRIZ OSPINA SANCHEZ, quien remitió el archivo el 30 de marzo de 2023 a las 5:46 p.m., advirtiendo de tal situación al despacho el 10 de abril de 2023 a las 8:00 a.m., como se ilustra a continuación:

Correo enviado por SOTELCOM SAS a la Dra. DORIS BEATRIZ OSPINA el 30 de marzo de 2023:

Tel .3216262 Cel. 316 5219627 Bogotá D.C.

De: Ing. Luis F Pabon T <luis.pabon@Sotelcom.co>
Enviado: jueves, 30 de marzo de 2023 3:21 p. m.
Para: informacion@gmsseguridad.com <informacion@gmsseguridad.com>; cmpl82bt@cendoj.ramajudicial.gov.co <cmpl82bt@cendoj.ramajudicial.gov.co>; dorisospinas@hotmail.com <dorisospinas@hotmail.com>; informacion@gmsseguridad.com <informacion@gmsseguridad.com>
Cc: Carolina Garrote <c.garrotejuridica@gmail.com>
Asunto: RV: TRASLADO DEMANDA PARCIALMENTE ILEGIBLE - GSM vs SOTELCOM

Sres.
JUZGADO OCHENTA Y DOS (82) CIVIL MUNICIPAL DE BOGOTA D.C. TRANSITORIAMENTE JUZGADO 64 DE PEQUEÑAS CAUSAS Y CMPETENCIA MULTIPLE DE BOGOTA D.C.
GRUPO MICROSISTEMAS COLOMBIA S.A.S.
L.C

El día martes 28 de marzo DE 2023 se recibió correo electrónico con comunicación electrónica en la cual se anexaban algunos documentos que se desean hacer valer como prueba dentro del proceso pero se encuentran ILEGIBLES. Por lo tanto solicito respetuosamente respetado juez que se ordene al demandante digitalizar nuevamente los anexos de la demanda porque en su mayoría no son legibles.

Este defecto al revisar la admisión de la demanda no se advirtió, siendo fundamental que las pruebas se puedan trasladar en debida forma a la parte demandada para ejercer el derecho de contradicción.

Así las cosas solicito respetuosamente señor juez se suspendan los términos de contestación de la demanda hasta que se corrija el defecto.

Cordialmente
Luis Fernando Pabon
Rep Legal
SOTELCOM SAS

Correo del 30 de marzo de 2023 remitido por la Dra. DORIS BETRAIZ OSPINA a SOTELCOM SAS a las 5:36 p.m. con la demanda y anexos legibles:

Tel .3216262 Cel. 316 5219627 Bogotá D.C.

De: Ing. Luis F Pabon T <luis.pabon@Sotelcom.co>
Enviado: jueves, 30 de marzo de 2023 3:21 p. m.
Para: informacion@gmsseguridad.com <informacion@gmsseguridad.com>; cmpl82bt@cendoj.ramajudicial.gov.co <cmpl82bt@cendoj.ramajudicial.gov.co>; dorisospinas@hotmail.com <dorisospinas@hotmail.com>; informacion@gmsseguridad.com <informacion@gmsseguridad.com>
Cc: Carolina Garrote <c.garrotejuridica@gmail.com>
Asunto: RV: TRASLADO DEMANDA PARCIALMENTE ILEGIBLE - GSM vs SOTELCOM

Sres.
JUZGADO OCHENTA Y DOS (82) CIVIL MUNICIPAL DE BOGOTA D.C. TRANSITORIAMENTE JUZGADO 64 DE PEQUEÑAS CAUSAS Y CMPETENCIA MULTIPLE DE BOGOTA D.C.
GRUPO MICROSISTEMAS COLOMBIA S.A.S.
L.C

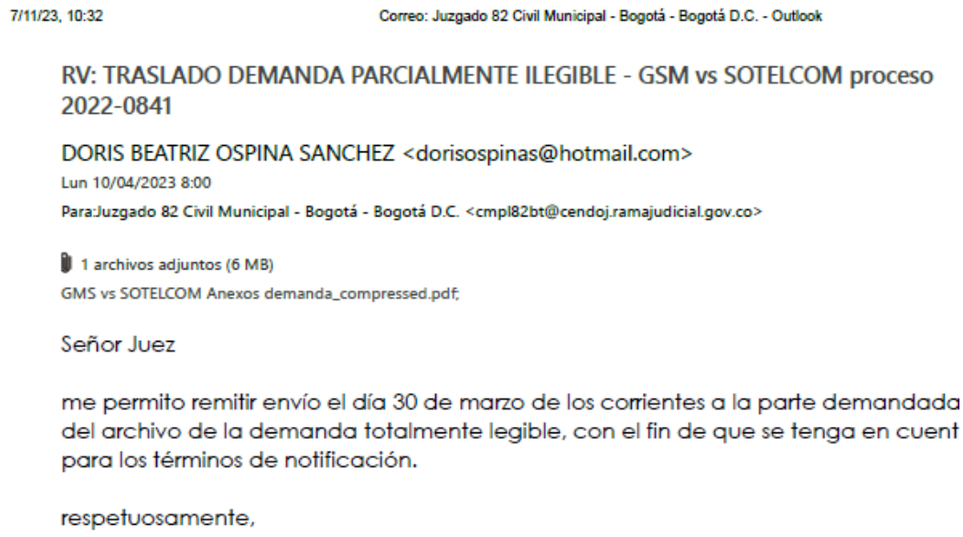
El día martes 28 de marzo DE 2023 se recibió correo electrónico con comunicación electrónica en la cual se anexaban algunos documentos que se desean hacer valer como prueba dentro del proceso pero se encuentran ILEGIBLES. Por lo tanto solicito respetuosamente respetado juez que se ordene al demandante digitalizar nuevamente los anexos de la demanda porque en su mayoría no son legibles.

Este defecto al revisar la admisión de la demanda no se advirtió, siendo fundamental que las pruebas se puedan trasladar en debida forma a la parte demandada para ejercer el derecho de contradicción.

Así las cosas solicito respetuosamente señor juez se suspendan los términos de contestación de la demanda hasta que se corrija el defecto.

Cordialmente
Luis Fernando Pabon
Rep Legal
SOTELCOM SAS

Correo del 10 de abril, de 2023 remitido por la Dra. **DORIS BETRAIZ OSPINA** al despacho informando la remisión de la demanda totalmente legible, aplicando de esa manera los principio de lealtad procesal y publicidad a efectos de evitar nulidades procesales como las que se pueden suscitar en el presente:



7/11/23, 10:32 Correo: Juzgado 82 Civil Municipal - Bogotá - Bogotá D.C. - Outlook

RV: TRASLADO DEMANDA PARCIALMENTE ILEGIBLE - GSM vs SOTELCOM proceso 2022-0841

DORIS BEATRIZ OSPINA SANCHEZ <dorisospinas@hotmail.com>
Lun 10/04/2023 8:00
Para:Juzgado 82 Civil Municipal - Bogotá - Bogotá D.C. <cmpl82bt@cendoj.ramajudicial.gov.co>

1 archivos adjuntos (6 MB)
GMS vs SOTELCOM Anexos demanda_compressed.pdf;

Señor Juez

me permito remitir envío el día 30 de marzo de los corrientes a la parte demandada del archivo de la demanda totalmente legible, con el fin de que se tenga en cuent para los términos de notificación.

respetuosamente,

Es así como el despacho comete dos yerros, el primero tiene que ver con la inobservancia de la contestación a la demanda radicada por SOTELCOM S.A.S el 25 de abril de 2023 y tampoco advirtió el envío de la demanda con los anexos ilegibles, lo que impidió en primera medida que la notificación surtiera efectos, pues tal situación se equipara a el envío sin anexos, pues de nada sirve recibir una demanda con documentos ilegibles.

La respecto es importante señalar que, para que la notificación surta efectos a la luz de la ley 2213 de 2022, se hace que la demanda sea remitida con su anexos, cosa que se intentó realizar pero no de la manera adecuada, pues se itera no se remitió con las pruebas legibles a efectos de hacerlas valer frente a mi representada, lo que conllevó a que la apoderada judicial de la parte activa los remitiera nuevamente y de esa manera empezar a contabilizar de nuevo los términos de notificación atemperándose a lo dispuesto en la normatividad en comento (ley 2213 de 2022).

Frente a lo anterior es preciso traer a colocación los dispuesto en la sentencia C-420 de 2020 para que entienda surtida la notificación de la demanda, condicionada por la corte Constitucional al realizar el control de constitucionalidad del Decreto Legislativo 806 del 4 de junio de 2020, en el cual dispuso lo siguiente:

> ***"Tercero. Declarar EXEQUIBLE*** *de manera condicionada el inciso 3 del artículo 8 y el parágrafo del artículo 9 del Decreto Legislativo 806 de 2020, en el entendido de que el* ***término allí dispuesto empezará a contarse cuando el iniciador recepcione acuse de recibo o se pueda por otro medio constatar el acceso del destinatario al mensaje."***

Ahora bien, al referirse al inciso 3º del artículo 8 del citado decreto, la alta corporación expuso:

> *351. El inciso 3 del artículo 8° del Decreto Legislativo 806 de 2020 prevé que "la notificación personal se entenderá realizada una vez transcurridos dos días hábiles siguientes al envío del mensaje y los términos empezarán a correr a partir del día siguiente al de la notificación". Una regla semejante se contiene en el parágrafo del artículo 9°, según el cual, "Cuando una parte acredite haber enviado un escrito del cual deba correrse traslado a los demás sujetos procesales, mediante la remisión de la copia por un canal digital, se prescindirá del traslado por secretaría, el cual se entenderá realizado a los dos (2) días hábiles siguientes al del envío del mensaje y el término respectivo empezará a correr a partir del día siguiente". Al ser consultado sobre las razones que motivaron estos apartados normativos, el*

*Gobierno nacional informó que la medida tiene por objeto conceder un término razonable para que los sujetos procesales puedan revisar su bandeja de entrada, partiendo del reconocimiento de que no todas las personas tienen acceso permanente a Internet . **De esta respuesta no se sigue que, al adoptar la medida, el Gobierno pretendiera desconocer el precedente descrito relativo a la validez de la notificación a partir de su recepción por el destinatario –en el caso de la primera disposición– o del traslado de que trata la segunda disposición**, **que no de su envío.***

*352. No obstante, la Corte encuentra que, tal como fue adoptada la disposición, es posible interpretar que el hito para calcular el inicio de los términos de ejecutoria de la decisión notificada o del traslado no corresponde a la fecha de recepción del mensaje en el correo electrónico de destino, sino a la fecha de envío. **Esta interpretación implicaría admitir que, aun en los eventos en que el mensaje no haya sido efectivamente recibido en el correo de destino, la notificación o el traslado se tendría por surtido por el solo hecho de haber transcurrido dos días desde su envío**. Una interpretación en este sentido desconoce la garantía constitucional de publicidad y por lo mismo contradice la Constitución.*

Finalmente la Corte en aras de precaver interpretaciones que desconozcan la teleología de las notificaciones, decir sobre la garantía de publicidad integrada al derecho al debido proceso arribó a la siguiente conclusión:

"En consecuencia, la Corte declarará la exequibilidad condicionada del inciso 3 del artículo 8° y del parágrafo del artículo 9° del Decreto Legislativo sub examine en el entendido de que el término de dos (02) días allí dispuesto empezará a contarse cuando el iniciador recepcione acuse de recibo o se pueda por otro medio constatar el acceso del destinatario al mensaje. A juicio de la Sala, este condicionamiento (i) elimina la interpretación de la medida que desconoce la garantía de publicidad, (ii) armoniza las disposiciones examinadas con la regulación existente en materia de notificaciones personales mediante correo electrónico prevista en los artículos 291 y 612 del CGP y, por último, (iii) orienta la aplicación del remedio de nulidad previsto en el artículo 8°, en tanto provee a los jueces mayores elementos de juicio para valorar su ocurrencia."

Ahora bien, además de la recepción del mensaje la norma comporta una situación más importante como es la remisión de la demanda y sus anexos, como los señala el artículo 6 del la ley 2213 de 2022, veamos:

"ARTÍCULO 6o. DEMANDA. La demanda indicará el canal digital donde deben ser notificadas las partes, sus representantes y apoderados, los testigos, peritos y cualquier tercero que deba ser citado al proceso, so pena de su inadmisión. No obstante, en caso que el demandante desconozca el canal digital donde deben ser notificados los peritos, testigos o cualquier tercero que deba ser citado al proceso, podrá indicarlo así en la demanda sin que ello implique su inadmisión.

Asimismo, contendrá los anexos en medio electrónico, los cuales corresponderán a los enunciados y enumerados en la demanda.

Las demandas se presentarán en forma de mensaje de datos, lo mismo que todos sus anexos, a las direcciones de correo electrónico que el Consejo Superior de la Judicatura disponga para efectos del reparto, cuando haya lugar a este.

De las demandas y sus anexos no será necesario acompañar copias físicas, ni electrónicas para el archivo del juzgado, ni para el traslado.

En cualquier jurisdicción, incluido el proceso arbitral y las autoridades administrativas que ejerzan funciones jurisdiccionales, salvo cuando se soliciten medidas cautelares previas o se desconozca el lugar donde recibirá

*notificaciones el demandado, el demandante, al presentar la demanda, simultáneamente deberá enviar por medio electrónico copia de ella y de sus anexos a los demandados. Del mismo modo deberá proceder el demandante cuando al inadmitirse la demanda presente.el escrito de subsanación****. El secretario o el funcionario que haga sus veces velará por el cumplimiento de este deber, sin cuya acreditación la autoridad judicial inadmitirá la demanda.*** *De no conocerse el canal digital de la parte demandada, se acreditará con la demanda el envío físico de la misma con sus anexos.*

En caso de que el demandante haya remitido copia de la demanda con todos sus anexos al demandado, al admitirse la demanda la notificación personal se limitará al envío del auto admisorio al demandado.

Es así como el último inciso del artículo en cita indica que deben enviarse todos los anexos para que al admitirse la demanda la notificación personal se limite al envío del auto admisorio al demandado.

Con el actuar del despacho se le está vulnerando el derecho de defensa y contradicción a mi representada, pues como se pudo demostrar con calidad de certeza, la notificación personal llevó a cabo en realidad el 31 de marzo de 2023, dado que el correo con las pruebas legibles fue enviado el 30 de marzo de 2023 a las 5:46 p.m., es decir por fuer del horario judicial, de ahí que se entienda surtida el 31 de marzo como ya se ilustró con suficiencia.

En consideración a lo anterior, se puede advertir que la notificación no se surtió en las condiciones dispuestas en el decreto y la sentencia C-420 de 2020, pues no se cumplió inicialmente con el principio de publicidad, subsanado con posterioridad, pero que el despacho no advirtió.

Con fundamento en los argumentos y razones de derecho argüidos en líneas anteriores, solicito al señor Juez lo siguiente:

PETICION

1. ***SE REPONGA*** la providencia mediante la cual se tuvo por no contestada la demanda por parte de mi representada, **SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S.**y en su lugar se sirva a reponer para revocar el auto recurrido, notificando nuevamente la demanda con el correspondiente traslado.

2. De ***NO REPONERSE PARA REVOCARSE*** la procidencia, solicito muy respetuosamente se remita al superior jerárquico, a fin de que desate el recurso de apelación y en aras de que revoque la decisión de primera instancia y en su lugar se ordene al JUZGADO OCHENTA Y DOS CIVIL MUNICIPAL DE BOGOTÁ, con fundamento en las razones de derecho expuestas en precedencia.

FUDAMENTOS DE DERECHO

El presente recurso se presenta de conformidad con lo dispuesto en el numeral tercero de los artículos 63 y 65 del Código Procesal del trabajo y de la seguridad Social, en concordancia con los artículos 321 y 322 del código general del proceso, los artículos 5 y 8 del decreto 806 de 2020.

La sentencia C-420 de 2020 proferida por la Corte Constitucional.

COMPETENCIA

Es usted competente señor Juez por conocer del recurso de reposición y en subsidio de apelación el Tribunal Superior del Distrito Judicial de Bogotá por ser el superior jerárquico.

PRUEBAS

- Copia del correo electrónico mediante el cual se remitió la demanda y anexos de fecha 25 de abril de 2023
- Copia de la contestación de la demanda.

ANEXOS

- Lo enunciado en el acápite pruebas

Del señor Juez, atentamente,

CAROLINA GARROTE MICOLTA
C.C No.1.130.664.298
TP. No.197771 del CS de la J

ASUNTO: CONTESTACIÓN DE LA DEMANDA _ VERBAL – RESPONSABILIDAD CIVIL / PROMOVIDA POR GRUPO MICROSISTEMAS COLOMBIA S.A.S. EN CONTRA DE SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S. “SOTELCOM SAS”. RAD: 110014003082-2022-00841-00

2 mensajes

ABOGADOS CG <notificacionabogadoscg@gmail.com> 25 de abril de 2023, 16:50
Para: cmpl82bt@cendoj.ramajudicial.gov.co
Cc: Carolina Garrote <c.garrotejuridica@gmail.com>

Señor
JUEZ OCHENTA Y DOS (82) CIVIL MUNICIPAL TRANSITORIAMENTE JUZGADO SESENTA Y CUATRO (64) DE PEQUEÑAS CAUSAS Y COMPETENCIA MÚLTIPLE DE BOGOTÁ
E.S.D

PROCESO : VERBAL – RESPONSABILIDAD CIVIL
DEMANDANTE : GRUPO MICROSISTEMAS COLOMBIA S.A.S.
DEMANDADO : SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S. “SOTELCOM SAS”.
RADICACIÓN : 110014003082-2022-00841-00

ASUNTO : CONTESTACIÓN DE LA DEMANDA

CAROLINA GARROTE MICOLTA, mayor de edad y vecina de Cali, identificada con la cédula de ciudadanía No 1.130.664.298, abogada en ejercicio, portadora de la Tarjeta Profesional No.197.771 del Consejo Superior de la Judicatura, apoderada judicial de la sociedad demandada **SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S. “SOTELCOM SAS”**, con domicilio principal en Cali, identificada con el NIT..900.368.512-4, me permito descorrer el traslado de la demanda instaurada por **GRUPO MICROSISTEMAS COLOMBIA S.A.S.,** en los términos del documento de contestación que se adjunta.

Se adjunta la demanda y anexos en un solo cuerpo.

Cordialmente,

CAROLINA GARROTE MICOLTA

C.C. No.1.130.664.298

T.P No.197.771 del CS de la J.

CONTESTACIÓN Y ANEXOS.pdf
7312K

ABOGADOS CG <notificacionabogadoscg@gmail.com> 25 de abril de 2023, 16:55
Para: cmpl82bt@cendoj.ramajudicial.gov.co

Por favor tener en cuenta este último documento de contestación ya que se envió el anterior incompleto.

Muchas gracias.
[El texto citado está oculto]

CONTESTACIÓN Y ANEXOS FN.pdf
8765K

Señor
JUEZ OCHENTA Y DOS (82) CIVIL MUNICIPAL TRANSITORIAMENTE JUZGADO SESENTA Y CUATRO (64) DE PEQUEÑAS CAUSAS Y COMPETENCIA MULTIPLE DE BOGOTÁ
E.S.D

PROCESO : PROCESO VERBAL – RESPONSABILDIAD CIVIL
DEMANDANTE : GRUPO MICROSISTEMAS COLOMBIA S.A.S.
DEMANDADO : SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S. "SOTELCOM SAS".
RADICACIÓN : 110014003082-2022-00841-00

CAROLINA GARROTE MICOLTA, mayor de edad y vecina de Cali, identificada con la cédula de ciudadanía No 1.130.664.298, abogada en ejercicio, portadora de la Tarjeta Profesional No.197.771 del Consejo Superior de la Judicatura, apoderada judicial de la sociedad demandada **SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S. "SOTELCOM SAS"**, con domicilio principal en Cali, identificada con el NIT..900.368.512-4, me permito descorrer el traslado de la demanda instaurada por **GRUPO MICROSISTEMAS COLOMBIA S.A.S.,** postura que hago de la siguiente manera:

I. FRENTE A LOS HECHOS

AL HECHO 1. ES CIERTO. Así se desprende del certificado de existencia y representación legal de la demandante.

AL HECHO 2. ES CIERTO SOLO RESPECTO el único servicio prestado por la empresa **GRUPO MICROSISTEMAS COLOMBIA S.A.S** a SOLTELCOM corresponde a un análisis forense realizado frente al incidente reportado en los servidores PJD y SAPRouter de la ALCALDIA DE CALI, quien es cliente de SOTELCOM SAS, servicio que fue cancelado por mi representada una vez culminada la prestación del servicio por valor de $4.025.000, a través de la factura de compra 2492 con fecha de creación del 12 de diciembre de 2019 y fecha de vencimiento del 12 de enero de 2020, cuya transferencia se realizó el 17 de enero de 2020.

Cabe señalar que, la empresa **GRUPO MICROSISTEMAS COLOMBIA S.A.S** pretende el pago de la factura de compra No.2443 por un servicio que nunca se prestó, pues la labor nunca se ejecuto por razones ajenas a la voluntad de SOTELCOM, ya que el cliente final no remitió la información correspondiente para iniciar la labores que se pretendieron contratar.

AL HECHO 3. NO ES CIERTO. Toda vez que el servicio que se pretendió mediante la orden de compra nunca se prestó por parte **de GRUPO MICROSISTEMAS COLOMBIA S.A.S,** ello en el entendido que, si bien se emitió la orden de compra, el

servicio nunca se prestó por falta por falta de una información técnica que debió suministrar el cliente final de SOTELCOM SAS para iniciar con la prestación del servicio que se pretendía.

Los servicios ofertados por la empresa de **GRUPO MICROSISTEMAS COLOMBIA S.A.S,** y sobre los cuales se pretendió contratar y que se describen a continuación nunca se prestaron:

- Cod.s0122 SERVICIOS
  Investigación protección de marca x 1 año (5 palabras clave + inforn mensual) por valor de $16.371.696
- Cod.s1022 SERVICIOS
  Consultoría ETHICAL HACKING TET Y RETEST por valor de $5.116.155

Tal es así que la empresa no tiene pruebas o informes de haber prestado el servicio, e incluso nunca remitió la factura física para el pago.

Aunado a lo anterior, de los correos cruzados entre el personal de la empresa se puede extraer claramente la aceptación de que la empresa **GRUPO MICROSISTEMAS COLOMBIA S.A.S** nunca prestó los servicios cobrados.

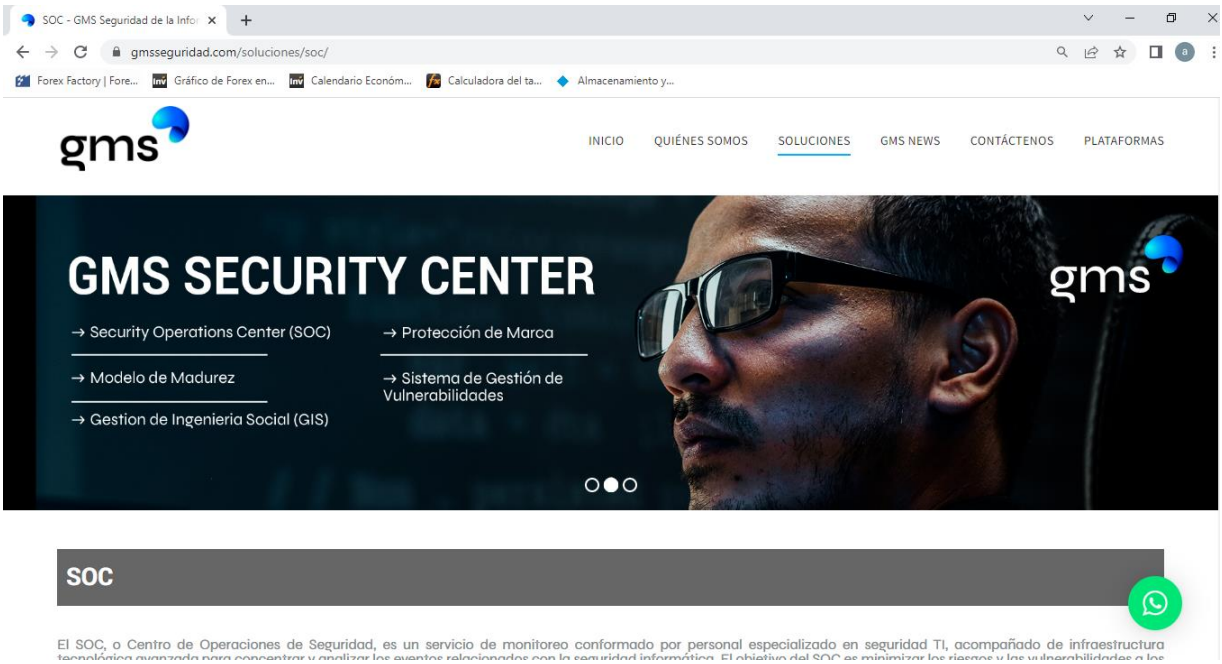
AL HECHO 4. ES PARCIALMENTE CIERTO. La empresa SOTELCOM SAS en efecto expidió la orden de compra, pero **GRUPO MICROSISTEMAS COLOMBIA S.A.S** nunca se prestó el servicio que se pretendió contratar, tal es así que, la factura no tiene fecha ni sello de recibido y fue rechazado el cobro por la falta de prestación del servicio.

AL HECHO 5. NO ES CIERTO. Si bien la factura se pretendió cobrar mediante correo electrónico de fecha 26 de noviembre de 2019, y posterior envío físico, la misma nunca se aceptó por parte de mi presentada, tal es así que brilla por su ausencia la firma o sello de aceptación por parte de SOTELCOM SAS.

Quiere decir entonces que la supuesta prestación del servicio solo quedó en una oferta de servicios, ya que nunca se desarrollo ninguna de las actividades ofrecidas por **GRUPO MICROSISTEMAS COLOMBIA S.A.S,** en tal sentido no es procedente cobrar un servicio que nunca se materializó.

AL HECHO 6. NO ES CIERTO. El presunto servicio contratado por GRUPO MICROSISTEMAS COLOMBIA S.A.S a su proveedor en Ecuador por la suma de US.5.700, no corresponde al servicio que pretendió contratar SOLTELCOM SAS, pues un servicio facturado por la empresa de Ecuador corresponde a un SOC, el cual aduce la demandante les tocó comprar para prestarnos el servicio, no tiene ningún sustento factico, ya que dicha plataforma (SOC) no es para uso exclusivo de prestar un servicio

a SOTELCOM SAS, toda vez que en ese centro de operación pueden integrar a varios cliente y prestarle el servicio tal cual como lo promocionan en su sitio WEB, como se ilustra a continuación:



Para mejor proveer se anexa el vínculo donde se oferta el servicio al que se hace alusión. https://gmsseguridad.com/soluciones/soc/

AL HECHO 7. NO ES CIERTO. Como se expuso frente al hecho sexto (6) de la demanda el SOC no es una plataforma utilizada exclusivamente para el uso o prestación del servicio a SOTEMCOM SAS, sino que se oferta a todo cliente que así lo requiera.

Aunado a lo anterior, la empresa **GRUPO MICROSISTEMAS COLOMBIA S.A.S** nunca prestó los servicios, por lo que se pretende la demandante enriquecerse sin justa causa a costas de mi representada. Quiere decir lo anterior que no se le causó ningún perjuicio a la sociedad demandante, pues la plataforma por la cual aduce pagó no es de uso exclusivo de un solo cliente, pues **GRUPO MICROSISTEMAS COLOMBIA S.A.S** oferta los servicios a el público en general.

Nótese señor Juez que la apoderada judicial de **GRUPO MICROSISTEMAS COLOMBIA S.A.S** pretendió el cobro de una factura mediante un proceso ejecutivo, aduciendo la prestación del servicio y pretendiendo hacer exigible una obligación inexistente y luego pretende el resarcimiento de perjuicios que nunca se dieron.

AL HECHO 8. NO ME CONSTA MÁS ALLÁ DE LAS PRUEBAS DOCUMENTALES ALLEGADAS CON LA DEMANDA. No obstante, el pago referido no tiene razón de causalidad entre el perjuicio que pretende indilgar a mi representada, pues como se expuso en líneas anteriores, el SOC por el que presuntamente pagó la empresa GRUPO MICROSISTEMAS COLOMBIA S.A.S no es un servicio exclusivo ofertado a SOTELCOM SAS, pues es ofertado a todo tipo de cliente que pretenda la utilización de tal plataforma.

AL HECHO 9. NO EC CIERTO. el pago referido no tiene razón de causalidad entre el perjuicio que pretende indilgar a mi representada, pues como se expuso en líneas anteriores, el SOC por el que presuntamente pagó la empresa GRUPO MICROSISTEMAS COLOMBIA S.A.S no es un servicio exclusivo ofertado a SOTELCOM SAS, pues es ofertado a todo tipo de cliente que pretenda la utilización de tal plataforma.

AL HECHO 10. NO ES CIERTO. La sociedad demandante nunca prestó los servicios a SOTELCOM SAS, pues tan solo se llegó hasta la oferta de servicios y se remitió un documento al cliente final de SOLTEMCOM SAS con el alcance de la prestación del servicio que se pretendió contratar y ejecutar, pero que, por falta de información técnica del cliente final, nunca se logró iniciar.

AL HECHO 11. ES CIERTO LO REFERENTE AL LUGAR DEL CUMPLIMIENTO DE LA OBLIGACIÓN. Pero se itera, el servicio nunca se prestó, pues tan solo se llegó hasta la oferta de servicios y la elaboración del alcance de la oferta de servicios.

AL HECHO 12. NO ES CIERTO. FALTA TOTALMENTE A LA VERDAD LA APODERADA JUDICIAL DEL DEMANTE Y SE CONTRADICE. Toda vez que nunca se prestó el servicio y además pretende el resarcimiento de unos perjuicios por la compra de una plataforma (SOC) que nunca fue utilizada para la prestación de un servicio SOLTELCOM SAS, y es ofertada en su página web a todo público. En suma el SOC no es de uso exclusivo de un solo cliente.

AL HECHO 13. NO ES UN HECHO CORRESPONDE A FUNDAMENTOS DE DERECHO, POR LO QUE ME ABSTENGO DE REALIZAR PRONUNCIAMIENTO ALGUNO.

AL HECHO 14. NO ES CIERTO. A mi representada no le correspondía pagar por un servicio no prestado, a pesar de haberlo solicitado.

En punto de la licitación, se cae de su peso lo manifestado por GRUPO MICROSISTEMAS COLOMBIA S.A.S, toda vez que el contrato fue adjudicado con anterioridad a la fecha en que se solicitó el servicio a la demandante, pues así se observa en el mismo documento de adición suscrito entre la ALCALDIA DE CALI Y

SOLTELCOM SAS el día 13 de diciembre de 2019, el cual fue arrimado por la misma demandante.

Nótese señor Juez que, el contrato celebrado por la ALCALDIA DE CALI y SOTELCOM tiene como fecha de suscripción del 10 de octubre de 2019 y fecha de inicio 12 de noviembre de 2019, fechas previas a la orden de compra remitida por mi representada a GRUPO MICROSISTEMAS COLOMBIA S.A.S, por lo que no tiene nada que ver la oferta y la factura emitida por esta ultima para ganar la licitación del referido contrato en favor de SOLTELCOM S.A.S.

AL HECHO 15. NO ES CIERTO. El contrato nunca nació a la vida jurídica, pues es necesario la prestación del servicio, pues de no ser así cualquier persona o entidad que no haya prestado sus servicios ejecutaría una obligación de pago sin haber prestado un servicio, lo cual no es lógico frente a la ley.

Cabe señalar que, la factura que pretendió ser cobrada con posterioridad para el año 2021, a través de correo electrónico, nunca fue aceptada frente a la falta de prestación del servicio.

AL HECHO 16. NO ES CIERTO. Como se expuso frente al hecho catorce (14) el contrato celebrado por la ALCALDIA DE CALI y SOTELCOM tiene como fecha de suscripción del 10 de octubre de 2019 y fecha de inicio 12 de noviembre de 2019, fechas previas a la orden de compra remitida por mi representada a GRUPO MICROSISTEMAS COLOMBIA S.A.S, por lo que no tiene nada que ver la oferta y la factura emitida por esta última para ganar la licitación del referido contrato en favor de SOLTELCOM S.A.S. Tan solo existió una oferta de servicios y la remisión del alcance de los servicios que se pretendió ejecutar pero que nunca se prestaron por falta de documentos técnicos del cliente final de SOTELCOM S.A.S.

AL HECHO 17. NO ES CIERTO. Como se expuso frente al hecho catorce (14) y dieciséis (16), el contrato celebrado por la ALCALDIA DE CALI y SOTELCOM tiene como fecha de suscripción del 10 de octubre de 2019 y fecha de inicio 12 de noviembre de 2019, fechas previas a la orden de compra remitida por mi representada a GRUPO MICROSISTEMAS COLOMBIA S.A.S, por lo que no tiene nada que ver la oferta y la factura emitida por esta última para ganar la licitación del referido contrato en favor de SOLTELCOM S.A.S. Tan solo existió una oferta de servicios y la remisión del alcance de los servicios que se pretendió ejecutar pero que nunca se prestaron por falta de documentos técnicos del cliente final de SOTELCOM S.A.S.

AL HECHO 18. NO ES CIERTO. La modificación se realiza el 13 de diciembre con la adición del servicio prestado por SOTELCOM SAS y subcontratado a GSM ante el incidente de reportado en los servidores PJD y SAPRouter de la ALCALDIA DE CALI, cuyo servicio que fue cancelado por mi representada una vez culminada la prestación del servicio por valor de $4.025.000, a través de la factura de compra 2492 con fecha

de creación del 12 de diciembre de 2019 y fecha de vencimiento del 12 de enero de 2020, cuya transferencia se realizó el 17 de enero de 2020.

Dicha adición o modificación del contrato no tiene nada que ver con los servicios ofertados por GRUPO MICROSISTEMAS COLOMBIA S.A.S, dado que nunca se prestó dicho servicio.

AL HECHO 19. ES FALSO. Como se expuso frente al hecho catorce (14), dieciséis (16) y diecisiete (17), el contrato celebrado por la ALCALDIA DE CALI y SOTELCOM tiene como fecha de suscripción del 10 de octubre de 2019 y fecha de inicio 12 de noviembre de 2019, fechas previas a la orden de compra remitida por mi representada a GRUPO MICROSISTEMAS COLOMBIA S.A.S, por lo que no tiene nada que ver la oferta y la factura emitida por esta última para ganar la licitación del referido contrato en favor de SOLTELCOM S.A.S. Tan solo existió una oferta de servicios y la remisión del alcance de los servicios que se pretendió ejecutar pero que nunca se prestaron por falta de documentos técnicos del cliente final de SOTELCOM S.A.S.

AL HECHO 20. ES CIERTO. En el enlace se puede verificar la veracidad de la información suministrada por SOLTELCOM SAS, al igual que la fecha de adjudicación y suscripción del contrato, que nada tiene que ver con los servicios cobrados por GRUPO MICROSISTEMAS COLOMBIA S.A.S y que nunca fueron prestados.

AL HECHO 21. NO ES CIERTO Y SE CONTRADICE LA DEMANDANTE. Toda vez que pretende cobrar servicios que nunca prestó e indilgar una compra de una plataforma (SOC) que oferta para el publico en general y que no es de uso exclusivo de un solo cliente. De ahí que no existe nexo de causalidad del perjuicio que reclama, pues se trató de un servicio ofertado, pero nunca prestado.

AL HECHO 22. NO ES CIERTO. Mi representada no tenia obligación de pagar un servicio que nunca se prestó, pues nunca se pudo empezar a ejecutar por culpa del cliente final de SOTELCOM SAS.

En suma, el contrato celebrado por la ALCALDIA DE CALI y SOTELCOM tiene como fecha de suscripción del 10 de octubre de 2019 y fecha de inicio 12 de noviembre de 2019, fechas previas a la orden de compra remitida por mi representada a GRUPO MICROSISTEMAS COLOMBIA S.A.S, por lo que no tiene nada que ver la oferta y la factura emitida por esta última para ganar la licitación del referido contrato en favor de SOLTELCOM S.A.S. Tan solo existió una oferta de servicios y la remisión del alcance de los servicios que se pretendió ejecutar pero que nunca se prestaron por falta de documentos técnicos del cliente final de SOTELCOM S.A.S.

No puede pretender la demandante alegar la validez de un contrato de prestación de servicios, cuando jamás se ejecutó el objeto del contrato, de ahí que, no surja obligación de pagar en cabeza del contratante cuando no recibió el servicio

contratado, menos cuando es claro en el presente asunto, que la obligación no se hizo exigible en el entendido se no haber surgido una contraprestación de las partes, pues no hubo ejecución del servicio y por tanto no surge la obligación de pagar.

Ahora bien, no puede el demandante alegar un daño que nunca existió, pues los contratos de prestación de servicios por ser bilaterales, en efectos surgen obligaciones de reciprocidad, por lo cual se itera, nadie está obligado a pagar un servicio que nunca recibió. Por lo anterior, no le asiste razón al demandante, pues no puede aducir que el daño se genera por el incumplimiento de mi representada, cuando GRUPO MICROSISTEMAS COLOMBIA S.A.S nunca tuvo que cumplir con la obligación de prestar el servicio de ninguna manera, ante lo cual no puede validar el incumplimiento con su incumplimiento en la obligación de hacer.

AL HECHO 23. ES CIERTO

AL HECHO 24. ES CIERTO. Mi representada no asistió dado que no le asiste animo conciliatorio, en el entendido que, no adeuda suma alguna ni le causó un perjuicio a la demandante, pues se itera, la empresa GRUPO MICROSISTEMAS COLOMBIA S.A.S nunca prestó los servicios que pretende cobrar.

II. FRENTE A LAS PRETENSIONES

Me opongo a todas y cada una de las pretensiones, pues toda vez que mi representada jamás incumplió con ninguna obligación contractual, dado que la demandante pretende le pago de un servicio que nunca fue prestado y por tanto no surge la obligación de pagar. Más aun cuando la factura fue rechazada para su pago bajo dicho argumento, por lo que las pretensiones y condenas están llamadas al fracaso.

Con fundamento en lo anterior paso a referirme sobre todas y cada una de las pretensiones.

A LA PRETENSIÓN 1. ME OPONGO por cuanto no existió incumplimiento por parte de mi representada a ninguna obligación contractual, pues la demandante nunca prestó los servicios que pretende cobrar y menos causo un perjuicio económico a la empresa GRUPO MICROSISTEMAS COLOMBIA S.A.S.

A LA PRETENSIÓN 2. ME OPONGO por cuanto no existió incumplimiento por parte de mi representada a ninguna obligación contractual, pues la demandante nunca prestó los servicios que pretende cobrar y menos causo un perjuicio económico a la empresa GRUPO MICROSISTEMAS COLOMBIA S.A.S.

Quiere decir lo anterior que, no se configuró ningún daño en favor de la demandante, toda vez que el SOC que aduce tuvo que pagar no es de uso exclusivo de un solo cliente y el servicio se oferta y se mantiene para el publico en general.

A LA PRETENSIÓN 3. ME OPONGO por cuanto no existió incumplimiento por parte de mi representada a ninguna obligación contractual, pues la demandante nunca prestó los servicios que pretende cobrar y menos causo un perjuicio económico a la empresa GRUPO MICROSISTEMAS COLOMBIA S.A.S, por que deberá ser condena la demandante GRUPO MICROSISTEMAS COLOMBIA S.A.S. por haber sido vencida en juicio.

A LAS PRETENSIONES SUBSIDIARIAS 1, 2, 3 y 4 ME OPONGO en igual sentido, por cuanto no existió incumplimiento por parte de mi representada a ninguna obligación contractual, pues la demandante nunca prestó los servicios que pretende cobrar y menos causo un perjuicio económico a la empresa GRUPO MICROSISTEMAS COLOMBIA S.A.S, por que deberá ser condena la demandante GRUPO MICROSISTEMAS COLOMBIA S.A.S. por haber sido vencida en juicio.

III. EXCEPCIONES DE MÉRITO

- **INEXISTENCIA DE LA BOLIGACIÓN ANTE LA FALTA DE PRESTACIÓN DEL SERVICIO.**

  Solicito al señor Juez que declare en favor de mi representada la presente excepción, toda vez que la entidad demanda de manera confusa pretende el pago de un servicio que nunca prestó o ejecutó, al tiempo que la factura fue rechazada ante la falta de ejecución del servicio que se ofertó y solo llegó hasta la presentación del alcance del objeto del servicio.

- **COBRO DE LO NO DEBIDO**

  Solicito al señor Juez que declare en favor de mi representada la presente excepción, toda vez que la entidad demanda de manera pretende el pago de una factura que nunca se aceptó por la falta de prestación del servicio, por lo cual mi representada no adeuda suma alguna a la demandante GRUPO MICROSISTEMAS COLOMBIA S.A.S., ya que nunca surgió la obligación de pago.

- **LA INEXISTENCIA DE CAUSALIDAD DE LOS PERJUICIOS CAUSADOS.**

  Solicito al señor Juez declare en favor de mi representada como **EXCEPCIÓN LA INEXISTENCIA DE CAUSALIDAD DE LOS PERJUICIOS CAUSADOS,** toda

vez que el demandante pretende probar los daños causados soportado en el pago de una factura mediante la cual compró una plataforma que oferta al público en general y que puede ser utilizada para varios clientes, de manera que, no existe nexo de causalidad en el pago pretendido como perjuicio, pues claramente no se demuestra que la plataforma hay sido comprada para efectos de prestar el servicio única y exclusivamente al SOTELCOM S.A.S.

- **FALTA DE DEMOSTRACIÓN DE LOS PERJUICIOS SOLICITADOS**

- Solicito al señor Juez declare en favor de mi representada como **EXCEPCIÓN LA FALTA DE DEMOSTRACIÓN DE LOS PERJUICIOS SOLICITADOS,** dado que la demandante no cumplió con la carga de probar los perjuicios que se deprecan con la demanda, pues se limitó a exponer el pago de una factura que por si sola no demuestra la causación de un daño por el presunto incumplimiento de mi representada en el pago de la supuesta prestación del servicio, cuando por el contrario, mi representada si demuestra con los documentos adjuntos que la prestación del servicio nunca existió y que la empresa GRUPO MICROSISTEMAS COLOMBIA S.A.S pretende el pago de una plataforma que compró para la prestación del servicio ante SOLTELCOM S.A.S, pero la misma es ofertada y utilizada para otros clientes. De ahí que no se prueba con la sola compra de la plataforma el presunto perjuicio económico que de depreca con la demanda.

- **BUENA FE**

  Solicito al señor Juez declare en favor de mi representada la **EXCEPCIÓN DE BUENA FE,** toda vez que mi representada siempre actuó de buena fe frente a la demandada, tal es así que, el servicio que realmente prestó fue cancelado por mi representada. También es demostrativo la buena fe de SOTELCOM SAS el hecho de haber expuesto las razones del porque nunca se inició con la prestación del servicio, mismas que obedecían a la falta de documentos técnicos por parte del Cliente final de mi representada.

- **INEXISTENCIA DE PERJUCIOS POR USO Y GOCE DE PLATAFORMA SOC**

  Solicito al señor Juez declare en favor de mi representada la presente **EXCEPCIÓN,** toda vez que estamos ante la inexistencia de perjuicios materiales o por lo menos no se demostró en el presente asunto, que la compra de la plataforma SOC haya causado un perjuicio a la demandante y que la misma no haya sido utilizada para otros clientes u ofertado a otra empresa, o fuese de uso exclusivo para SOTELCOM SAS.

- **PRESCRIPCIÓN**

Sin que implique aceptación o reconocimiento alguno de nuestra parte respecto de los hechos y pretensiones que se deprecan con la demanda, solicito al señor Juez se sirva reconocer y decretar, en favor de la SOTELCOM SAS., la **EXCEPCIÓN DE PRESCRIPCIÓN,** de todas y cada una de las pretensiones y condenas incoadas con la demanda, toda vez que, con el paso del tiempo y la inactividad de parte activa, se configuró el fenómeno extintivo de la prescripción, lo cual hace que sea legalmente inviable la exigencia de las condenas que aquí se reclaman, a la luz de lo dispuesto en el artículo 2512 y 2535 y ss.

- **LAS INNOMINADA O GENÉRICA**

Solicito al Señor Juez se sirva reconocer oficiosamente en favor de SOTELCOM SAS, cualquier excepción de mérito que se resulte probada dentro del proceso.

IV. FUNDAMENTOS DE DERECHO

SON FUNDAMENTOS DE LA CONTESTACIÓN DE LA DEMANDA LOS SIGUEINTES:

- LA LEY 2213 DE 2022 QUE DECLARO PERMANENTE EL DECRETO 806 DE 2020.
- EL ARTICULO 96 DEL CODIGO GENRAL DEL PROCESO QUE TRATA SOBRE LA FORMA Y REQUISITOS DE LA CONTESTACION DE LA DEMANDA.
- EL ARTICULO 1546 DEL CÓDIGO CIVIL
- EL ARTICULO 374 DEL CÓDIGO GENERAL DEL PROCESO
- LOS ARTÍCULOS 2512 y 2535 Y S.S. DEL CÓDIGO CIVIL
- EL ARTÍCULO 1915 Y S.S. DEL CODIGO CIVIL

VI. PRUEBAS

DOCUMENTALES

- Copia de la oferta de servicios realizada por GRUPO MICROSISTEMAS COLOMBIA S.A.S
- Copia de la carta de rechazo de la factura remitida al GRUPO MICROSISTEMAS COLOMBIA S.A.S
- Copia de los correos cruzados entre la demandante y SOLTELCOM SAS en la cual se evidencia la aceptación en la falta de prestación del servicio.
- Copia de la factura cancelada al GRUPO MICROSISTEMAS COLOMBIA S.A.S por la prestación del servicio ante el incidente presentado por la ALCALDIA DE CALI.
- Copia del informe presentado por GRUPO MICROSISTEMAS COLOMBIA S.A.S por la prestación del servicio.
- Copia del comprobante de pago de la factura.

- Copia del comprobante de egreso por el pago de los servicios a GRUPO MICROSISTEMAS COLOMBIA S.A.S
- Documento con la definición del SOC y enlace para acceder a la página de GRUPO MICROSISTEMAS COLOMBIA S.A.S.

INTERROGATORIO DE PARTE

De manera comedida y respetuosa solicito al señor Juez se cite al demandante y se fije fecha y hora, para que concurra al despacho a fin de que en audiencia pública absuelvan el interrogatorio que le formularé de manera verbal o en sobre sellado.

TESTIMONIALES:

Para que declaren sobre los hechos que obran en la presente demanda, solicito comedidamente se cite a las siguientes personas:

Al señor **JUAN FELIPE MORA MOSTACILLA**, quien funge como **GERENTE TÉCNICO** de la empresa SOTELCOM SAS, quien podrá ubicado en Avenida 5an # 23dn - 68. Oficina 322 y 323 del Centro Comercial Pasarela. Cali; en la dirección electrónica: juan.mora@sotelcom.co

Al señor **CRISTIAN CAICEDO DUARTE**, quien labora para SOTELCOM y fue el encargado del proyecto, quien podrá ubicado en la calle 61 Norte No,3AN-80 en Cali; Dirección electrónica: cristian.caicedo@sotelcom.co.

OPOSICION A LAS PRUEBAD DE OFICIO POR IMPROCEDENTES.

Señor Juez solicito de manera respetuosa se denieguen las pruebas solicitadas de oficio, toda vez que, en los procesos de naturaleza civil, las partes acuden a confirmar, y no averiguar, sus aseveraciones, por lo tanto, el derecho a probar se lleva a efecto conforme a los parámetros que reflejan los principios de libertad y de apreciación probatoria.

Quiere decir entonces que, a modo de regla general cualquiera de los medios de convicción enlistados en el artículo 165 del estatuto procesal, entre otros, sirven para ese fin, salvo que la ley diga lo contrario y que, allegado al proceso el elemento suasorio, este debe ser apreciado de manera crítica, razonada, individual y en conjunto por el sentenciador, de suerte que, las partes tienen la libertad para acreditar los hechos debatidos a través de los diferentes canales que lleven a convencimiento al Juzgador acerca de las situaciones fácticas en disputa.

En tal sentido, se advierte improcedente la solicitud de decreto de oficio de las pruebas solicitadas de oficio por la apoderada de la demandante, por cuanto, el artículo 167

del C.G.P., prevé que "Incumbe a las partes probar el supuesto de hecho de las normas que consagran el efecto jurídico que ellas persiguen."

Por su parte el artículo 173 del mismo código señala sobre las OPORTUNIDADES PROBATORIAS lo siguiente:

> *"Para que sean apreciadas por el juez las pruebas deberán solicitarse, practicarse e incorporarse al proceso dentro de los términos y oportunidades señalados para ello en este código.*
>
> *En la providencia que resuelva sobre las solicitudes de pruebas formuladas por las partes, el juez deberá pronunciarse expresamente sobre la admisión de los documentos y demás pruebas que estas hayan aportado.* ***El juez se abstendrá de ordenar la práctica de las pruebas que, directamente o por medio de derecho de petición, hubiera podido conseguir la parte que las solicite, salvo cuando la petición no hubiese sido atendida, lo que deberá acreditarse sumariamente."***
>
> (Negrillas y cursivas nuestras)

Por lo anterior, la parte demandante es quien debió allegar los documentos solicitados de oficio o al menos haber demostrado que las solicitó directamente o a través de derecho de petición, pero no dejar a discreción del Juez la carga de la prueba, pues, es la parte interesada quien se debe mostrar su interés por llegar al convencimiento al Sentenciador y no como se pretende en esta oportunidad.

VII. NOTIFICACIONES

AL DEMANDANTE en las direcciones indicadas en la demanda.

A LA DEMANDADA SOTELCOM SAS Avenida 5an # 23dn - 68. Oficina 322 y 323 del Centro Comercial Pasarela. Cali; correo electrónico: info@sotelcom.com; Teléfono: 5246043

A LA SUSCRITA en la carrera 75 No.13-196 apto 301 en Cali-Valle; Correo electrónico: c.garrotejuridica@gmail.com y notificacionabogadoscg@gmail.com; Celular: 310-4186306 – 316-8297294

Cordialmente,

CAROLINA GARROTE MICOLTA
C.C. No.1.130.664.298
T.P No.197.771 del CS de la J.

Gmail

Jovanni Valencia Zuloaga <jovanni.juridico2@gmail.com>

Fwd: PODER CONTESTACIÓN SOTELCOM

1 mensaje

Carolina Garrote <c.garrotejuridica@gmail.com> 25 de abril de 2023, 16:18
Para: Jovanni Valencia Zuloaga <jovanni.juridico2@gmail.com>

Enviado desde mi iPhone

Inicio del mensaje reenviado:

De: "Ing. Luis F Pabon T" <luis.pabon@sotelcom.co>
Fecha: 25 de abril de 2023, 3:18:54 p.m. COT
Para: Carolina Garrote <c.garrotejuridica@gmail.com>
Asunto: Rv: PODER CONTESTACIÓN SOTELCOM

Dra Carolina buenas tardes,

Adjunto poder para su gestión.

Gracias,
Luis Fernando Pabón Tovar
<PODER CONTESTACIÓN GSM.pdf>

Señor
JUEZ OCHENTA Y DOS (82) CIVIL MUNICIPAL TRANSITORIAMENTE JUZGADO SESENTA Y CUATRO (64) DE PEQUEÑAS CAUSAS Y COMPETENCIA MULTIPLE DE BOGOTÁ
E.S.D

PROCESO : PROCESO VERBAL – RESPONSABILDIAD CIVIL
DEMANDANTE : GRUPO MICROSISTEMAS COLOMBIA S.A.S.
DEMANDADO : SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S. "SOTELCOM SAS".
RADICACIÓN : 110014003082-2022-00841-00

ASUNTO : PODER ESPECIAL

LUIS FERNANDO PABON TOVAR, mayor de edad, vecina y residente de Cali, identificada con la cédula de ciudadanía No.6.390.188, Representante Legal de la sociedad demandada **SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO S.A.S. "SOTELCOM SAS"**, identificada con el NIT.900.368.512-4, manifiesto al señor juez que confiero **PODER ESPECIAL**, amplio y suficiente a la Doctora **CAROLINA GARROTE MICOLTA,** igualmente mayor de edad, identificada con la cédula de ciudadanía 1.130.664.298, abogada en ejercicio, portadora de la Tarjeta Profesional No.197.771 del Consejo Superior de la Judicatura, para actúe como judicial dentro del proceso de la referencia y represente los intereses de la empresa **SOTELCOM S.A.S.**

Mi apoderada queda investida de las facultades contenidas en el artículo 77 de Código General del Proceso y en especial queda autorizado para notificarse, desistir, transigir, recibir, recurrir, sustituir y reasumir este poder, proponer toda clase de incidentes, tachas, excepciones, llamamientos en garantía y denuncios del pleito y en general para realizar todas las actividades judiciales propias del mandato que se le confiere.

El presente poder de confiere a través de mensaje de datos a la dirección electrónicas de la apoderada c.garrotejuridica@gmail.com

Atentamente,

LUIS FERNANDO PABON TOVAR
Representante Legal
SOTELCOM S.A.S,

Acepto,

CAROLINA GARROTE MICOLTA
C.C No. 1.130.664.298 de Cali
T.P. No.197.771 del CS de la J.

Juan Felipe Mora Mostacilla

De: Juan Felipe Mora Mostacilla <juan.mora@sotelcom.co>
Enviado el: martes, 28 de marzo de 2023 12:19 p. m.
Para: Carolina Garrote
Asunto: RV: Solicitud cotización servicios
Datos adjuntos: Alcance [Protección de marca][Alcaldia de Cali][2019].pdf; Alcance [Ethical Hacking] [Alcaldia de Cali][2019].pdf

Esta fue la propuesta de lo que están cobrando y las actividades que nunca se realizaron.

Saludos.

sotelcom
tecnología que impulsa

Juan Felipe Mora Mostacilla
Gerente Tecnico
CCSE # CP0000101034

www.sotelcom.co · info@sotelcom.co
Avenida 5an # 23dn - 68. Oficina 322 y 323.
Centro Comercial Pasarela. Cali, Colombia.

Correo: juan.mora@sotelcom.co
PBX: (2) 524 6043 Ext.: 105
Móvil: 3185327566

De: Cristian Caicedo <cristian.caicedo@sotelcom.co>
Enviado el: martes, 28 de marzo de 2023 12:16 p. m.
Para: Juan Felipe Mora Mostacilla <juan.mora@sotelcom.co>
Asunto: RV: Solicitud cotización servicios

psi

De: María Sandra Galvez <mariasandra.galvez@gmsseguridad.com>
Enviado el: jueves, 14 de noviembre de 2019 4:20 p. m.
Para: Cristian Caicedo <cristian.caicedo@sotelcom.co>; Adrian Calvopiña <adrian.calvopina@gmsseguridad.com>; Ana Betancourt <ana.betancourt@gmsseguridad.com>
Asunto: Fwd: Solicitud cotización servicios

Buenos tardes Cristian Caicedo:

Dando alcance al compromiso generado en nuestra reunion del dia viernes y el avance con el ingeniero Adrian Calvopiña, adjunto precios especiales para Sotelcom.

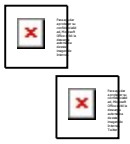
A su vez adjuntamos el alcance de cada solucion

Precios no incluyen IVA

Item	Producto	Descripción
1	INVESTIGACION	Protección de marca x 1 año (5 palabras clave + informe mensual)
2	CONSULTORIA	Ethical Hacking (Test y Retest)
		Total en US
		Servicios adicionales bajo demanda
3	INVESTIGACION	Dar de baja x demanda un (1) sitio (Cada sitio tiene costo adicional)
4	INVESTIGACION	Investigacion x demanda CSIRT (costo por hora)

Cordialmente;

María Sandra Galvez
Gerente de Cuenta
mariasandra.galvez@gmsseguridad.com
Oficina: +57 17433559 Ext. 8041
Cel: +57 313 764 6126
Dir:
www.gmsseguridad.com



Juan Felipe Mora Mostacilla

De: Adrian Calvopiña <adrian.calvopina@gmsseguridad.com>
Enviado el: jueves, 13 de febrero de 2020 1:04 p. m.
Para: Juan Felipe Mora Mostacilla
CC: Cristian Caicedo; María Sandra Galvez; Ana Betancourt
Asunto: Re: Alcance Técnico - Protección de Marca y EH - Alcaldía de Cali

Sres. espero que les haya ido muy bien en EEUU...

Estoy pendiente de sus comentarios con el fin de avanzar con el tema.

Atento a sus comentarios

Slds

Adrian Calvopiña Mancheno
Ingeniero Preventa
adrian.calvopina@gmsseguridad.com
Oficina:
Cel: +57 3008542347
www.gmsseguridad.com

El jue., 23 ene. 2020 a las 15:38, Adrian Calvopiña (<adrian.calvopina@gmsseguridad.com>) escribió:

Juan / Cristian

Por favor su ayuda con los detalles que faltan en función del levantamiento de información para iniciar con el servicio de protección de marca, además su amable confirmación sobre la finalización de implementación del Firewall Checkpoint para coordinar las actividades de Ethical Hacking respectivas.

Slds

Adrian Calvopiña Mancheno
Ingeniero Preventa
adrian.calvopina@gmsseguridad.com
Oficina:
Cel: +57 3008542347
www.gmsseguridad.com

Remitente notificado con
Mailtrack

El mar., 14 ene. 2020 a las 13:59, Adrian Calvopiña (<adrian.calvopina@gmsseguridad.com>) escribió:

Buena tarde

Juan / Cristian

Les deseo un excelente año, éxitos en todo lo que emprendan en este 2020

Estoy atento a los detalles faltantes para iniciar la ejecución del servicio de protección de marca.

Atento a sus comentarios

Slds

Adrian Calvopiña Mancheno
Ingeniero Preventa
adrian.calvopina@gmsseguridad.com
Oficina:
Cel: +57 3008542347
www.gmsseguridad.com

Remitente notificado con
Mailtrack

El mié., 11 dic. 2019 a las 12:04, Adrian Calvopiña (<adrian.calvopina@gmsseguridad.com>) escribió:

ok, quedo pendiente.

Slds

Adrian Calvopiña Mancheno
Ingeniero Preventa
adrian.calvopina@gmsseguridad.com
Oficina:
Cel: +57 3008542347
Dir: Transversal 22 # 98 - 82 / 26 OF 303 Edificio PORTA 100, Bogotá
www.gmsseguridad.com

Remitente notificado con Mailtrack

El mié., 11 dic. 2019 a las 11:29, Juan Felipe Mora Mostacilla (<juan.mora@sotelcom.co>) escribió:

Adrian buen día el Ingeneiro de la alcaldía está en una capacitación, por tal motivo no me ha enviado la información, la idea que está me la suministre a más tardar el viernes

Obtener Outlook para iOS

De: Adrian Calvopiña <adrian.calvopina@gmsseguridad.com>
Enviado: Wednesday, December 11, 2019 10:28:04 AM
Para: Juan Felipe Mora Mostacilla <juan.mora@sotelcom.co>; Cristian Caicedo <cristian.caicedo@sotelcom.co>; María Sandra Galvez <mariasandra.galvez@gmsseguridad.com>; Ana Betancourt <ana.betancourt@gmsseguridad.com>
Asunto: Re: Alcance Técnico - Protección de Marca y EH - Alcaldía de Cali

Juan / Cristian

Buen dia,

Me encuentro a la espera de los datos faltantes para arrancar con la ejecución de protección de marca.

Slds

Adrian Calvopiña Mancheno
Ingeniero Preventa
adrian.calvopina@gmsseguridad.com
Oficina:
Cel: +57 3008542347
Dir: Transversal 22 # 98 - 82 / 26 OF 303 Edificio PORTA 100, Bogotá
www.gmsseguridad.com

Remitente notificado con Mailtrack

El mié., 4 dic. 2019 a las 10:32, Adrian Calvopiña (<adrian.calvopina@gmsseguridad.com>) escribió:

Buen dia

Juan / Cristian

Como lo hablamos en la reunión de esta mañana, adjunto los formularios que diligenciamos en conjunto, sobre la información faltante quedo a la espera de tu retroalimentación previa validación con el cliente.

Una vez me envies esa información faltante coordinaremos el proceso internamente para que en 5 días hábiles el proceso de Protección de Marca arranque.

Sobre el EH a los 2 Firewalls HA (Checkpoint 16000) es necesario que ustedes nos notifiquen con 15 días de anterioridad tras haber implementado los Checkpoint en Alcaldía de Cali de forma satisfactoria para coordinar la disponibilidad de nuestro consultor a cargo. (agenda tentativa para la segunda semana de enero).

Sobre el tema de los viáticos y logística del consultor tanto para el test y retest (después de 3 meses) @Cristian Caicedo estamos atentos a tus comentarios para coordinar el tema.

Slds

Adrian Calvopiña Mancheno
Ingeniero Preventa
adrian.calvopina@gmsseguridad.com
Oficina:
Cel: +57 3008542347
Dir: Transversal 22 # 98 - 82 / 26 OF 303 Edificio PORTA 100, Bogotá
www.gmsseguridad.com

Juan Felipe Mora Mostacilla

De: Juan Felipe Mora Mostacilla <juan.mora@sotelcom.co>
Enviado el: martes, 28 de marzo de 2023 12:33 p. m.
Para: Carolina Garrote
Asunto: RV: Cotizacion Servicios Atencion y respuesta a incidentes
Datos adjuntos: Propuesta GMS - [Atencion y respuesta a incidentes][Alcaldia de Cali][2019].pdf

PSI

sotelcom
tecnología que impulsa
www.sotelcom.co · info@sotelcom.co
Avenida 5an # 23dn - 68. Oficina 322 y 323.
Centro Comercial Pasarela. Cali, Colombia.

Juan Felipe Mora Mostacilla
Gerente Tecnico
CCSE # CP0000101034
Correo: juan.mora@sotelcom.co
PBX: (2) 524 6043 Ext.: 105
Móvil: 3185327566

De: Cristian Caicedo <cristian.caicedo@sotelcom.co>
Enviado el: martes, 28 de marzo de 2023 12:23 p. m.
Para: Juan Felipe Mora Mostacilla <juan.mora@sotelcom.co>
Asunto: RV: Cotizacion Servicios Atencion y respuesta a incidentes

Psi
Propuesta que le pagamos

De: Cristian Caicedo
Enviado el: miércoles, 11 de diciembre de 2019 3:53 p. m.
Para: María Sandra Galvez <mariasandra.galvez@gmsseguridad.com>
CC: Adrian Calvopiña <adrian.calvopina@gmsseguridad.com>; Ana Betancourt <ana.betancourt@gmsseguridad.com>; Juan Felipe Mora Mostacilla <juan.mora@sotelcom.co>
Asunto: RV: Cotizacion Servicios Atencion y respuesta a incidentes

Sandra
Cordial Saludo

Ya la alcaldía nos confirmó la actividad por tal razón te confirmo la aceptación de la propuesta adjunta.

Mañana en la mañana te estamos enviando la orden, porfa para agilizar ayúdame cuadrando una reunión de inicio que pidió Roger para mañana en la mañana a las 8:00 am.

Para que estén ustedes y nuestro ingeniero juan Felipe que va estar al tanto del tema.

Gracias.

De: María Sandra Galvez <mariasandra.galvez@gmsseguridad.com>
Enviado el: martes, 10 de diciembre de 2019 6:36 p. m.
Para: Cristian Caicedo <cristian.caicedo@sotelcom.co>; Ana Betancourt <ana.betancourt@gmsseguridad.com>
Asunto: Cotizacion Servicios Atencion y respuesta a incidentes

Buenas Cristian:

Con base al alcance técnico realizado el dia de hoy con la Alcaldia Santiago de Cali, adjuntamos oferta del servicio remoto de 20 horas .

Quedamos atentas a tus inquietudes y pasos a seguir

Gracias por contar con nosotros!

Cordialmente,

María Sandra Gálvez
Gerente de Cuenta
mariasandra.galvez@gmsseguridad.com
Oficina: +57 17433559 Ext. 8041
Cel: +57 3058573929
Dir:
www.gmsseguridad.com

Propuesta de Servicios de Atención y respuesta a incidentes

Preparada para:

Alcaldía de Cali

Diciembre 2019

AGRADECIMIENTO

Cali, 10 de diciembre del 2019

Alcaldia de Cali

Estimados Ingenieros,

GMS agradece la oportunidad de presentarle esta oferta de soluciones informáticas. Somos una empresa de Seguridad de la Información con más de 39 años de experiencia, durante los cuales hemos podido atender a muchas de las compañías más importantes de la región. Nuestras soluciones cubren las más altas exigencias de nuestros clientes, y nos caracterizamos por cumplir proyectos de alta complejidad. Asumimos el papel de socio estratégico para establecer relaciones exitosas a largo plazo.

Esperamos que esta propuesta sea de su conveniencia y quedo a su disposición para atender cualquier inquietud o comentario que pudiera surgir respecto a la misma.

Atentamente,

María Sandra Galvez
Gerente de Cuenta
mariasandra.galvez@gmsseguridad.com
Oficina: +57 17433559 Ext. 8041
Cel: +57 3058573929
www.gmsseguridad.com

I. Introducción

Descripción.

GMS Seguridad de la Información, ofrece el servicio de Atención y respuesta a incidentes, el cual es un servicio proporcionado por **GMS** conformado por personal especializado en **Seguridad TI**.

Características del servicio.

- Personal especializado en seguridad informática e investigación.
- Difusión de la información detallada del incidente.

Objetivos

Objetivo general

- Obtener visibilidad de potenciales riesgos a la seguridad de información de la empresa, mediante el análisis forense.
- Brindar capacidad de respuesta frente a incidentes de seguridad, recomendaciones y pasos a seguir para contención de eventos de seguridad informática, mitigación de riesgos asociados y apoyo en la recuperación frente a un ataque exitoso.

Objetivos Específicos

- Ejecutar actividades especializadas de evaluación de incidente de seguridad informática, analizar los indicadores de compromiso y coordinar con el cliente las actividades de contención, mitigación y recuperación del evento.

II. Alcance

El servicio de atención y respuesta a incidentes está enfocado a investigar:

- Evento reportado sobre el acceso no autorizado a la plataforma de SAP.
- 20 horas para respuesta a incidentes (remoto)

Para el servicio de respuesta a incidentes, dependiendo del evento o criticidad, se podrá realizar de manera remota o presencial y se deberá prestar todas las facilidades y accesos requeridos.

Los gastos de movilización, alimentación, y alojamiento van por cuenta del cliente en caso de que los servicios se deban realizar fuera de Bogotá.

ENTREGABLES:

- Informe de análisis de incidente.

III. Descripción del servicio

Identificación:

- Identificar la estructura de red del objetivo atacado.
  - Activos asociados, Hardware y Software.
  - Activos que puedan contener evidencia.
  - Establecer mecanismos para preservar evidencia

Investigación:

- Se emplearán herramientas de escaneo, análisis, investigación, indexación y de penetración.
- Preservar información encontrada que puede aportar datos relevantes
- Analizar de eventos o logs, rastreo.
- Recoger los datos en su formato nativo, firma digitalmente y marca con tiempo los datos.
- Se almacena de forma segura el registro sin formato, preservando la integridad de los datos.
- Pruebas de vulnerabilidades
- Análisis de IoCs, Uso de la metodología Threat Hunting (figura 3).
- Determinar los equipos comprometidos y trazar una cuarentena, aplicar YARA.
- Determinar tipo de ataque.
- Determinar vectores de infección utilizados.
- Determinar malware reconocido y no reconocido por sus herramientas de seguridad endpoint.

Resultados:

- Entrega de datos recopilados en formato informe de recomendaciones para que un incidente parecido no pueda repetirse.
- Entregar tareas específicas de remediación al personal de TI
- Entregar recomendaciones de endurecimiento de políticas de antivirus y firewall.
- Entrega de informe final.
- Planteamiento de recomendaciones y medidas preventivas.

METODOLOGÍA DE INVESTIGACIÓN

El servicio de respuesta a incidentes se basa en los estándares de la industria, con personal capacitado y especializado, certificado sen CISSP, CEH, GCFA, Security+ y entre otros conocimientos transmitidos de fabricantes especialista y reconocidos a nivel mundial.

Figura 3. Metodología Threat Hunting y seguridad accionable. – fuente: Kaspersky Lab.

Es importante recalcar que para el éxito de una investigación (encontrar indicios y/o responsables) es necesario cumplir con las siguientes condiciones:

- Tiempo transcurrido posterior al evento, bajo.
- Apoyo de la dirección.
- Conservación de los logs.
- Identificación e individualización de los usuarios.

Factores clave de éxito

Adicional a los hitos identificados y cumplimiento del alcance, en nuestra experiencia, podemos mencionar que el éxito del proyecto y la satisfacción de nuestros anteriores clientes, depende de:

- El nivel de compromiso y autoridad del responsable del proyecto por parte de la organización y alguien alterno en su ausencia
- Coordinación interna adecuada
- Entrega oportuna de información
- Comunicación oportuna y fluida en cualquier aspecto que se aleje de lo planificado
- Flexibilidad en el manejo de imprevistos y situaciones no contempladas en el alcance
- Informe inmediato en caso de evidenciar escenarios de alto riesgo

Hitos Importantes

Para realizar este análisis se debe, de común acuerdo, tener en consideración los siguientes pasos relevantes:

- Firma del acuerdo de confidencialidad entre las partes.
- Presentación de reportes (según lo acordado)

Condiciones de trabajo

- El cliente debe proporcionar un área específica para la ejecución de las actividades si se llevan a cabo presencialmente.
- El cliente será el encargado de coordinar al interior de la organización el calendario presentado para la ejecución de las actividades.
- En caso de que alguna actividad se realice de manera remota y se deberá prestar todas las facilidades y accesos requeridos.

IV. Información Adicional

Fortalezas del equipo de trabajo

Contamos con personal certificado y altamente experimentado en seguridad informática. Nuestro personal cuenta con las siguientes certificaciones:

- Master en Seguridad de Tecnología de Información y Comunicaciones
- Especialización en Seguridad en Bases de Datos y Aplicaciones
- Ec – Council Ethical Hacking and Countermeasures
- CISSP Certified Information Systems Security Professional.
- ATM Security Training
- Diplomado en Gobierno de TI, Auditoría y Seguridad de los Sistemas de Información
- Formación de Auditor Interno ISO27001
- ISACA CISM Certified Information Security Manager
- ISACA Certified Member
- CEH – Certified Ethical Hacker.
- Certified Forensics Analyst
- CompTIA Security Certified Professional
- ITIL Foundation
- COBIT5 Foundation
- AlienVault USM Security Engineer
- Enterprise Incident Response
- Qualys Certified Specialist
- Kaspersky Accredited Technical Specialist
- Dirección Profesional de Proyectos
- Auditor Líder ISO27001

V. Experiencia

Nuestro equipo está conformado por personas con la mayor experiencia en seguridad informática, con más de 40 años en Latinoamérica, GMS ha estado involucrado directa e indirectamente (subcontratado) en un sinnúmero de implementaciones y evaluaciones estratégicas de Seguridad de Información.

Cuadro de algunos clientes y servicios realizados:

CLIENTE	SERVICIO	AÑO
Banco General Rumiñahui	Ethical Hacking	2017
Banco Amazonas	Ethical Hacking	2016 2015
Cooperativa 15 de abril	Evaluación de Nivel de Madurez en Seguridad de Información. Vulnerability Assessment	2017
CONECEL - CLARO	Ethical Hacking	2016 2017 2018
Red Transaccional de Cooperativas COONECTA	SOC	2017
Metro de Medellín	SOC Servicios administrados de sistemas de seguridad perimetral	2018 2019
Banco Comercial de Manabí	Ethical Hacking.	2016 2018
DATAFAST	SOC, Hardening Management Ingeniería Social	2017
Difare	Cybersecurity Maturity Assessment Ethical Hacking	2014 2018
Banco Pichincha	Security APT Monitoring	2015
Banco Internacional	Risk Assesment y Clasificación de Información	2017
Banco Finca	Ethical Hacking Ingeniería Social	2018
Banco Procredit	Ethical Hacking Ingeniería Social SOC	2018
Cobrando BPO	SOC Atención y Respuesta a incidentes	2019
Hyundai Colombia	Ingeniería Social	2019
Credifinanciera	SOC Protección de Marca SGSI	2019
Credifamilia	SOC	2019
Heinsohn	Gap Análisis 27001:2013 Consultoría Circular 007 Risk Assesment Vulnerability Assessment Etichal Hacking Hardening	2018 2019

VI. Propuesta Económica

ITEM	DESCRIPCIÓN	Eventos	PRECIO (COP)
1	**RESPUESTA A INCIDENTES** 20 horas para atención y respuesta a incidente (remoto)	1	3´500 000
		SUBTOTAL	**$ 3´500 000**

Condiciones Generales

- Los valores antes indicados están en pesos colombianos.
- Los valores antes indicados no incluyen el IVA.
- Forma de pago: 30 días posterior a la radicación de la factura.
- Validez de la oferta: 15 días
- Tiempo de entrega: 2 días laborables a la confirmación de compra.

*******0,00

GRUPO MICROSISTEMAS COLOMBIA SAS

CERO PESOS CON 00/100 M/L

SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO SAS - PRINCIPAL N.I.T: 900.368.512-4		COMPROBANTE DE EGRESO N°	0000009024
		PAGO A PROVEEDOR N°	0000005695
FECHA	20 ENE. 2020	CHEQUE	0
PAGADO A	GRUPO MICROSISTEMAS COLOMBIA SAS	TRANSFERENCIA	4.025.000
CC ó NIT	900.418.656 - 1	TOTAL	$4.025.000

SON: CUATRO MILLONES VEINTICINCO MIL PESOS CON 00/100 M/L

OBSERVACIONES PAGO FACTURA 2492

CHEQUE/DOC N

CTA SUB AUX	DOCUMENTO	TERCERO	%	DEBITO	CREDITO
1110 05 005	9024	BANCOLOMBIA - CORRIENTE - 38112825035	0,00	0	4.025.000
2205 05 005	0000002492	GRUPO MICROSISTEMAS COLOMBIA SAS	0,00	4.025.000	0

Elaborado Por	Autorizado por	Revisado Por	Recibido
AUX MIREYA VALENCIA			Firma y Sello- CC ó NIT:

*******0,00

GRUPO MICROSISTEMAS COLOMBIA SAS

CERO PESOS CON 00/100 M/L

SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO SAS - PRINCIPAL		**COMPROBANTE DE EGRESO N°**	**0000009024**
N.I.T: 900.368.512-4		**PAGO A PROVEEDOR N°**	**0000005695**
FECHA	20 ENE. 2020	**CHEQUE**	0
PAGADO A	GRUPO MICROSISTEMAS COLOMBIA SAS	**TRANSFERENCIA**	4.025.000
CC ó NIT	900.418.656 - 1	**TOTAL**	$4.025.000

SON: CUATRO MILLONES VEINTICINCO MIL PESOS CON 00/100 M/L

OBSERVACIONES PAGO FACTURA 2492

CHEQUE/DOC N

CTA SUB AUX	DOCUMENTO	TERCERO	%	DEBITO	CREDITO
1110 05 005	9024	BANCOLOMBIA - CORRIENTE - 38112825035	0,00	0	4.025.000
2205 05 005	0000002492	GRUPO MICROSISTEMAS COLOMBIA SAS	0,00	4.025.000	0

Elaborado Por	Autorizado por	Revisado Por	Recibido
ALIX MIREYA VALENCIA			Firma y Sello- CC ó NIT:

GRUPO MICROSISTEMAS COLOMBIA SAS

CERO PESOS CON 00/100 M/L ------0.00

SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO SAS - PRINCIPAL N.I.T: 900.368.512-4		COMPROBANTE DE EGRESO N°	0000009024
FECHA	20 ENE. 2020	PAGO A PROVEEDOR N°	0000005895
PAGADO A CC ó NIT	GRUPO MICROSISTEMAS COLOMBIA SAS 900.418.656 - 1	CHEQUE TRANSFERENCIA	0
SON: CUATRO MILLONES VEINTICINCO MIL PESOS CON 00/100 M/L		TOTAL	4.025.000 $4.025.000
OBSERVACIONES PAGO FACTURA 2492			
CHEQUE/DOC N			

CTA SUB AUX	DOCUMENTO	TERCERO	%	DEBITO	CREDITO
1110	9024	BANCOLOMBIA - CORRIENTE - 38112625035	0.00	0	4.025.000
2205 05 005	0000002492	GRUPO MICROSISTEMAS COLOMBIA SAS	0.00	4.025.000	0

Elaborado Por	Autorizado por	Revisado Por	Recibido
ALBA MARIA VALENCIA			Firma y Sello- CC ó NIT:

*******0,00

GRUPO MICROSISTEMAS COLOMBIA SAS

CERO PESOS CON 00/100 M/L

SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO SAS - PRINCIPAL		**COMPROBANTE DE EGRESO N°**	**0000009024**
N.I.T: 900.368.512-4		**PAGO A PROVEEDOR N°**	**0000005695**
FECHA	20 ENE. 2020	**CHEQUE**	0
PAGADO A	GRUPO MICROSISTEMAS COLOMBIA SAS	**TRANSFERENCIA**	4.025.000
CC ó NIT	900.418.656 - 1	**TOTAL**	$4.025.000

SON: CUATRO MILLONES VEINTICINCO MIL PESOS CON 00/100 M/L

OBSERVACIONES PAGO FACTURA 2492

CHEQUE/DOC N

CTA SUB AUX	DOCUMENTO	TERCERO	%	DEBITO	CREDITO
1110 [illegible]	9024	BANCOLOMBIA - CORRIENTE - 38112825035	0,00	0	4.025.000
2205 05 005	0000002492	GRUPO MICROSISTEMAS COLOMBIA SAS	0,00	4.025.000	0

Elaborado Por	Autorizado por	Revisado Por	Recibido
ALIX MIREYA VALENCIA			Firma y Sello- CC ó NIT:

gms

seguridad de la información

Factura de Venta

2492

GRUPO MICROSISTEMAS COLOMBIA S.A.S.

NIT: 900.418.656-1 - RÉGIMEN COMÚN
Resolución DIAN: 18762011763060
del 2018/12/12 - Habilita 2001 - 3000
Actividad Económica 6202 y Tarifa 6,9 x 1000
NO SOMOS GRANDES CONTRIBUYENTES, NI AUTORRETENEDORES
NI AGENTES RETENEDORES DE IVA

Cliente: SOTELCOM (SOLUCIONES DE TELECOMUNICACIONES Y COMPUTO SAS Cod
Nit/CC: 900.368.512-4
Dirección: AVENIDA 5A # 23D DN - 68
Teléfono: 5246043 Ciudad: SANTIAGO DE
Fecha Factura: 12 DICIEMBRE DE 2019
Fecha Vencimiento: 12 ENERO DE 2020

CODIGO	REFERENCIA	CANT.	V. UNITARIO	V. TOTAL
GMS	Consultoria - Seguridad Respuesta a Incidentes 20 Horas para atención y respuesta a Incidentes (Remoto)	1	$ 3.500.000	$ 3.500.000

Favor realizar sus pagos a nombre de GRUPO MICROSISTEMAS COLOMBIA S.A.S. en la CTA. CTE. 300-955197-85 de BANCOLOMBIA.

El pago de esta factura debe hacerse a favor de GRUPO MICROSISTEMAS COLOMBIA S.A.S.
Esta factura se asimila en todos sus efectos a una letra de cambio (art. 774 del C.C.)
En caso de mora el deudor pagará un interés, a la tasa máxima legal vigente en la fecha de su causación.
La firma de terceros en representación, mandato u otra calidad similar a nombre del Comprador; implica su obligación de acuerdo el Art. 640 del C.C. igualmente constancia de entrega real y a entera satisfacción.

Impreso por Corfecitel Colombia S.A.S. Nit 900.389.517-0

CUATRO MILLONES CIENTO SESENTA Y CINCO MIL con CERO CENTAVOS

Son:

Subtotal:	$ 3.500.000
IVA (%):	$ 665.000
Total:	$ 4.165.000
ICA:	$ 0
ReteIVA:	$ 0
Retefuente: 4% 140000	$ 0
Total Neto:	$ 4.165.000

Aceptada

Nombre:
C.C.
Fecha
Sello Cliente

Firma Autorizada

Transversal 22 # 98-82 - Ofi. 303 Edi. Porta 100 - Tel. (57-1) 743 3559 - Bogotá - Colombia
informacion@gmsseguridad.com

COPIA

Bancolombia
NIT. 890.903.938-8

Empresa: SOTELCOM S.A.S.
NIT: 900368512
Tipo de pago: PAGO A PROVEEDORES

Nombre del pago: provedores17012020
Secuencia: B
Número de cuenta a debitar: 38112825035

Fecha: 20-01-2020 **Hora:** 11:06:28
Fecha de Generación: 20-01-2020

Fecha de envío del pago: 17-01-2020
Fecha para Procesar el pago: 17-01-2020

Impreso por: alixvalencia

Total Registros del Lote: 15	**Registros Procesados:** 10	**Registros Rechazados:** 2	**Registros Pendientes:** 3
Valor Total del Pago: $470,614,350.00	**Valor Registros Procesados:** $39,245,901.00	**Valor Registros Rechazados:** $1,202,300.00	**Valor Registros Pendientes:** $430,166,149.00

NÚMERO DE CUENTA	TIPO DE CUENTA	DOCUMENTO BENEFICIARIO	NOMBRE BENEFICIARIO	VALOR	ENTIDAD	ESTADO	FECHA APLICACIÓN
256023698	Corriente	890304345	electricos del val	1,504,196.00	BANCO DE BOGOTA	POR APLICAR EN ENTIDAD DE ACH	17-01-2020
30095519785	Corriente	900418656	GRUPO MICROSISTEMA	4,025,000.00	BANCOLOMBIA	ABONADO EN BANCOLOMBIA, PROVENIENTE DE CLIENTE	17-01-2020
82575427315	Corriente	900298074	GVS COLOMBIA SAS	286,630.00	BANCOLOMBIA	ABONADO EN BANCOLOMBIA, PROVENIENTE DE CLIENTE	17-01-2020
03400641441	Corriente	800091549	IMPRESISTEM	678,417.00	BANCOLOMBIA	ABONADO EN BANCOLOMBIA, PROVENIENTE DE CLIENTE	17-01-2020
05427926983	Corriente	900091709	LICENCIAS ONLINE	10,000,000.00	BANCOLOMBIA	ABONADO EN BANCOLOMBIA, PROVENIENTE DE CLIENTE	17-01-2020
06411465716	Corriente	805024696	Lince Comercial	4,062,187.00	BANCOLOMBIA	ABONADO EN BANCOLOMBIA, PROVENIENTE DE CLIENTE	17-01-2020
20785693651	Ahorros	830067005	MILENIO PC LTDA	2,413,380.00	BANCOLOMBIA	ABONADO EN BANCOLOMBIA, PROVENIENTE DE CLIENTE	17-01-2020
25005477557	Corriente	830018214	MPS Mayorista	5,165,650.00	BANCOLOMBIA	ABONADO EN BANCOLOMBIA, PROVENIENTE DE CLIENTE	17-01-2020
03203577605	Corriente	800035776	NexsysMayorista	596,790.00	BANCOLOMBIA	ABONADO EN BANCOLOMBIA, PROVENIENTE DE CLIENTE	17-01-2020
22769156751	Corriente	860450450	Nicomar Electronic	90,635.00	BANCOLOMBIA	ABONADO EN BANCOLOMBIA, PROVENIENTE DE CLIENTE	17-01-2020
06476406360	Corriente	901075762	SMT	11,927,212.00	BANCOLOMBIA	ABONADO EN BANCOLOMBIA, PROVENIENTE DE CLIENTE	17-01-2020
496001405	Corriente	830089336	westcon group colo	428,461,953.00	BANCO BBVA	POR APLICAR EN ENTIDAD DE ACH	17-01-2020
82582963866		1151956666	Kevin Agudelo	400,000.00	BANCOLOMBIA	NIT PAGADOR NO INSCRITO AL SERVICIO DE TARJETAS	17-01-2020
5871008886	Ahorros	4957254	JESUS PISO SIERRA	200,000.00	SCOTIABANK COLPATRIA S.A	POR APLICAR EN ENTIDAD DE ACH	17-01-2020
75832293202		14636826	Manuel Alejandro V	802,300.00	BANCOLOMBIA	NIT PAGADOR NO INSCRITO AL SERVICIO DE TARJETAS	17-01-2020

Juan Felipe Mora Mostacilla

De: Juan Felipe Mora Mostacilla <juan.mora@sotelcom.co>
Enviado el: martes, 28 de marzo de 2023 12:05 p. m.
Para: Carolina Garrote
Asunto: RV: PROF00046505 cliente Sotelcom SAS
Datos adjuntos: RESPUESTA GMS.pdf

Doctora Carolina,
Esta son algunos correo que se cruzaron con ellos. Del tema GMS.

Saludos.

sotelcom
tecnología que impulsa

Juan Felipe Mora Mostacilla
Gerente Tecnico
CCSE # CP0000101034

www.sotelcom.co · info@sotelcom.co
Avenida 5an # 23dn - 68. Oficina 322 y 323.
Centro Comercial Pasarela. Cali, Colombia.

Correo: juan.mora@sotelcom.co
PBX: (2) 524 6043 Ext.: 105
Móvil: 3185327566

De: Cristian Caicedo <cristian.caicedo@sotelcom.co>
Enviado el: martes, 28 de marzo de 2023 12:01 p. m.
Para: Juan Felipe Mora Mostacilla <juan.mora@sotelcom.co>
Asunto: RV: PROF00046505 cliente Sotelcom SAS

RE: PROF00046505 cliente Sotelcom SAS

Ing. Luis F Pabon T

Responder | Responder a todos | Reenviar

Para alejandro.navarro@gmsseguridad.com

domingo 9/05/20

CC Cristian Caicedo; Contabilidad

RESPUESTA GMS.pdf
157 KB

Buenos días Sr. Alejandro Navarro,

Adjunto documento como respuesta para cerrar el caso de la factura 2443.

Agradezco su atención y gestión al respecto.

Saludo cordial,

sotelcom
tecnología que impulsa

Luis Fernando Pabón Tovar
Gerente General.

www.sotelcom.co - info@sotelcom.co
Avenida 5an # 23dn - 68. Oficina 322 y 323.
Cali, Colombia.

Correo: luis.pabon@sotelcom.co
PBX: (2) 524 6043 Ext.: 104
Móvil: 3164728465

De: Ing. Luis F Pabon T <luis.pabon@Sotelcom.co>
Enviado el: domingo, 9 de mayo de 2021 7:22 a. m.
Para: alejandro.navarro@gmsseguridad.com
CC: Cristian Caicedo <cristian.caicedo@sotelcom.co>; Contabilidad <contabilidad@sotelcom.co>
Asunto: RE: PROF00046505 cliente Sotelcom SAS

Buenos días Sr. Alejandro Navarro,

Adjunto documento como respuesta para cerrar el caso de la factura 2443.

Agradezco su atención y gestión al respecto.

Saludo cordial,

sotelcom
tecnología que impulsa

Luis Fernando Pabón Tovar
Gerente General.

www.sotelcom.co · info@sotelcom.co
Avenida 5an # 23dn - 68. Oficina 322 y 323.
Cali, Colombia.

Correo: luis.pabon@sotelcom.co
PBX: (2) 524 6043 Ext.: 104
Móvil: 3164728465

De: Alejandro Navarro <alejandro.navarro@gmsseguridad.com>
Enviado el: martes, 23 de febrero de 2021 5:49 p. m.

Para: Cristian Caicedo <cristian.caicedo@sotelcom.co>
CC: María Sandra Gálvez <mariasandra.galvez@gmsseguridad.com>; Ing. Luis F Pabon T <luis.pabon@Sotelcom.co>
Asunto: RE: PROF00046505 cliente Sotelcom SAS

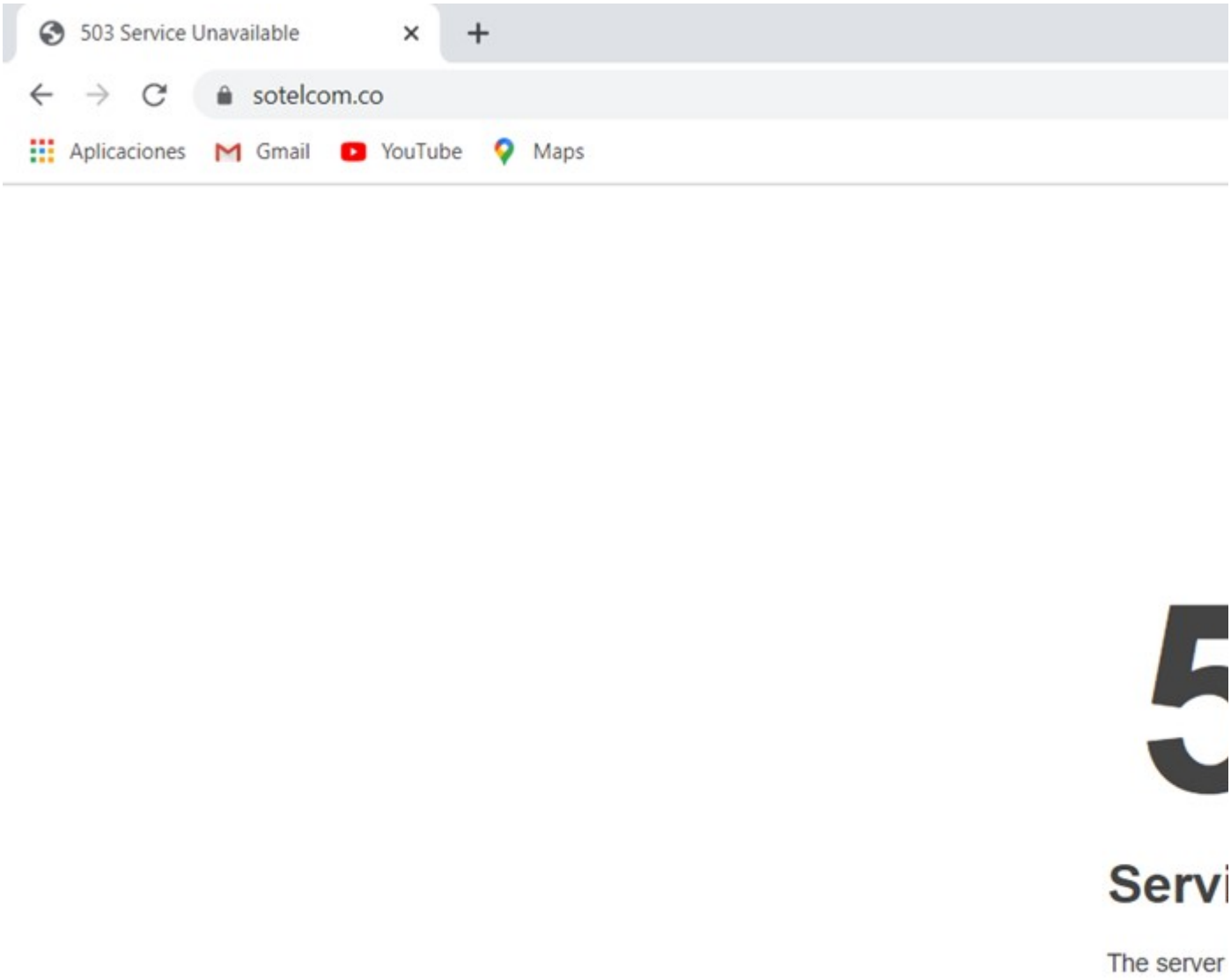
Hola Cristian, como vas, buenas tardes.

Gracias por el planteamiento, pero el lio es que por tratarse de una factura de un periodo que en GMS ya esta cerrado, no podemos hacer modificaciones. Si generaramos una NC, nos estaría restando de 2021 que de por si ya empezó apretado.

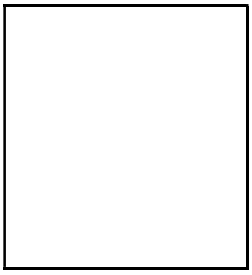
Estoy seguro que vamos a encontrar los espacios para poder ejecutar estos servicios en conjunto, y mas bien te planteo que nos realicen un pago inmediato del 50% de la factura y el otro 50% lo dejamos a 60 días. El objetivo en estos 60 dias es que comercialmente las dos empresas nos pongamos estrategias comerciales para no solo cubrir el monto total, sino poder seguir haciendo negocios a largo plazo.

Me interesa revisar el portafolio de Sotelcom, estuve tratando de verlo en el portal web pero esta caída la pag, vale la pena el momento para avisarles.

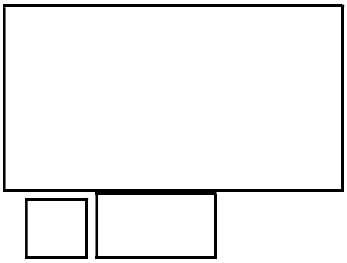
Quedo atento a tu confirmación para empezar a trabajar en ejecutar estos servicios.



Saludos,



Alejandro Navarro
Gerente General
alejandro.navarro@gmsseguridad.com
Oficina: +57 17433559 Ext. 7801
Cel: +57 3043430956
www.gmsseguridad.com



De: Cristian Caicedo <cristian.caicedo@sotelcom.co>
Enviado el: martes, 23 de febrero de 2021 1:59 p. m.
Para: Alejandro Navarro <alejandro.navarro@gmsseguridad.com>
CC: María Sandra Gálvez <mariasandra.galvez@gmsseguridad.com>; Ing. Luis F Pabon T <luis.pabon@Sotelcom.co>
Asunto: RV: PROF00046505 cliente Sotelcom SAS

Alejandro
Cordial Saludo

Según nuestro análisis sobre la factura que nos hicieron para el servicio en mención que nunca se prestó, y sabemos que fue por culpa del cliente final, y teniendo en cuenta la disposición de ustedes para el tema.

Proponemos que partamos diferencias, de bajarle el monto a la mitad, y nosotros nos comprometemos a comprarles como mínimo productos o servicios de aquí a que se acabe el año sobre el valor de la mitad que es $10.743.000 MAS IVA

Teniendo en cuenta que la factura es de 21.487.000 MAS IVA Y que son servicios que no nos prestaron.

Hay muchas líneas en seguridad en las cuales no manejamos y que ustedes son expertos en el tema y podemos trabajar oportunidades que nosotros detectamos . VERACODE, ETHIKAL HACKING, PROTECCION DE MARCA, INGENIERIA SOCIAL. ETC.

Hay otros que si manejamos y tenemos algunos clientes con el producto pero que podemos tener unos precios favorables a través de ustedes por el nivel de partner que son y por la experticia, los cuales son Kaspersky y Sophos.

Así que creo que es una forma de empezar a tener sinergias que nos ayuden a ambas compañías a crecer. SOTELCOM y a GMS

Quedo atento a tus comentarios o sugerencias.

sotelcom
tecnología que impulsa
www.sotelcom.co ·
Avenida 5an # 23dn - 68. Oficina 322 y 323.
Cali, Colombia.

Cristian Andres Caicedo Duarte (Ing, MBA)
Key Account Manager
Skype:caicedocristian
Correo: cristian.caicedo@sotelcom.co
PBX: (2) 524 6043 Ext.: 108
Móvil: 3187235595-3184178013

Asunto: RV: Informe Alcaldía de Cali

Juan Felipe Mora Mostacilla <juan.mora@sotelcom.co>
para Carolina Garrote, Ing. Luis F Pabon T, Cristian Caicedo

lun, 3 abr, 11:03

Estás viendo un mensaje adjunto. Gmail no puede verificar la autenticidad de los mensajes adjuntos.

Dra. Carolina este fue el servicio del otro si del contrato de alcaldía. Este servicio lo realizo GMS generando el informe, luego se procedió con el pago este.

Para los otros servicio si fueron realizado se espera un informe similar.

Adjunto.

sotelcom
tecnología que impulsa

Juan Felipe Mora Mostacilla
Gerente Tecnico
CCSE # CP0000101034

www.sotelcom.co · info@sotelcom.co
Avenida 5an # 23dn - 68. Oficina 322 y 323.
Centro Comercial Pasarela. Cali, Colombia.

Correo: juan.mora@sotelcom.co
PBX: (2) 524 6043 Ext.: 105
Móvil: 3185327566

De: Luis Fernando Vinueza <luisfernando.vinueza@gmsseguridad.com>
Enviado el: martes, 24 de diciembre de 2019 9:20 a. m.
Para: Juan Felipe Mora Mostacilla <juan.mora@sotelcom.co>
Asunto: Informe Alcaldía de Cali

Estimado Juan,

Le envío el informe

Salud

Luis Fernando Vinueza
Consultor TI
luisfernando.vinueza@gmsseguridad.com
Oficina: +593 23993000 Ext. 7548
Cel: +593 989086314
www.gmsseguridad.com

Un archivo adjunto • Analizado por Gmail

AF-ALCCALI-INF...

Sres.
GMS SEGURIDAD SAS
Atención: Alejandro Navarro
L.C.

REFERENCIA: NO ACEPTACION Y SOLICITUD DE ANULACION DE LA FACTURA

Cordial saludo.

Revisión de la solicitud de pago de la factura no acepta, es el nuevo consultoría experta para determinar la procedencia de la factura, en este sentido se determinó que toda vez que la factura no fue aceptada por parte de la compañía y en el sentido que no fue ejecutado ningún servicio, no existe exigibilidad del título valor, careciendo de uno de los requisitos mínimos.

Frente al Código de Comercio, Artículo 773. Aceptación de la factura, establece la norma que: "El comprador o beneficiario del servicio deberá aceptar de manera expresa el contenido de la factura, por escrito colocado en el cuerpo de la misma o en documento separado, físico o electrónico. Igualmente, deberá constar el recibo de la mercancía o del servicio por parte del comprador del bien o beneficiario del servicio, en la factura y/o en la guía de transporte, según el caso, indicando el nombre, identificación o la firma de quien recibe, y la fecha de recibo. El comprador del bien o beneficiario del servicio no podrá alegar falta de representación o indebida representación por razón de la persona que reciba la mercancía o el servicio en sus dependencias, para efectos de la aceptación del título valor".

Lea más: https://leyes.co/codigo_de_comercio/773.htm

En este sentido, no fue aceptada la factura como tampoco se recibió la prestación del servicio, lo que trae como consecuencia que no exista ninguna obligación de pago.

Solicitamos respetuosamente se anule la factura, toda vez que no hay lugar al pago.

Cordialmente,

Luis Fernando Pabón Tovar.
Representante Legal
SOTELCOM, SAS

DEFINICIÓN DE SOC (SECURITY OPERATIONS CENTER)

SOC

El SOC, o Centro de Operaciones de Seguridad, es un servicio de monitoreo conformado por personal especializado en seguridad TI, acompañado de infraestructura tecnológica avanzada para concentrar y analizar los eventos relacionados con la seguridad informática. El objetivo del SOC es minimizar los riesgos y las vulnerabilidades a los que están expuestos las empresas.

¿Por qué se debe contratar un SOC (Security Operations Center)?

Disponer de personal especializado en seguridad de la información es muy valioso para una compañía, pero no es suficiente. La combinación de conocimientos, herramientas, procesos y desempeños puede proporcionar la seguridad que necesita cada institución. Por esta razón, la implementación de un SOC es necesaria para cualquier tipo de compañía.

Link para ingresar a la página de GMS https://gmsseguridad.com/soluciones/soc/

19-12-2019

Informe: AF-ALCCALI-INF001

INFORME DE RESULTADOS

Análisis Forense
Alcaldía de Cali - GMS

Cali - Colombia

CONTROL DOCUMENTAL

PROYECTO:	Análisis Forense
ENTIDAD:	Alcaldía de Santiago de Cali
TITULO:	Informe de resultados
VERSIÓN:	Versión 1.0
FECHA EDICIÓN:	19 de diciembre de 2019
FICHERO:	AF-ALCCALI-INF001.docx
HERRAMIENTAS DE EDICIÓN:	Microsoft Office Word
AUTORES:	Consultoría - GMS
RESUMEN:	Resumen de resultados

CONTROL DE VERSIONES

VERSIÓN	AUTOR	FECHA DE VALIDACIÓN	DESCRIPCIÓN
1.0	GMS	19 de diciembre de 2019	Informe de resultados

ÚLTIMA REVISIÓN

PÁG.:	MODIFICACIÓN

VALIDACIONES Y APROBACIONES

Elaborado Por:	Luis Fernando Vinueza
Validado Por:	Jefferson Curay
Aprobado Por:	Jonathan Córdoba

Tabla de Contenidos

Vigencia

Este documento entrará en vigor en el momento en que la versión de la documentación haya alcanzado la versión 1.0. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de GMS.

Las versiones anteriores a la versión 1.0 que hayan podido distribuirse constituyen borradores; por lo que su posible vigencia queda anulada y se sustituyen por la última versión del documento. Las modificaciones sugeridas se someterán a la aprobación de la Alcaldía de Santiago de Cali. Esta versión seguirá vigente mientras no se aprueben y publiquen modificaciones.

Perfil del Consultor

Estudios

- Ingeniería Electrónica y redes de información
- Maestría en TI con mención en Seguridad de Redes

Certificaciones

- Sophos Central Overview – Engineer
- Sophos XG Firewall v17.0 – Engineer
- Sophos Central Endpoint and Servers v1.0 – Engineer
- Intercept X Advanced with EDR
- KLE 002.11 – Kaspersky fundamentals
- Kaspersky Cybersecurity
- Certificado de Explotación de Vulnerabilidades
- Certificado de Análisis de Vulnerabilidades
- Certificado de Information Gathering
- Kaspersky Endpoint Security and Management
- Sophos Email Appliance
- Sophos Email Protection v4.0 – Engineer
- Sophos Cerified Engineer
- Sophos Central Email Gateway
- Sophos UTM v9.5 – Engineer
- Sophos Central Device Encription
- Sophos Central Wireless v1.1
- Phish Threat
- Intercept X

Experiencia

- EH Leterago del Ecuador
- AF Quito Tennis y Golf Club
- AF Interlab S.A
- EH Coop. Ambato
- EH Mutualista Pichincha
- EH ENAMI EP
- AF ENAMI EP
- EH a varias empresas por confidencialidad no es posible revelar el nombre
- AF a varias empresas por confidencialidad no es posible revelar el nombre

1 Introducción

Visión

Para el año 2027 el municipio de Santiago de Cali será un territorio reconocido a nivel nacional e internacional como el municipio líder en la integración social, económica y cultural de su población, habiendo logrado reducir sustancialmente sus brechas sociales, a través de un desarrollo incluyente, sostenido, participativo y transparente en su gestión pública. Soportando dicho desarrollo en su papel de principal polo de desarrollo económico y social de la ciudad - región, en el uso eficiente de sus recursos naturales y de su infraestructura de servicios, en la dinámica de su riqueza socio-cultural urbana y rural, en la competitividad de sus propuestas artísticas, culturales y deportivas, en la integración de su diversidad étnica, en la fortaleza estructurante de su sector académico, en el esfuerzo articulado de su sector empresarial y en el dialogo permanente entre la ciudadanía y la administración, para la construcción constante de la paz y convivencia en su territorio. En el marco de esta visión de desarrollo, Santiago de Cali se consolidará como un territorio incluyente, líder, innovador, que le apuesta al bienestar de su población como motor principal y centro de sus decisiones; priorizando el talento, la disciplina, el trabajo, la dedicación, la honestidad, la cultura ciudadana y el desarrollo de los aspectos propios de su diversidad multicultural y pluriétnica; facilitando las condiciones para la generación de ingresos que permitan mejorar las condiciones de vida de todos sus habitantes y la competitividad de la ciudad.

Convirtiéndose en modelo de política social en el país, promoviendo la construcción de entornos y estilos de vida saludables que conlleven a una mejor calidad de vida de su población; destacándose por el liderazgo en la adopción, formulación y adaptación de políticas públicas con plena participación de la población, diferentes sectores y actores que incidan de manera favorable y potente sobre la salud, la educación, la cultura, el deporte, el bienestar social y la calidad de vida de los ciudadanos.

Propendiendo por un ordenamiento territorial sostenible que dinamice las diferentes zonas de la ciudad, facilitando el crecimiento sostenible, e incluyendo su ruralidad bajo criterios de sustentabilidad y sostenibilidad ambiental, humana, económica y equidad social; en el cual los sistemas establecidos en su Plan de Ordenamiento Territorial - espacio público, equipamientos, servicios públicos y movilidad- se

desarrollen sobre la lógica de la eficiencia, responsabilidad ambiental, equidad, competitividad y disfrute de sus habitantes, fortaleciendo el concepto de espacio público y de uso compartido de la ciudad, con un sistema de movilidad, donde se respete el peatón y tenga prioridad el transporte público y los medios alternativos sobre el automóvil particular.

Consolidando la relación de Santiago de Cali con sus municipios vecinos, convirtiéndose en la ciudad líder de la región de la cuenca del Pacífico con centro de actividades de alcance subnacional, nacional e internacional, con un propósito que permitirá aprovechar sus ventajas económicas comparativas identificando y favoreciendo acciones sobre el territorio que impulsen su competitividad.

Misión

"El Municipio de Santiago de Cali, como ente territorial, genera las condiciones necesarias para la oportuna prestación de los servicios públicos y sociales, a través de la planificación del desarrollo económico, social, ambiental y del territorio y, de la administración efectiva de los recursos, propiciando la participación ciudadana en la gestión pública, el ejercicio de los derechos y deberes constitucionales y la convivencia pacífica de sus habitantes, con el fin de mejorar su calidad de vida".

2 Contexto

El equipo de especialistas responsables del servicio de análisis forense de GMS ha ejecutado tareas de recolección y análisis de información sobre el incidente reportado en los servidores PJD y SAPRouter.

Las técnicas, tácticas y habilidades aplicadas por el equipo de especialistas nos permiten presentar en este documento un registro integral de las acciones desarrolladas en torno al incidente de seguridad informática presentado.

3 Alcance

La investigación se centra en el incidente reportado por parte de la Alcaldía de Cali que se dio en dos de sus servidores.

En el proceso de investigación se realiza análisis en los dos servidores tratando de encontrar información en la cual apoye a tener una visión más clara de los sucesos acontecidos.

4 Objetivos

4.1 Objetivo General

Desarrollar un documento técnico que revele los resultados obtenidos en el análisis forense, en la cual se detalle información relacionada al incidente.

4.2 Objetivos Específicos

- Recolectar información relacionada al incidente en cada uno de los servidores.
- Analizar los logs de los servidores y eventos para aportar con más información.
- Analizar evidencias de archivos adjuntos.

5 Hallazgos

5.1 Análisis a los servidores SAProuter 172.18.20.17

5.1.1 Análisis realizado

Al mantener reuniones con el Ing. Roger González y con toda la información facilitada en correos se pudo establecer una línea de tiempo de acontecimientos, a su vez lograr una mejor investigación y recolección de información en el servidor. En el caso de SAPRouter los puntos más importantes a tomar en cuenta son los siguientes:

- El hostname se encuentra como “NONE”
- El 2 de diciembre de 2019 a las 17h15 se realizó la instalación/actualización de 48 paquetes RPM

En la investigación se inició con el análisis de accesos al servidor, al tratar de encontrar eventos de acceso validos o inválidos al servidor cercanos al 2 de diciembre del 2019 no fue posible ya que los eventos más antiguos eran del 12 de diciembre de 2019, lo cual llama la atención debido a que estos eventos por lo general se almacenan de tres meses, al revisar se validó que no se tienen eventos más antiguos debido a que existen aparentes ataques de fuerza bruta al servidor desde la IP 45.136.108.85, lo cual llenó los logs y se eliminaba el más antiguo.

En la imagen 1 se puede validar que existen demasiados intentos inválidos desde dicha IP por lo cual se recomienda bloquear desde perímetro de forma urgente.

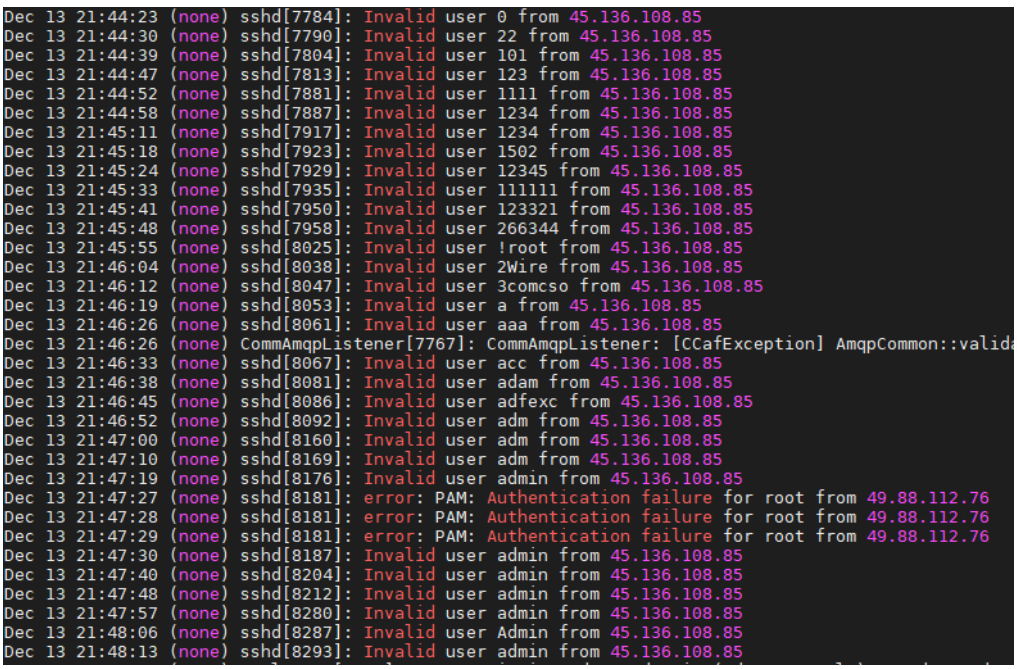


Imagen 1. Evidencia de posible ataque de fuerza bruta.

Posteriormente al revisar el acceso al servidor se valida que todos los ingresos realizados en diciembre son por root, sería importante validar si efectivamente desde el 2 de diciembre al 13 no existieron ingresos al servidor por que no existen registros de posibles ingresos.

```
wtmp begins Tue Mar 12 14:46:39 2019
(none):~ # last -n 20
root     pts/0        192.168.249.1    Mon Dec 16 17:11   still logged in
root     pts/0        172.18.15.247    Fri Dec 13 11:47 - 12:35  (00:48)
root     pts/0        172.18.15.247    Fri Dec 13 11:36 - 11:46  (00:09)
reboot   system boot  3.0.13-0.27-defa Fri Dec 13 10:48         (3+06:26)
root     pts/0        172.18.15.247    Mon Dec  2 19:39 - 19:55  (00:16)
root     pts/0        172.18.15.247    Mon Dec  2 19:27 - 19:38  (00:10)
root     pts/0        10.20.255.3      Mon Dec  2 15:52 - 18:04  (02:11)
root     pts/2        10.20.255.3      Mon Dec  2 10:00 - 14:11  (04:11)
root     pts/1        10.20.255.3      Mon Dec  2 09:52 - 13:03  (03:10)
root     pts/0        10.20.255.3      Mon Dec  2 07:36 - 10:47  (03:11)
root     pts/2        10.20.255.3      Sun Dec  1 19:34 - 22:45  (03:11)
root     pts/1        10.20.255.4      Sun Dec  1 17:47 - 20:00  (02:12)
root     pts/0        10.20.255.4      Sun Dec  1 17:31 - 20:42  (03:11)
root     pts/3        10.20.255.4      Sun Dec  1 10:49 - 15:01  (04:11)
root     pts/2        10.20.255.4      Sun Dec  1 10:44 - 13:56  (03:11)
root     pts/1        10.20.255.3      Sun Dec  1 10:35 - 12:47  (02:12)
root     pts/0        10.20.255.3      Sun Dec  1 10:21 - 11:05  (00:44)
reboot   system boot  3.0.13-0.27-defa Sat Nov 30 05:14         (13+05:21)
root     pts/0        10.20.255.5      Thu Nov 28 11:23 - 11:26  (00:02)
root     pts/0        10.20.255.7      Wed Nov 20 11:39 - 14:51  (03:11)
```

Imagen 2. Evidencia de loggeos exitosos.

Posteriormente se valida el error que da en el hostname, se valida esto en la imagen 3 y adicionalmente se valida si el nombre de servidor también presenta errores, se determina que el nombre de máquina no presenta errores como se visualiza en la imagen 4.

```
(none):~ # hostname
(none)
```

Imagen 3. Evidencia de error en hostname.

```
(none):~ # cat /etc/hostname
farallones.alcaldia.gov.co
```

Imagen 4. Evidencia de nombre de servidor.

Se valida que el error de hostname se da por varios archivos de configuración que se encuentran corruptos, esto puede deberse a mal apagado de la máquina o error en actualizaciones, como se puede revisar en la siguiente imagen.

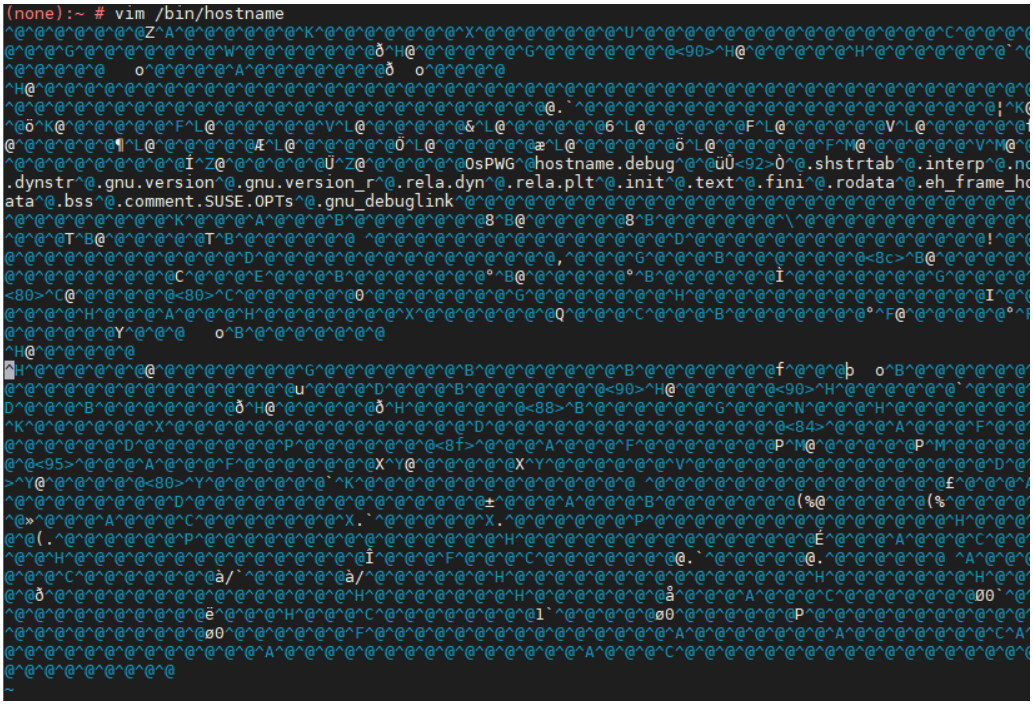


Imagen 5. Evidencia de archivo corrupto.

Imagen 6. Evidencia de archivo corrupto.

En cuanto a la revisión de los supuestos archivos instalados se revisa que en el historial de instalación la última instalación es con fecha 01/03/2019, como se muestra en la imagen 7.

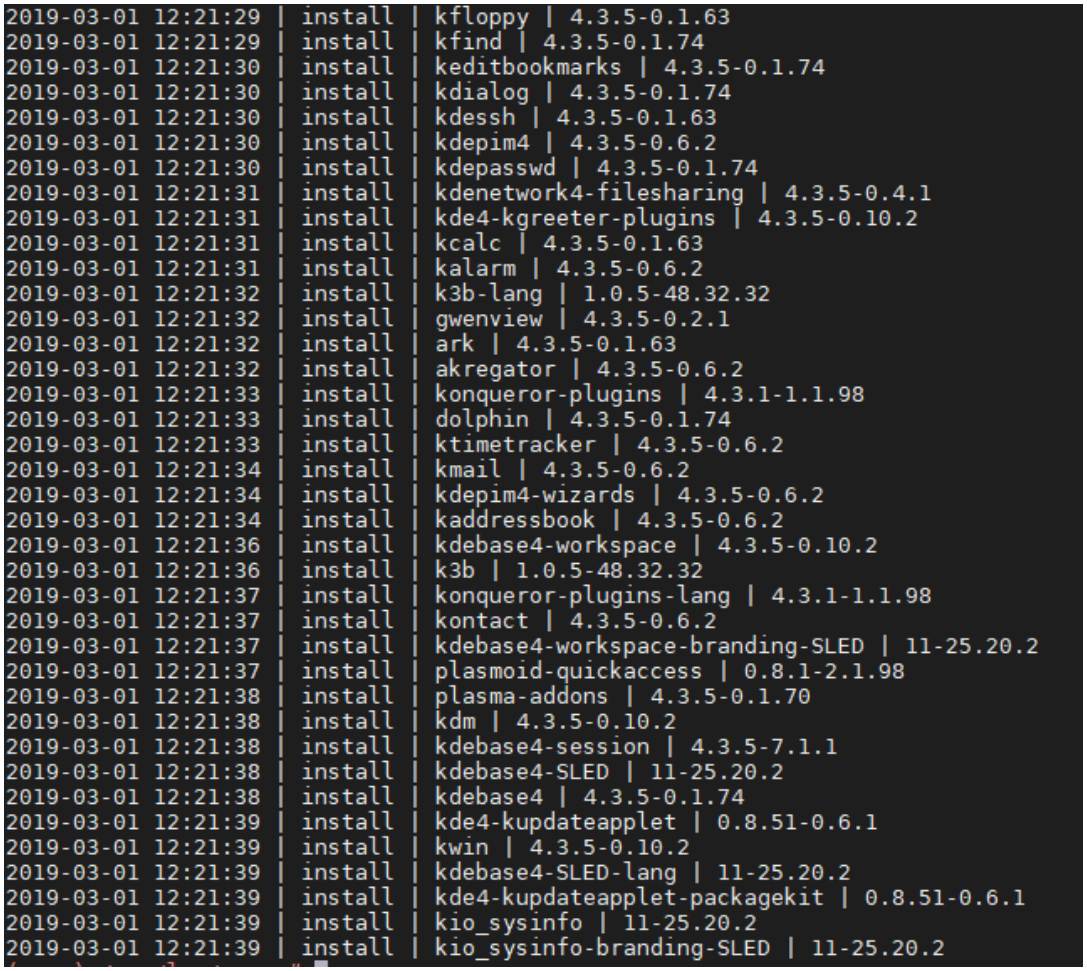


Imagen 7. Evidencia de paquetes instalados.

Se revisa lo reportado por el cliente, pero se determina que son paquetes añadidos de forma automática como parches por el SO, lo cual no indica que existió un ingreso como root para dicha instalación. Las instalaciones de parches se valida que se han dado mucho antes de los sucesos reportados y aún se da estas instalaciones, la última fue el 11/12/2019 como se puede evidenciar en la imagen 8.

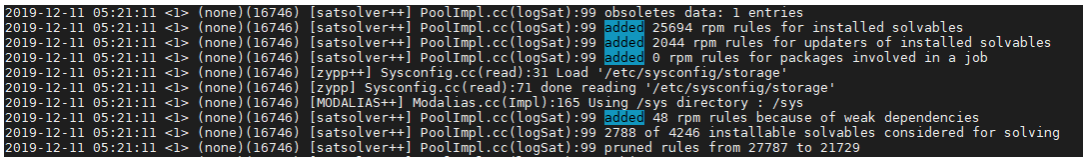
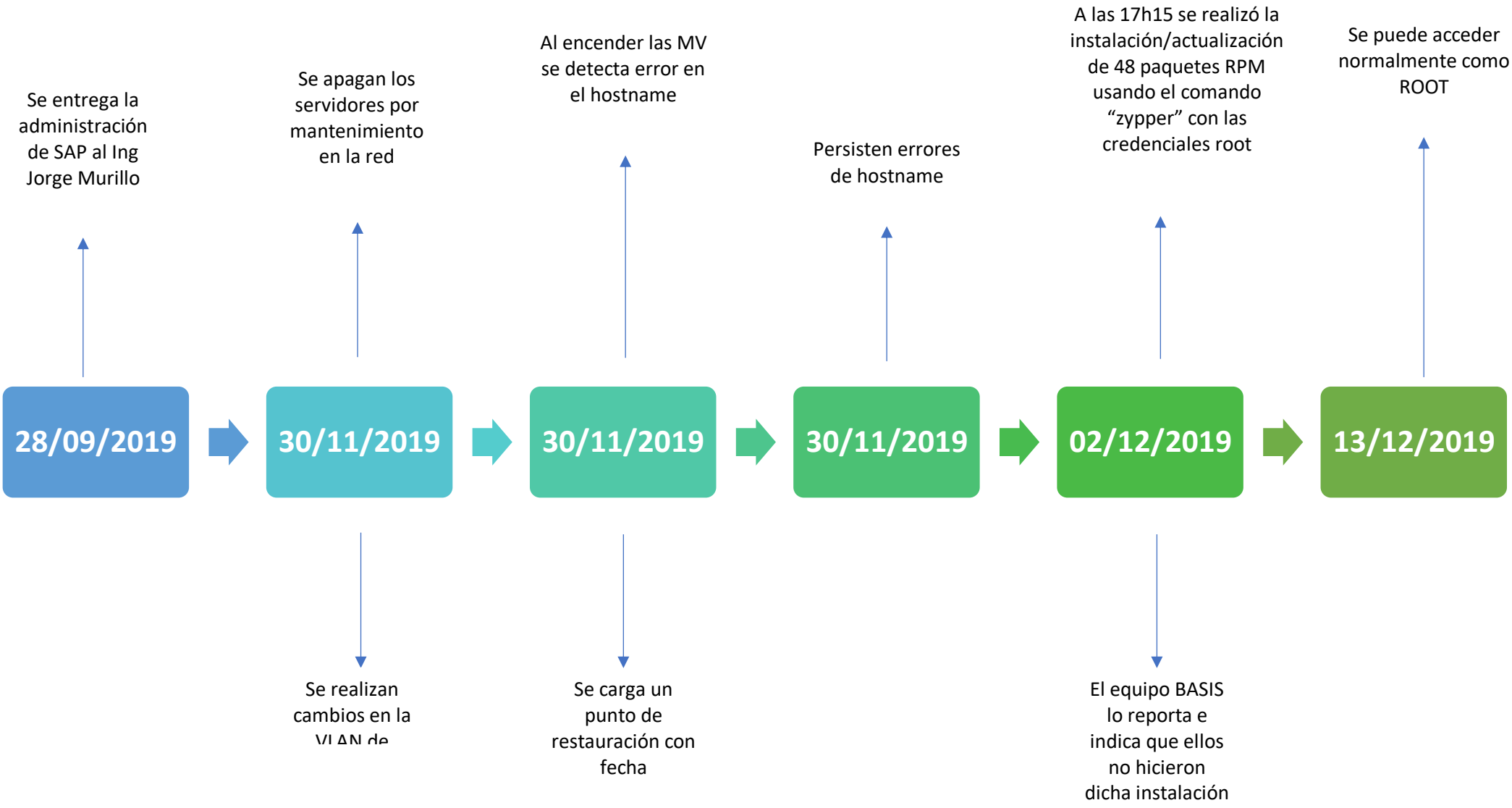


Imagen 8. Evidencia de paquetes instalados.

Se estableció una línea de tiempo de los sucesos de dicho servidor la cual es la siguiente:


Se entrega la administración de SAP al Ing Jorge Murillo
28/09/2019
Se apagan los servidores por mantenimiento en la red
30/11/2019
Se realizan cambios en la VLAN de
Al encender las MV se detecta error en el hostname
30/11/2019
Se carga un punto de restauración con fecha
Persisten errores de hostname
30/11/2019
A las 17h15 se realizó la instalación/actualización de 48 paquetes RPM usando el comando “zypper” con las credenciales root
02/12/2019
El equipo BASIS lo reporta e indica que ellos no hicieron dicha instalación
Se puede acceder normalmente como ROOT
13/12/2019

5.2 Análisis a los servidores PJD 172.18.20.22

5.2.1 Análisis de resultados

Al tratar de ingresar al servidor con las claves entregadas por el Ing.Roger González no fue posible por lo cual se solicitó se reestablezca las contraseñas de root, una vez realizado este proceso se ingresa al servidor y se nota que el servidor no tiene el problema del hostname, tal como se puede validar en la imagen 9.

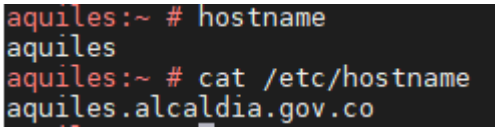


Imagen 9. Evidencia de hostname.

Posteriormente se trata de revisar los eventos de cambio de clave al servidor, pero no se puede encontrar esto debido a que el registro de eventos muestra sus eventos más antiguos con fecha 18/12/2019. Lo cual no nos resulta útil para saber los eventos anteriores, al parecer al momento en el que se reestableció la clave de root se perdió este registro.

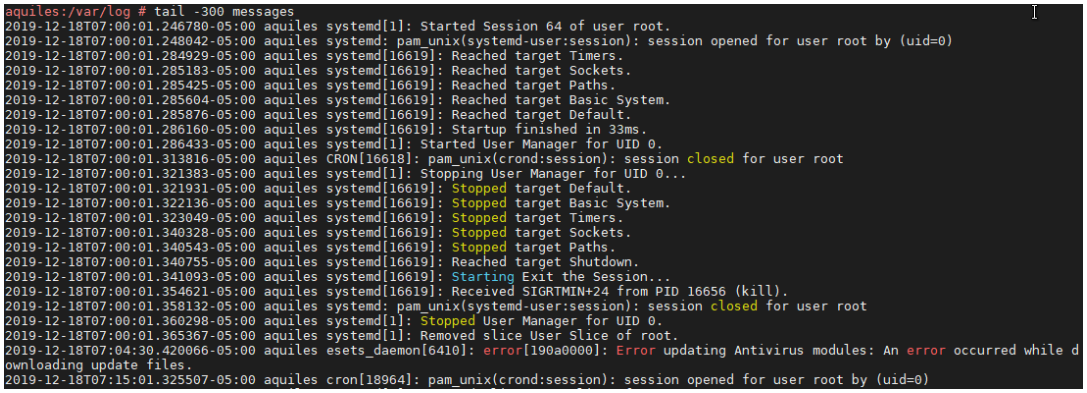
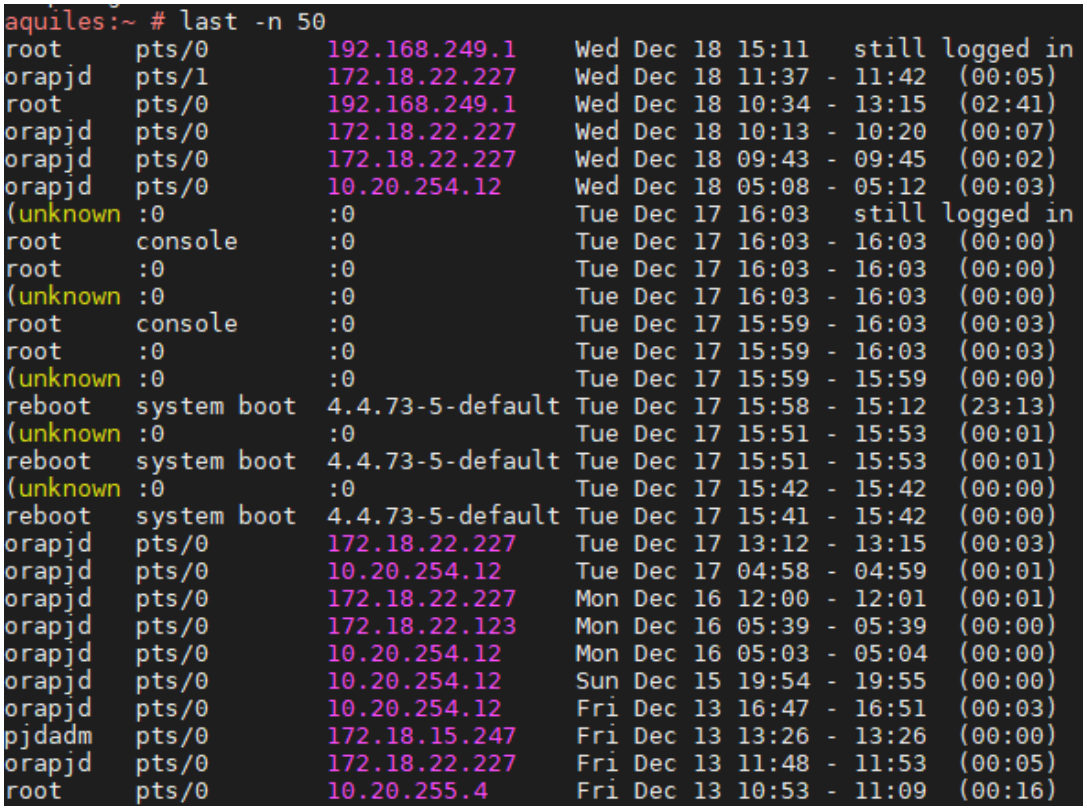


Imagen 10. Evidencia de eventos del sistema.

Posteriormente con el fin de validar si existieron loggeos exitosos al servidor las fechas que aparentemente no se tenía la clave de root se encuentra que si existieron accesos exitosos y de forma continua al servidor desde antes del 28 de noviembre hasta la fecha de la investigación 18/12/2019. Se puede observar que existieron ingresos por parte del usuario orapjd y el usuario root ingresó el 13 de diciembre a las 10h53 hasta las 11h09.

```
orapjd   pts/0        10.20.254.12     Fri Dec 13 16:47 - 16:51  (00:03)
pjdadm   pts/0        172.18.15.247    Fri Dec 13 13:26 - 13:26  (00:00)
orapjd   pts/0        172.18.22.227    Fri Dec 13 11:48 - 11:53  (00:05)
root     pts/0        10.20.255.4      Fri Dec 13 10:53 - 11:09  (00:16)
orapjd   pts/0        172.18.22.227    Fri Dec 13 06:21 - 06:25  (00:03)
orapjd   pts/0        10.20.254.12     Fri Dec 13 04:49 - 04:50  (00:00)
orapjd   pts/1        10.20.254.12     Thu Dec 12 11:05 - 11:07  (00:01)
orapjd   pts/1        10.20.254.12     Thu Dec 12 05:17 - 05:18  (00:00)
orapjd   pts/1        10.20.254.12     Wed Dec 11 05:03 - 05:04  (00:00)
oracle   pts/0        172.18.22.226    Tue Dec 10 14:41 - 15:48 (2+01:06)
orapjd   pts/0        10.20.254.12     Tue Dec 10 04:45 - 04:46  (00:01)
orapjd   pts/0        172.18.22.227    Mon Dec  9 12:30 - 12:35  (00:05)
orapjd   pts/0        172.18.22.227    Mon Dec  9 08:16 - 08:17  (00:00)
orapjd   pts/0        10.20.254.12     Mon Dec  9 04:58 - 05:00  (00:01)
orapjd   pts/0        172.18.22.227    Fri Dec  6 11:43 - 11:48  (00:05)
orapjd   pts/0        172.18.22.227    Fri Dec  6 06:49 - 06:51  (00:01)
orapjd   pts/0        172.18.22.227    Fri Dec  6 06:36 - 06:40  (00:04)
orapjd   pts/0        172.18.22.227    Thu Dec  5 12:14 - 12:21  (00:07)
orapjd   pts/0        10.20.254.12     Thu Dec  5 04:56 - 04:58  (00:01)
orapjd   pts/0        172.18.22.227    Wed Dec  4 10:55 - 11:02  (00:06)
orapjd   pts/0        172.18.22.227    Wed Dec  4 10:34 - 10:35  (00:01)
orapjd   pts/0        10.20.254.12     Wed Dec  4 05:15 - 05:16  (00:01)
orapjd   pts/0        172.18.22.227    Tue Dec  3 13:19 - 13:23  (00:04)
orapjd   pts/0        10.20.254.12     Tue Dec  3 04:57 - 04:58  (00:00)
pjdadm   pts/0        172.18.15.247    Mon Dec  2 15:17 - 15:17  (00:00)
orapjd   pts/0        172.18.22.227    Mon Dec  2 12:39 - 12:45  (00:06)
orapjd   pts/0        172.18.22.227    Mon Dec  2 12:16 - 12:20  (00:03)
(unknown :0           :0               Mon Dec  2 12:16 - 15:37 (15+03:21)
reboot   system boot  4.4.73-5-default Mon Dec  2 12:15 - 15:38 (15+03:22)
orapjd   pts/0        172.18.22.227    Mon Dec  2 06:45 - 06:49  (00:03)
orapjd   pts/0        10.20.254.12     Mon Dec  2 05:06 - 05:07  (00:00)
orapjd   pts/0        10.20.254.12     Sat Nov 30 05:50 - 05:51  (00:01)
(unknown :0           :0               Sat Nov 30 05:01 - 12:15 (2+07:13)
reboot   system boot  4.4.73-5-default Sat Nov 30 05:01 - 12:15 (2+07:13)
orapjd   pts/1        172.18.22.227    Fri Nov 29 11:39 - 11:43  (00:04)
orapjd   pts/1        172.18.22.227    Fri Nov 29 06:57 - 06:58  (00:00)
orapjd   pts/1        10.20.254.12     Fri Nov 29 05:01 - 05:02  (00:01)
orapjd   pts/1        172.18.22.227    Thu Nov 28 11:34 - 11:41  (00:06)
```

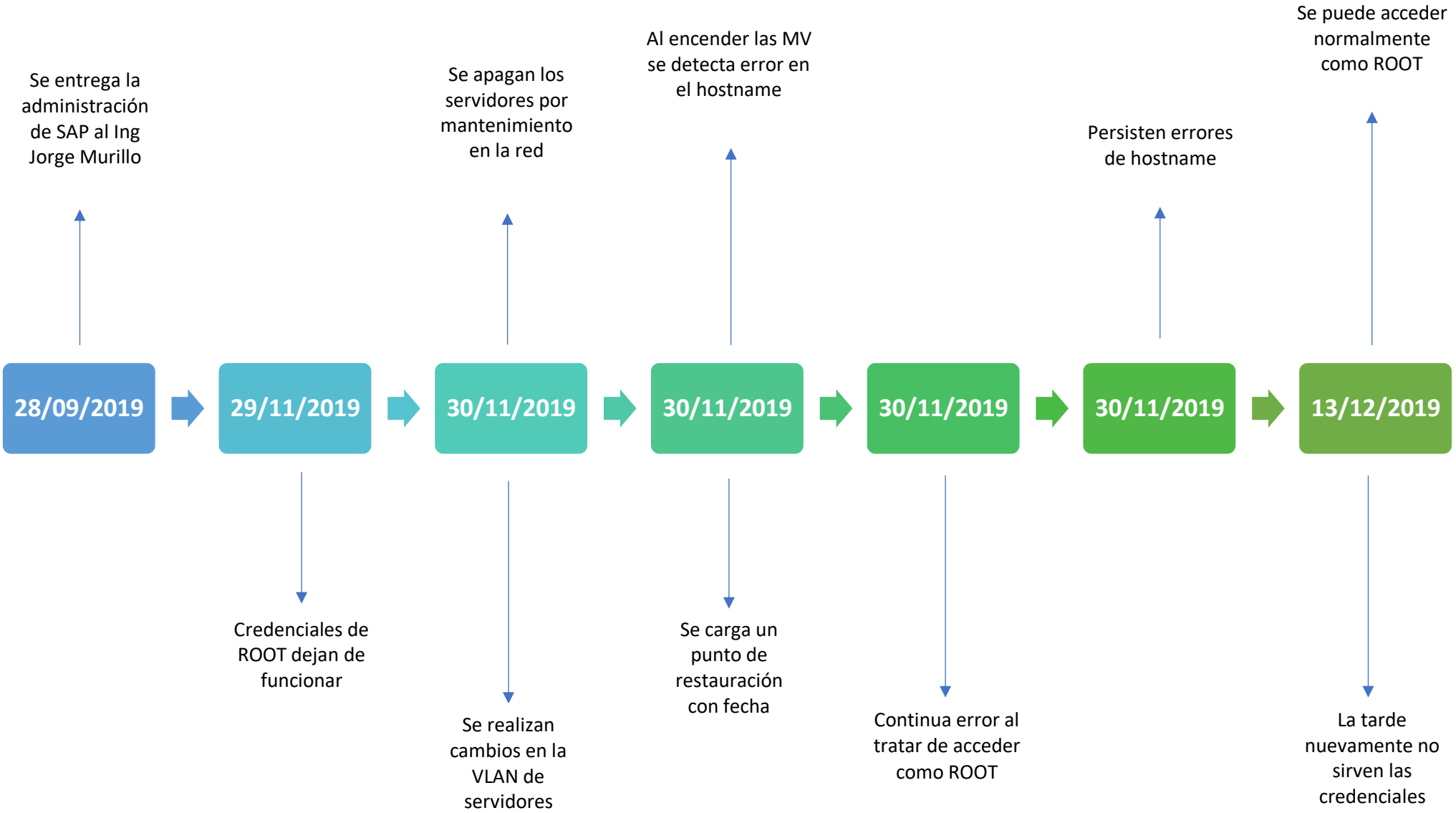
Imagen 11. Evidencia de ingreso al servidor.



```
aquiles:~ # last -n 50
root     pts/0        192.168.249.1    Wed Dec 18 15:11   still logged in
orapjd   pts/1        172.18.22.227    Wed Dec 18 11:37 - 11:42  (00:05)
root     pts/0        192.168.249.1    Wed Dec 18 10:34 - 13:15  (02:41)
orapjd   pts/0        172.18.22.227    Wed Dec 18 10:13 - 10:20  (00:07)
orapjd   pts/0        172.18.22.227    Wed Dec 18 09:43 - 09:45  (00:02)
orapjd   pts/0        10.20.254.12     Wed Dec 18 05:08 - 05:12  (00:03)
(unknown :0           :0               Tue Dec 17 16:03   still logged in
root     console      :0               Tue Dec 17 16:03 - 16:03  (00:00)
root     :0           :0               Tue Dec 17 16:03 - 16:03  (00:00)
(unknown :0           :0               Tue Dec 17 16:03 - 16:03  (00:00)
root     console      :0               Tue Dec 17 15:59 - 16:03  (00:03)
root     :0           :0               Tue Dec 17 15:59 - 16:03  (00:03)
(unknown :0           :0               Tue Dec 17 15:59 - 15:59  (00:00)
reboot   system boot  4.4.73-5-default Tue Dec 17 15:58 - 15:12  (23:13)
(unknown :0           :0               Tue Dec 17 15:51 - 15:53  (00:01)
reboot   system boot  4.4.73-5-default Tue Dec 17 15:51 - 15:53  (00:01)
(unknown :0           :0               Tue Dec 17 15:42 - 15:42  (00:00)
reboot   system boot  4.4.73-5-default Tue Dec 17 15:41 - 15:42  (00:00)
orapjd   pts/0        172.18.22.227    Tue Dec 17 13:12 - 13:15  (00:03)
orapjd   pts/0        10.20.254.12     Tue Dec 17 04:58 - 04:59  (00:01)
orapjd   pts/0        172.18.22.227    Mon Dec 16 12:00 - 12:01  (00:01)
orapjd   pts/0        172.18.22.123    Mon Dec 16 05:39 - 05:39  (00:00)
orapjd   pts/0        10.20.254.12     Mon Dec 16 05:03 - 05:04  (00:00)
orapjd   pts/0        10.20.254.12     Sun Dec 15 19:54 - 19:55  (00:00)
orapjd   pts/0        10.20.254.12     Fri Dec 13 16:47 - 16:51  (00:03)
pjdadm   pts/0        172.18.15.247    Fri Dec 13 13:26 - 13:26  (00:00)
orapjd   pts/0        172.18.22.227    Fri Dec 13 11:48 - 11:53  (00:05)
root     pts/0        10.20.255.4      Fri Dec 13 10:53 - 11:09  (00:16)
```

Imagen 12. Evidencia de ingreso al servidor.

Se estableció una línea de tiempo de los sucesos de dicho servidor la cual es la siguiente:


Se entrega la administración de SAP al Ing Jorge Murillo
28/09/2019
29/11/2019
Credenciales de ROOT dejan de funcionar
Se apagan los servidores por mantenimiento en la red
30/11/2019
Se realizan cambios en la VLAN de servidores
Al encender las MV se detecta error en el hostname
30/11/2019
Se carga un punto de restauración con fecha
30/11/2019
Continua error al tratar de acceder como ROOT
Persisten errores de hostname
30/11/2019
Se puede acceder normalmente como ROOT
13/12/2019
La tarde nuevamente no sirven las credenciales

6 Conclusiones

Durante el análisis realizado al servidor SAProuter 172.18.20.17 se concluye que:

- El inconveniente con la perdida del hostname es un error de SO, pudo haberse dado por un mal apagado del equipo o problemas durante actualización
- El servidor ha venido recibiendo ataques de fuerza bruta de varias IP pero la que más intentos a realizado es 45.136.108.85
- Existen varios archivos de configuración corruptos que sería importante repararlos.
- En cuanto a la instalación de los 48 parches es de forma automática realizada por el servidor.
- La última instalación que hubo en este servidor fue 01/03/2019.
- Al parecer no existió acceso no autorizado al mismo pero se debe tener en cuenta de los constantes ataques de fuerza bruta.

Durante el análisis realizado al servidor SAProuter 172.18.20.17 se concluye que:

- El inconveniente de hostname ya no se presenta
- Al tratar de encontrar evidencia de ataques de fuerza bruta no fue posible ya que solo existen registros con fecha de 18/12/2019
- No se registran accesos como root posteriores al 13/12/2019 que es cuando la clave aparentemente funcionaba
- No fue posible determinar cambios en la clave del usuario root esto debido a que al reestablecer la clave se borró esta información

7 Recomendaciones

- Bloquear de manera urgente a nivel de perímetro la IP pública que estaba haciendo ataques de fuerza bruta.
- Reparar los archivos de configuración dañados.
- Para futuros reinicios o apagados de los equipos hacerlo de forma correcta para evitar problemas en el SO.
- En caso de que exista una situación similar tratar de sacar una copia de la maquina y no realizar modificaciones para no modificar o alterar evidencia.
- Se recomienda no entregar las credenciales de root, estas credenciales únicamente las debe manejar gerencias.
- Se debe entregar perfiles con permisos de root con previa validación de las necesidades de cada usuario.
- Se recomienda bloquear a nivel de perímetro por países que no sean necesarios que consuman servicios de la Alcaldía de Cali
- Validar que el puerto SSH no se encuentre publicado al mundo

8 Proyectos Futuros

De acuerdo a los resultados obtenidos se recomienda tener en cuenta la ejecución de los siguientes proyectos para mejorar la seguridad de infraestructura y procesos.

ID PROYECTO	Proyectos	Producto / Servicio	Documentación	Normativa	Indicadores	Mejora Continua
P01	Implementación de Correlación de Eventos	Herramienta de Correlación de eventos: Procesamiento de Logs. Monitoreo de Netflow. Monitoreo de disponibilidad de activos de red. Monitoreo de IDS.	1.- Manual de Operación. 2.- Informe de configuración. 3.- Información de capacitación.	1.- Política de Monitoreo y análisis. 2.- Política de Respuesta a Incidentes de Seguridad de Información.	Alarmas de seguridad establecidas por los atacantes.	Revisiones periódicas de cumplimiento en el comité de seguridad de información
P02	Gestión de contraseñas seguras	Implementación de protocolos de contraseñas seguras en todos los sistemas críticos de la organización	1.- Informe de configuración. 2.- Repositorio de Gestión de Cambios Información de capacitación.	1.- Política de gestión de usuarios. 2.- Política de contraseñas. 3.- Política de Auditoría.	Vulneración de contraseñas de usuario en la Dark web.	Revisiones periódicas de cumplimiento en el comité de seguridad de información
P03	Implementar doble factor de autenticación para acceso a sistemas críticos	Implementar una herramienta de doble factor de autenticación que permita mitigar el riesgo de acceso a sistemas críticos de personal no autorizado	1.- Manual de Operación Informe de configuración. 2.- Repositorio de Gestión de Cambios Información de capacitación.	1.- Política de gestión de usuarios. 2.- Política de contraseñas. 3.- Política de Auditoría.	Vulneración de credenciales de usuarios en la Dark Web.	Revisiones periódicas de cumplimiento en el comité de seguridad de información
P04	Gestionar la política de clasificación de información y seguridad de información sensible	Política de clasificación de información	1.- Proceso de clasificación. 2.- Matriz de información clasificada. 3.- Metodología de clasificación de información.	1.- Política de Clasificación de información. 2.- Política de Auditoría.	Informacion sensible expuesta en servicios en la nube	Revisiones periódicas de cumplimiento en el comité de seguridad de información
P05	Plan de formación y concientización	Implementar un plan de formación periódico de conceptos y prácticas de seguridad de información	1.- Manual de Operación. 2.- Información de capacitación.	1.- Política de capacitaciones en Seguridad de Información.	Indicadores de malas prácticas de seguridad detectados	Revisiones periódicas de cumplimiento en el comité de seguridad de información

Tabla 1. Proyectos recomendados en función de la investigación realizada.