EN LO PRINCIPAL : QUERELLA

PRIMER OTROSÍ : PROPONE DILIGENCIAS

SEGUNDO OTROSI : NOTIFICACIÓN

TERCER OTROSÍ : PERSONERIA

CUARTO OTROSÍ : PATROCINIO Y PODER

SR. JUEZ DE GARANTÍA DE SANTIAGO (1°)

FELIPE FERNÁNDEZ GONZÁLEZ, cédula nacional de identidad número quince millones setecientos diecinueve mil cuatrocientos sesenta y seis guion seis, y **ANAHÍ CANE CHARPENTIER**, cédula nacional de identidad número [redacted] representación de **ATACAMA MINERALS CHILE S.C.M**, todos domiciliado para estos efectos en Avenida Presidente Riesco 5435, piso 8, Las Condes, Santiago, con todo respeto digo:

Que de conformidad a lo dispuesto en los artículos 53, 109 letra b), 111 y 113 del Código Procesal Penal, venimos en interponer Querella Criminal fundada en la comisión de los hechos delictuales que se detallan más adelante, tipificados en los artículos 1 y 3 de la Ley 19.223 que Tipifica Figuras Penales Relativas a la Informática, en contra de **TODOS QUIENES RESULTEN RESPONSABLES** de la comisión de los referidos delitos por la afectación de la información de propiedad de Atacama Minerals Chile S.C.M contenida en el sistema de gestión de información contable ERP SAP B1, solicitando así admitirla a tramitación y enviar los antecedentes al Ministerio Público a fin de que se dé curso a la investigación, en base a los fundamentos de hecho y de derecho que pasamos a exponer.

Para un adecuado orden en nuestra exposición hemos estructurado esta presentación en los siguientes capítulos:

I. ANTECEDENTES PRELIMINARES

A. Actividades y operaciones comerciales de la Querellante

B. Operaciones administrativas

II. LOS HECHOS

III. INFORMACIÓN CONTENIDA EN SISTEMA SAP

IV. INFORME REALIZADO POR LA EMPRESA JAG

V. ANTECEDENTES DE DERECHO

A. Contexto actual en materia de ciberseguridad y ataques cibernéticos

B. Calificación Jurídica

C. Jurisprudencia

VI. PARTICIPACIÓN E ITER CRIMINIS.

VII. CONCLUSIONES.

El desarrollo de los capítulos antes señalados es el que pasamos a exponer detalladamente a continuación.

I. ANTECEDENTES PRELIMINARES

A. Actividad y operaciones comerciales de la Querellante:

ATACAMA MINERALS CHILE S.C.M (en adelante "la Querellante" o "la Empresa"), es una *Sociedad Contractual Minera*.

Actualmente, la Querellante concentra sus operaciones en el desierto de Atacama, en el norte de nuestro país, donde posee el 100% del depósito de yodo, sulfatos y nitratos en dos dominios del yacimiento salitrero de Aguas Blancas, en la comuna de Antofagasta.

Debido a su exitosa gestión, ya en el año 2007 la Querellante había incrementado a un total de 24,6 millones de toneladas las reservas probadas y probables ubicada en Aguas Blancas, lo que implicó un aumento cercano al 20% desde las estimaciones de producción que se habían hecho en junio de 2005.

Debido a su éxito, la Querellante se encuentra en un período de expansión de su producción de yodo y, además, continua con la realización de estudios de investigación para la exploración de nitratos.

Hacemos presente que, si bien su actividad industrial se encuentra concentrada en el norte de Chile, cuenta con sus oficinas en la ciudad de Santiago, en la comuna de Las Condes, desde donde dirige sus operaciones.

Esto es relevante al tenor de lo que se expondrá en las secciones siguientes, ya que se relaciona con la determinación del tribunal competente para conocer sobre estos hechos.

B. Operaciones administrativas:

La Querellante desarrolla parte de sus operaciones administrativas utilizando un sistema de información contable llamado ERP SAP B1, el cual le permite llevar un registro de su contabilidad, operaciones de tesorería, compras, entre otros.

Así, este sistema permite un mejor manejo y control de dicha información para generar una planificación empresarial eficiente. Más adelante en esta presentación explicaremos el funcionamiento y la relevancia de la información de propiedad de la Querellante contenida en el sistema en cuestión.

Además, la Querellante cuenta con el arriendo de un Rack (estructura que alberga los dispositivos de operación), en un Datacenter perteneciente a la compañía Entel, **desde donde puede operar sus distintos sistemas destinados a la administración de datos, tales como el sistema ERP SAP B1 antes mencionado**.

Esta red de Datacenter se encuentra ubicada en Los Vientos N°22043, comuna de Pudahuel, Ciudad de los Valles, Santiago, Región Metropolitana.

II. LOS HECHOS

El sábado 15 de enero del 2022, aproximadamente a las 17:00 horas, el testigo Luis Llanos Vásquez, IT Manager de la Querellante, recibió un llamado por parte de la testigo Paola Andaur Silva, Invoice Controller y miembro del Departamento de Finanzas, indicándole que al intentar ingresar al sistema ERP SAP B1, vía remota y a través de una red privada virtual ("VPN", por las siglas en inglés de *virtual private network*), detectó una *anomalía*.

Unas horas más tarde, aproximadamente a las 19:00 horas del mismo sábado 15 de enero del año en curso, Luis Llanos Vásquez ingresó a los sistemas de la Empresa y revisó el estado de los mismos, como también de las bases de datos, percatándose de que la información disponible en los sistemas ERP SAP B1, Active Directory, File Server y también del servidor de respaldo, **habría sido *encriptada*, esto es, cifrada en términos tales que no era posible acceder a la información de la Empresa disponible en el sistema en cuestión**, salvo que se contara con un determinado algoritmo.

Hacemos presente que los archivos e información que fueron afectados corresponden al Departamento de Finanzas de la Querellante, y se relacionan con documentos contables hasta el mes de diciembre del 2021, copias de facturas emitidas y recibidas, base de datos del sistema de información SAP, copias digitalizadas de escrituras y extractos de información legal de la Empresa, como también variados documentos, reportes y presentaciones del área contable y financiera.

Adicionalmente, la Querellante detectó, aproximadamente 5 horas después del incidente, **un archivo con un mensaje para que se comunicaran con quien sería**

el responsable del ataque cibernético y recibir, a cambio de un pago en moneda Bitcoins, los algoritmos para desencriptar nuestra información.

Es muy importante hacer presente que la Querellante **no tomó contacto ni realizó pago alguno para estos efectos**.

Enseguida, Luis Llanos Vásquez se puso en contacto con la empresa VZOR, la cual presta servicios a la Querellante respecto del soporte y monitoreo del Datacenter ubicado en Los Vientos N°22043, comuna de Pudahuel, para solicitar el **aislamiento** de toda la red corporativa y evitar así que el ataque sufrido se propagara por las demás redes. Afortunadamente para los intereses y continuidad operacional de la Empresa, el aislamiento fue exitoso, no extendiéndose el *ransomware* a otros activos de la organización.

Posteriormente, el testigo realizó un llamado telefónico a la empresa *JAG Cybersecurity Innovation* (en adelante e indistintamente "JAG"), especialistas en asuntos relacionados con ciberseguridad, para solicitar un análisis detallado de lo ocurrido lo que se traduciría, finalmente, en la elaboración de un informe con el detalle del ciberataque.

De esa forma, JAG concluyó en su informe que **el ataque se habría producido mediante el ingreso de un *host* identificado con la IP 94.232.41.216, los días 12 y 15 de enero del 2022, afectando los sistemas de almacenamiento de información contable de la Querellante a través de un archivo ejecutable con el nombre "nevmot.exe"**.

Más adelante, en la sección IV se analizará en detalle el informe realizado por esta empresa, el que se acompañará oportunamente en esta investigación.

Finalmente, los efectos de esta afectación a la información de la Empresa produjeron la imposibilidad de utilizar la información contable almacenada y operada a través de los sistemas de la Querellante.

III. INFORMACIÓN CONTENIDA EN EL SISTEMA SAP

La información afectada por el ataque informático que sufrió la Querellante es **clave para el funcionamiento de cualquier compañía**.

Y no podría ser de otra manera, si se tiene en consideración que dicha **información de carácter contable y financiera es procesada a través del sistema informático SAP**, un sistema consistente en un software de planificación de recursos empresariales (o ERP por la sigla en inglés del término "*Enterprise Resource Planning*") que integra básicamente a todas las áreas de una empresa, controlando las funciones operativas y administrativas de una organización.

En términos sencillos, SAP es uno de los ERP más conocidos no solo en Chile, sino que, también utilizado por muchas empresas en el extranjero, y de acuerdo a la información publicada por esta compañía, SAP de hecho tiene más de 230 millones de usuarios solo considerando en la nube y más de 100 soluciones que cubren todas las funciones de negocio y la cartera de productos en la nube más grande de todos los proveedores.

La **transversalidad del funcionamiento de este tipo de soluciones informáticas es clave en el día a día de una empresa como lo es la del Querellante**.

En este contexto, un software de ERP incluye programas para prácticamente todas las áreas de negocio centrales de una organización, tales como compras, producción, gestión de materiales, ventas, marketing, finanzas y recursos humanos, entre otras.

Si tuviéramos que explicar de forma simple y breve qué hace este sistema informático, creemos que lo siguiente ilustra adecuadamente lo anterior[1]:

> Los modelos de negocio tradicionales a menudo descentralizan la gestión de datos, y cada función de negocio almacena sus propios datos operativos en una base de datos

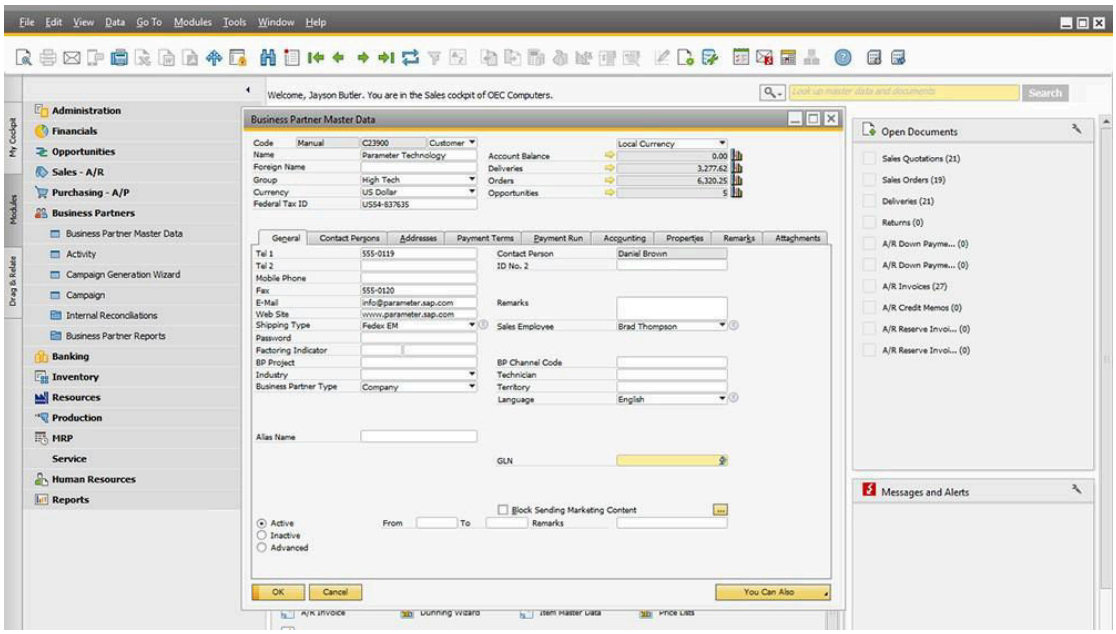
[1] Ver www.sap.com/latinamerica/about/company/what-is-sap.html.

separada. Esto dificulta el acceso de los empleados de diferentes funciones de negocios a la información de los demás. Además, la duplicación de datos entre múltiples departamentos aumenta los costos de almacenamiento de TI y el riesgo de errores en los datos.

Al centralizar la gestión de datos, el software de SAP brinda múltiples funciones de negocio con una única visión de la verdad. Esto ayuda a las empresas a gestionar mejor los procesos de negocio complejos dándoles a los empleados de diferentes departamentos un acceso fácil a información en tiempo real en toda la empresa. Como resultado, las empresas pueden acelerar los flujos de trabajo, mejorar la eficiencia operativa, aumentar la productividad, mejorar las experiencias de cliente y, en última instancia, aumentar los beneficios.

Ahora bien, en el caso de la Querellante, la versión del software donde se almacenaba la información afectada por el ataque cibernético es el que comercialmente se conoce como **SAP Business One o SAP B1**, que para los efectos de la investigación cuyo inicio se requiere en esta presentación cumple con finalidades y objetivos similares a los expuestos anteriormente en este capítulo.

Para fines meramente ilustrativos, la siguiente imagen corresponde a la interfaz de usuario del programa utilizado por la Querellante:



¿Por qué es tan importante para la Querellante la información afectada por el ataque cibernético?

Como se expuso anteriormente, la información de la Querellante no disponible en la actualidad contiene antecedentes contables y financieros que impactan el normal y periódico funcionamiento de la organización.

Lo anterior no solo es importante en el día a día de las operaciones de la Querellante, sino que además obliga a la Empresa a realizar **esfuerzos adicionales** para, por ejemplo, **poder proporcionar información de carácter económico a organismos nacionales competentes** como por ejemplo podría serlo el Servicio de Impuestos Internos.

En síntesis, el ataque en cuestión afectó no solo el ordinario funcionamiento de los negocios de la Querellante, sino que además impuso cargas adicionales en lo que dice relación con el cumplimiento de deberes normativos.

IV. INFORME REALIZADO POR LA EMPRESA JAG

La Querellante contrató en enero del 2022, los servicios de la empresa JAG, para que realizara una auditoria respecto del funcionamiento de sus sistemas de administración de información.

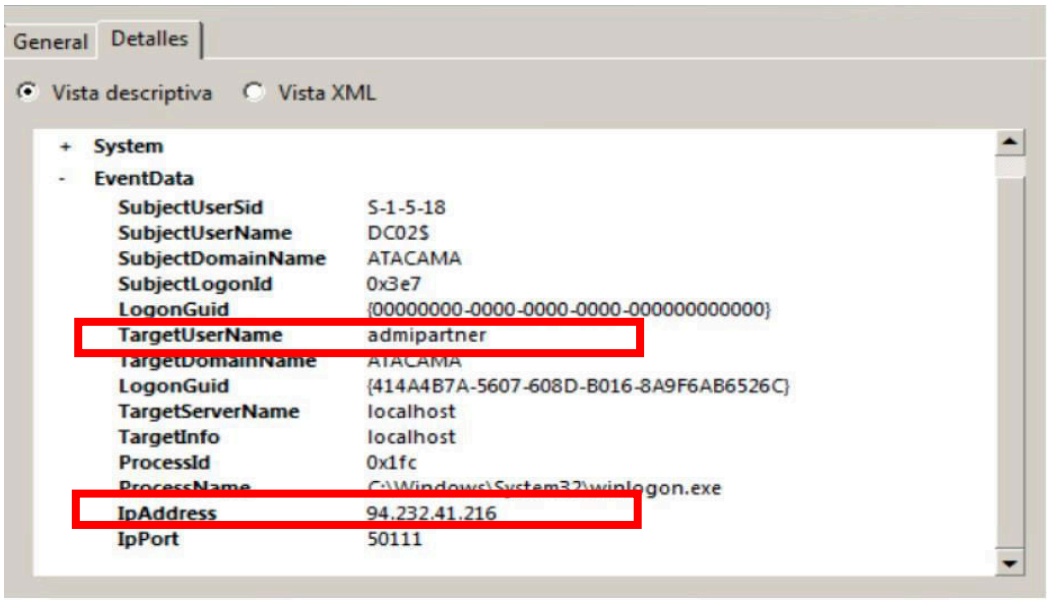
En dicha oportunidad y con ocasión de la revisión, JAG detectó una **vulneración en los sistemas de la Empresa que impedía acceder a la información contable de propiedad de la Querellante**, lo que afectó (hasta la fecha), la posibilidad de recuperar y utilizar la información en cuestión.

En virtud de la investigación y auditoría realizada por la empresa JAG, esta concluyó que entre los días 12 y 15 de enero del 2022, un host identificado con la **IP**

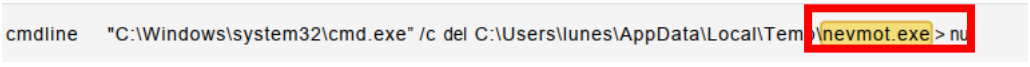
0x001a2555	admipartner	ATACAMA	DC02.ATACAMA.STGO	16-01-2022 3:24:30			10.0.9.10	Unlock (7)
0x97fabbdf	admipartner	ATACAMA	DC02.ATACAMA.STGO	12-01-2022 13:07:20			94.232.41.216	Remote Interactive (10)
0x98268404	admipartner	ATACAMA	DC02.ATACAMA.STGO	12-01-2022 15:27:38			94.232.41.216	Remote Interactive (10)
0x9d9f2371	admipartner	ATACAMA	DC02.ATACAMA.STGO	15-01-2022 13:11:55			94.232.41.216	Remote Interactive (10)
0x9da7e9d3	admipartner	ATACAMA	DC02.ATACAMA.STGO	15-01-2022 13:25:31			192.168.10.3	Remote Interactive (10)
0x9dd80511	admipartner	ATACAMA	DC02.ATACAMA.STGO	15-01-2022 16:03:15			94.232.41.216	Unlock (7)
0x9df5c0df	admipartner	ATACAMA	DC02.ATACAMA.STGO	15-01-2022 18:04:00			94.232.41.216	Remote Interactive (10)
0x9e391b40	admipartner	ATACAMA	DC02.ATACAMA.STGO	15-01-2022 22:38:57			127.0.0.1	Interactive (2)

94.232.41.216, y utilizando el nombre de usuario *"admipartner"*, realizó distintos ingresos vía remota, lo cual se detalla en la siguiente imagen:

El mismo nombre de usuario y dirección IP se observa en la siguiente imagen:



Como se mencionó anteriormente, la afectación de los sistemas se realizó mediante **un *ransomware* de fácil propagación con el nombre *"nevmot.exe"***, el cual habría logrado el acceso a través de un método de **descubrimiento forzoso** de una de las cuentas de usuario de la Querellante que contaba con privilegios de administrador.



De esta forma, dicho *ransomware* de nombre "nevmot.exe" se fue propagando por los distintos directorios y carpetas compartidas, **logrando la encriptación de parte del contenido relacionado con la administración contable y financiera de la Querellante**.

Un dato interesante de la auditoría de esta empresa fueron ciertos cambios en la ejecución del *ransomware* con posterioridad a los días 12 y 15 de enero según dan cuenta las siguientes, y por vía meramente ilustrativa, imágenes:

- Imagen 1

cmdline	"C:\Windows\system32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" cd %userprofile%\documents\ attrib Default.rdp -s -h del Default.rdp for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
cmdline	C:\Windows\System32\cmd.exe /c del C:\Users\lunes\AppData\Local\Temp\nevmot.exe > nul
cmdline	"C:\Windows\system32\cmd.exe" /c del C:\Users\lunes\AppData\Local\Temp\nevmot.exe > nul
cmdline	C:\Windows\System32\cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" cd %userprofile%\documents\ attrib Default.rdp -s -h del Default.rdp for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"

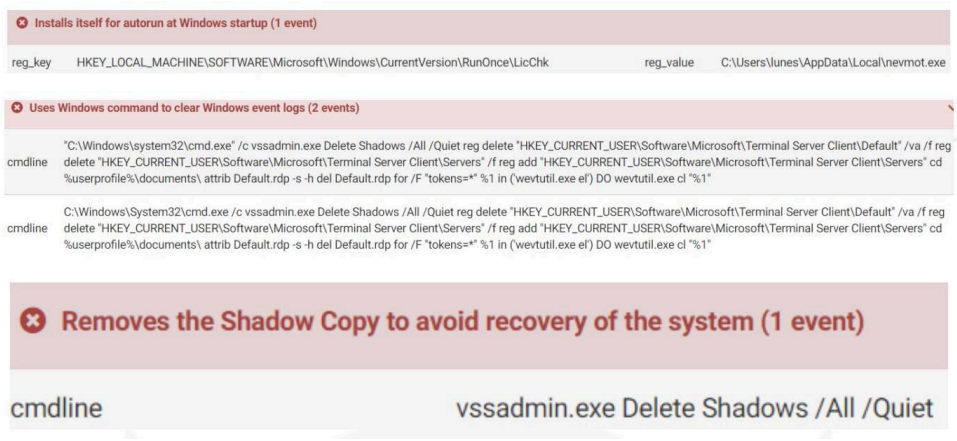
- Imagen 2

ShellExecuteExW Jan. 18, 2022, 5:02 a.m.	show_type: 0 filepath_r: C:\Windows\system32\cmd.exe parameters: /c vssadmin.exe Delete Shadows /All /Quiet reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" cd %userprofile%\documents\ attrib Default.rdp -s -h del Default.rdp for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1" filepath: C:\Windows\System32\cmd.exe
ShellExecuteExW Jan. 18, 2022, 5:03 a.m.	show_type: 0 filepath_r: C:\Windows\system32\cmd.exe parameters: /c vssadmin.exe Delete Shadows /All /Quiet reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" cd %userprofile%\documents\ attrib Default.rdp -s -h del Default.rdp for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1" filepath: C:\Windows\System32\cmd.exe
ShellExecuteExW Jan. 18, 2022, 5:03 a.m.	show_type: 0 filepath_r: C:\Windows\system32\cmd.exe parameters: /c del C:\Users\lunes\AppData\Local\Temp\nevmot.exe > nul filepath: C:\Windows\System32\cmd.exe

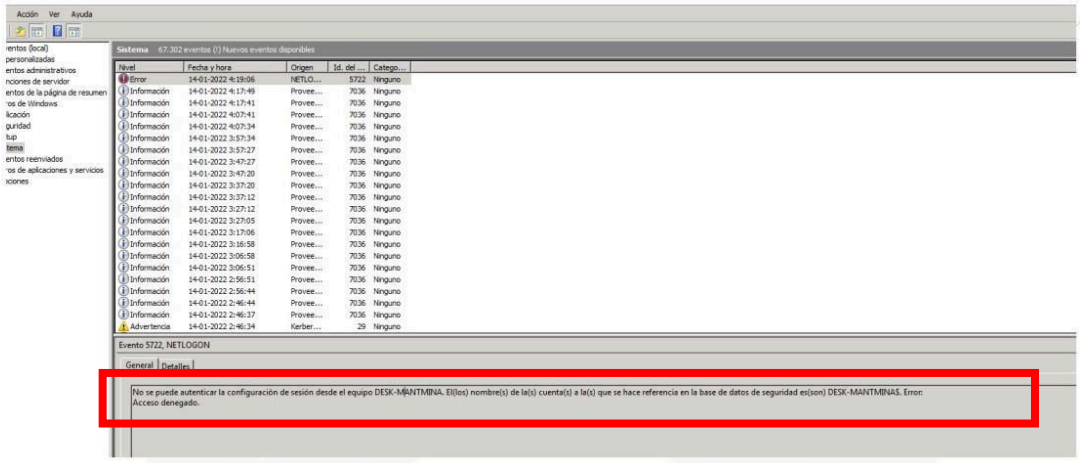
- Imagen 3

cmdline	"C:\Windows\system32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" cd %userprofile%\documents\ attrib Default.rdp -s -h del Default.rdp for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
cmdline	C:\Windows\System32\cmd.exe /c del C:\Users\lunes\AppData\Local\Temp\nevmot.exe > nul
cmdline	"C:\Windows\system32\cmd.exe" /c del C:\Users\lunes\AppData\Local\Temp\nevmot.exe > nul
cmdline	C:\Windows\System32\cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" cd %userprofile%\documents\ attrib Default.rdp -s -h del Default.rdp for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"

- Imagen 4



Por otra parte, la auditoría de JAG además detectó situaciones anómalas como intentos de autenticación fallida del usuario "*desk-mntmina*", no siendo descartable, como se señaló anteriormente, que el ingreso del *ransomware* haya sido el resultado de la aplicación del método de descubrimiento forzoso de una cuenta de usuario con privilegios de administrador, según da cuenta la siguiente imagen:



Finalmente, y como se anticipó, la conclusión del informe de auditoría realizado por esta empresa concluye que los datos asociados al autor del ataque cibernético son los siguientes:

Reiteramos que el informe realizado por la empresa JAG será oportuna y debidamente acompañado a la investigación que se inicie con ocasión de la presente querella.

V. ANTECEDENTES DE DERECHO

A. Contexto actual en materia de ciberseguridad y ataques cibernéticos:

Como será de conocimiento de S.S, los ataques cibernéticos o informáticos lamentablemente han tomado protagonismo en los últimos años, siendo relativamente frecuente tener noticias sobre este tipo de delitos que afectan no solo a particulares, sino que también a entidades gubernamentales.

Esto ha motivado a que diferentes actores del exosistema legal chileno hayan realizado esfuerzos en orden a mejorar las herramientas legales para enfrentar frente, investigar y condenar a los responsables de este tipo de delitos.

Ejemplos de lo anterior hay muchos, pero destacan por ejemplo lo siguientes:

(i) *Proyecto de Ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información:*

Este proyecto de ley (boletín 14847-06) ingresado al Senado en marzo pasado reconoce la relevancia de la ciberseguridad tanto en el sector

público como privado, señalando en su Mensaje lo siguiente respecto a las finalidades del proyecto en cuestión[2]:

> Se prevendrán ciberamenazas al mejorar las instancias de comunicación, coordinación y colaboración entre diversas instituciones, organizaciones y empresas, tanto del sector público como privado, nacionales e internacionales, con el propósito de fortalecer la confianza y entregar una respuesta común a los riesgos que se presentan en el ciberespacio, previniendo el fenómeno del ciberataque y evitando la expansión de los efectos perjudiciales de un incidente de ciberseguridad. Lo anterior, debido a que la prevención de los delitos informáticos es distinta a la prevención de los delitos tradicionales, principalmente por factores como la motivación delictiva, las formas sofisticadas y las capacidades técnicas necesarias para su comisión.
>
> Se gestionarán los riesgos del ciberespacio, lo que permitirá identificar las vulnerabilidades, amenazas y riesgos en el uso, procesamiento, almacenamiento y transmisión de la información. En virtud de lo anterior, se procurará generar las capacidades para la prevención, mitigación, la efectiva y pronta recuperación ante incidentes de ciberseguridad que afecten a instituciones que posean infraestructura crítica de la información, conformando un ciberespacio seguro, estable y resiliente.

Lo anterior se recoge en el artículo *1. Objeto* del proyecto de ley en comento, donde se dispone lo siguiente[3]:

> Establecer la institucionalidad, los principios y la normativa general que permiten estructurar, regular y coordinar las acciones de ciberseguridad de los órganos de la Administración del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los órganos del Estado así como los deberes de las instituciones privadas que posean infraestructura de la información calificada como crítica y, en ambos casos, los

[2] Disponible en https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06.
[3] Ibidem.

> mecanismos de control, supervisión, y de responsabilidad por la infracción de la normativa

Este proyecto de ley, entre otras cosas, propone la creación de una nueva institucionalidad para hacerse cargo de la ciberseguridad, destacando la creación de la Agencia Nacional de Ciberseguridad y de los diversos Equipos de Respuesta a Incidentes de Seguridad Informática (o "CSIRTs"), los cuales se organizarían por área ya sea privadas o del sector público.

(ii) *Proyecto de Ley que establece Normas sobre Delitos Informáticos, Deroga la Ley N° 19.223 y modifica otros Cuerpos Legales con El Objeto De Adecuarlos al Convenio de Budapest:*

Otro proyecto de ley muy ligado a los hechos que motivan esta presentación, y que a la fecha de la presente querella fue aprobado por el Congreso y probablemente sea promulgado en el muy breve plazo, tiene dentro de sus principales objetivos adecuar la normativa actual en materia de delitos informáticos para para alcanzar el tratado internacional Convenio sobre la Ciberdelincuencia del Consejo de Europa también conocido como Convenio de Budapest (Boletín N° 12.192-25[4]). Conforme al Mensaje del proprio proyecto de ley, la relevancia de dicho convenio radica en lo siguiente[5]:

> En estos términos, el principal objetivo del Convenio es el desarrollo de una política criminal común frente a la ciberdelincuencia, mediante la homologación de los conceptos fundamentales y del tratamiento de la legislación penal,

[4] Disponible en https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=12192-25.
[5] Ibidem.

> sustantiva y procesal, así como del establecimiento de un sistema rápido y eficaz de cooperación internacional.
>
> Nuestro país promulgó el Convenio a través del Decreto Nº 83 del Ministerio de Relaciones Exteriores, con fecha 27 de abril del 2017, entrando posteriormente en vigencia el 28 de agosto del mismo año. En ese orden de ideas, el contenido del mismo y los compromisos internacionales adquiridos por nuestro país –sin perjuicio de las reservas hechas en su oportunidad- se han vuelto mandatorios.
>
> Lo anterior tiene lugar en un mundo globalizado, en el cual Chile no se encuentra ajeno a este fenómeno criminal, unido al aumento del acceso a Internet y otros dispositivos electrónicos, de modo que resulta indispensable una actualización a nuestra legislación en esta materia.

> Dentro de las principales novedades de este proyecto se encuentran la adición de ciertos tipos penales en materia de delitos informáticos, así como la consagración de ciertas facultades otorgadas al Ministerio Público para poder perseguir eficazmente este tipo de delitos.

Lo anteriormente expuesto a propósito de ambos proyectos de ley tiene por objetivo dar cuenta de la **importancia que actualmente tiene la ciberseguridad y los delitos informáticos en nuestro país**, con el fin de visibilizar la gravedad de los delitos de los que fue víctima la Querellante.

B. Calificación jurídica:

Ahora bien, en el contexto del delito informático del que fue víctima la Querellante, los hechos en cuestión son efectivamente **constitutivos de los delitos informáticos tipificados en los artículos 1 y 3 de la Ley de Delitos Informáticos**.

En este sentido, de conformidad a lo dispuesto en el artículo 1 de la referida ley:

> Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o **impida, obstaculice o modifique su funcionamiento**, sufrirá la pena de presidio menor en su grado medio a máximo.
> Si como consecuencia de estas conductas **se afectaren los datos contenidos en el sistema**, se aplicará la pena señalada en el inciso anterior, en su grado máximo.
>
> [Énfasis agregado]

En el presente caso, se ha **impedido y/u obstaculizado y/o modificado el correcto funcionamiento del sistema informático utilizado por la Querellante, lo que adicionalmente a afectado los datos financieros y contables contenidos en el sistema en cuestión**, lo que agrava el delito debiendo ser sancionado con presidio menor en su grado máximo.

Por su parte, el artículo 3 de la Ley de Delitos Informáticos dispone que:

> Artículo 3°.- El que maliciosamente **altere, dañe o destruya los datos** contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.
>
> [Énfasis agregado]

El referido artículo también es aplicable a los hechos cuya investigación se investiga, teniendo presente que **datos financieros y contables de la Querellante** han sido **alterados y/o dañados** en términos tales que los mismos no son accesibles para la Empresa, causando los problemas y consecuencias negativas que ya se han expuesto en esta presentación.

En ambos casos el **dolo y actuar malicioso** del autor del delito queda en evidencia con la exigencia de realizar un **pago** por liberar la información objeto del ataque cibernético.

C. Jurisprudencia:

En cuanto al bien jurídico protegido por la Ley de Delitos Informáticos las decisiones de los tribunales chilenos han reconocido que el mismo dice relación con la calidad, pureza e idoneidad de la información en cuanto tal y de los productos que de ella se obtengan.

Algunos ejemplos de la jurisprudencia en cuestión son los siguientes:

- *Tribunal Oral en lo Penal de Curicó (Ruc 0910014546-1)*

> "Se debe tener presente que la ley 19.223 lo que protege es la información de los datos contenidos en las redes informáticas y lo que se pretende con su aplicación es la constitución de un bien jurídico nuevo cual es "la calidad, pureza e idoneidad de la información" (Hernán Silva Silva) y así de algún modo impedir que dichos sistemas sean burlados para obtener beneficios tales como apropiación, uso o conocimiento de la información en ellos contenida para fines propios y diversos a aquellos para los cuales fueron creados o generados".

- *Juzgado de Garantía de Concepción (Ruc 1410003541-4)*

> "(…) al alero de nuestra deficiente legislación en materia de delitos informáticos, lo que se ha afectado como bien jurídico protegido es la información, pues conforme a la historia de la Ley 19.223, el autor de la moción que la origina, diputado Antonio Viera Gallo, fundamentando su propuesta señala que el propósito que se persigue es proteger la calidad, pureza e idoneidad de la información contenida en un sistema automatizado de tratamiento de la misma, y los productos que de su operación se obtengan, opinión sostenida por el autor Hernán Silva en su libro "Las Estafas, Doctrina, Jurisprudencia y Derecho Comparado", Editorial Jurídica, páginas 214 y siguientes (sobre la criminalidad informática v. también la obra de Manuel Jaén Vallejo, Estudios Penales, Editorial Lexis Nexis, páginas 136 y siguientes)".

- *Corte de Apelaciones de Concepción (Rol 844-2014).*

> 6.- (…) La acción delictiva está destinada a alterar, destruir o dañar los datos contenidos en un sistema de tratamiento de información. Alterar los datos contenidos en un sistema sería, en consecuencia, alteraciones conductas como el ingreso o introducción de datos erróneos, el borrado de datos verdaderos, transformaciones o desfiguraciones de los datos, y en general toda conducta que implique cambiar la información contenida en un sistema de tratamiento de la misma sin destruirla. Por lo tanto, lo afectado es el sentido, veracidad, claridad o pureza y alcance de la información contenida, la cual se verá afectada con conductas como las descritas.
>
> 7.- Que la sentencia recurrida en el motivo 8 se refiere al bien jurídico protegido señalando que "…este ilícito fue introducido por el cuerpo legal citado y, tal como se dejó constancia en sus diversos trámites legislativos, el bien jurídico a proteger por tal tipo penal es la calidad, pureza e idoneidad de la información, contenida en los sistemas automatizados de tratamiento de la misma, así como los productos provenientes de la operación de dichos sistemas. (Primer Trámite Constitucional, Moción Parlamentaria, Pág. 4; Primer Trámite Constitucional, Discusión en Sala, Pág. 38 y 47; Segundo Trámite Constitucional, Segundo Informe de Comisión de Constitución, Pág. 77).
>
> 8.- Que tal como se señaló precedentemente, en la hipótesis del artículo 3° de la ley mencionada, el bien jurídico tutelado es el sentido, veracidad, claridad o pureza de la información. Así lo señalan los autores Rodrigo Medina Jara, en su artículo Los delitos Informáticos en la Legislación Chilena, publicado en Revista Electrónica de Derecho Informático, N°44, marzo 2002; los autores Marcelo Huerta y Claudio Líbano, en su obra Delitos Informáticos, Editorial Jurídica; Alejandro Vera Quilodrán en Delito e Informática, etc.
>
> En el caso sub litis puede decirse, propiamente, que el bien jurídicamente protegido es colectivo y se traduce en la información como valor económico de la actividad de la empresa. Distinto ocurre en el fraude informático, en que el verdadero bien a cautelar es el patrimonio, ya que el interés general en el adecuado funcionamiento del tratamiento electrónico de datos, de creciente importancia para la

> economía y la administración, resulta protegido sólo en forma refleja. (Nelson Pozo Silva, La tecno-estafa o la estafa informática, Gaceta Jurídica N°245, pág.10 y ss.)".

Las sentencias anteriores dan cuenta de que la información de la Querellante afectada por el delito informático cuya investigación se requiere corresponde precisamente al bien jurídico tutelado por los artículos transcritos en el apartado anterior de esta sección.

VI. PARTICIPACIÓN E ITER CRIMINIS

Para efectos de determinar la participación e iter criminis se debe estar a lo dispuesto en los artículos 7 y 15 del Código Penal.

En este contexto, el artículo 7 del referido cuerpo legal dispone lo siguiente:

> ART. 7.
> Son punibles, no sólo el crimen o simple delito consumado, sino el frustrado y la tentativa.
> Hay crimen o simple delito frustrado cuando el delincuente pone de su parte todo lo necesario para que el crimen o simple delito se consume y esto no se verifica por causas independientes de su voluntad.
> Hay tentativa cuando el culpable da principio a la ejecución del crimen o simple delito por hechos directos, pero faltan uno o más para su complemento.

Por su parte, el artículo 15 del Código Penal establece:

> ART. 15.
> Se consideran autores:
> 1.° Los que toman parte en la ejecución del hecho, sea de una manera inmediata y directa; sea impidiendo o procurando impedir que se evite.
> 2.° Los que fuerzan o inducen directamente a otro a ejecutarlo.
> 3.° Los que, concertados para su ejecución, facilitan los medios con que se lleva a efecto el hecho o lo presencian sin tomar parte inmediata en él.

Teniendo presente las disposiciones anteriores, a los querellados les cabe responsabilidad en calidad de **autores en los delitos denunciados**, en grado de **consumado**.

VII. CONCLUSIONES

Lo expuesto en esta presentación da cuenta de una situación **extremadamente grave** como lo fue el ataque cibernético del que fue víctima la Querellada.

Como vimos la afectación de información financiera y contable de la Empresa no solo **el normal curso de sus actividades comerciales**, sino que incluso podría incluso llegar a **dificultar el cumplimiento de deberes u obligaciones de índole normativo**.

En este contexto, la **Ley de Delitos Informáticos sanciona específicamente actos de esta naturaleza**, en particular en lo dispuesto en sus artículos 1 y 3 a los que nos hemos referido con anterioridad. Así por lo demás lo han ratificado las sentencias de tribunales a propósito de hechos que han afectado la información de sus respectivos titulares.

En definitiva, solicitamos que se investigue, identifique y condene a los autores de un delito lamentablemente cada vez más recurrente en Chile, pero que nuestro ordenamiento jurídico sanciona con dureza dado teniendo presente la relevancia del bien jurídico tutelado.

POR TANTO;

En mérito de lo expuesto, de las disposiciones legales citadas y demás disposiciones legales aplicables;

A S.S. PIDO se sirva tener por interpuesta querella en contra de **TODOS QUIENES RESULTEN RESPONSABLES** por los delitos tipificados en los artículos 1 y 3 de la

Ley 19.223 que Tipifica Figuras Penales Relativas a la Informática, ordenando enviar los antecedentes al Ministerio Público a objeto de iniciar la investigación tendiente a sancionar a todos los que resulten responsables al máximo de las penas que la ley contempla para estos delitos.

PRIMER OTROSÍ: A S.S. pido conforme lo dispone el artículo 113 letra e) del Código Procesal Penal tener presente que proponemos como diligencias de investigación las siguientes:

1. Se despache orden amplia de investigar por los hechos denunciados a la Brigada Investigadora del Cibercrimen de Santiago, al objeto de que investigue los hechos relatados y entre otras diligencias se efectúen las siguientes:

a) Se tome declaración [redacted] RUT: [redacted]

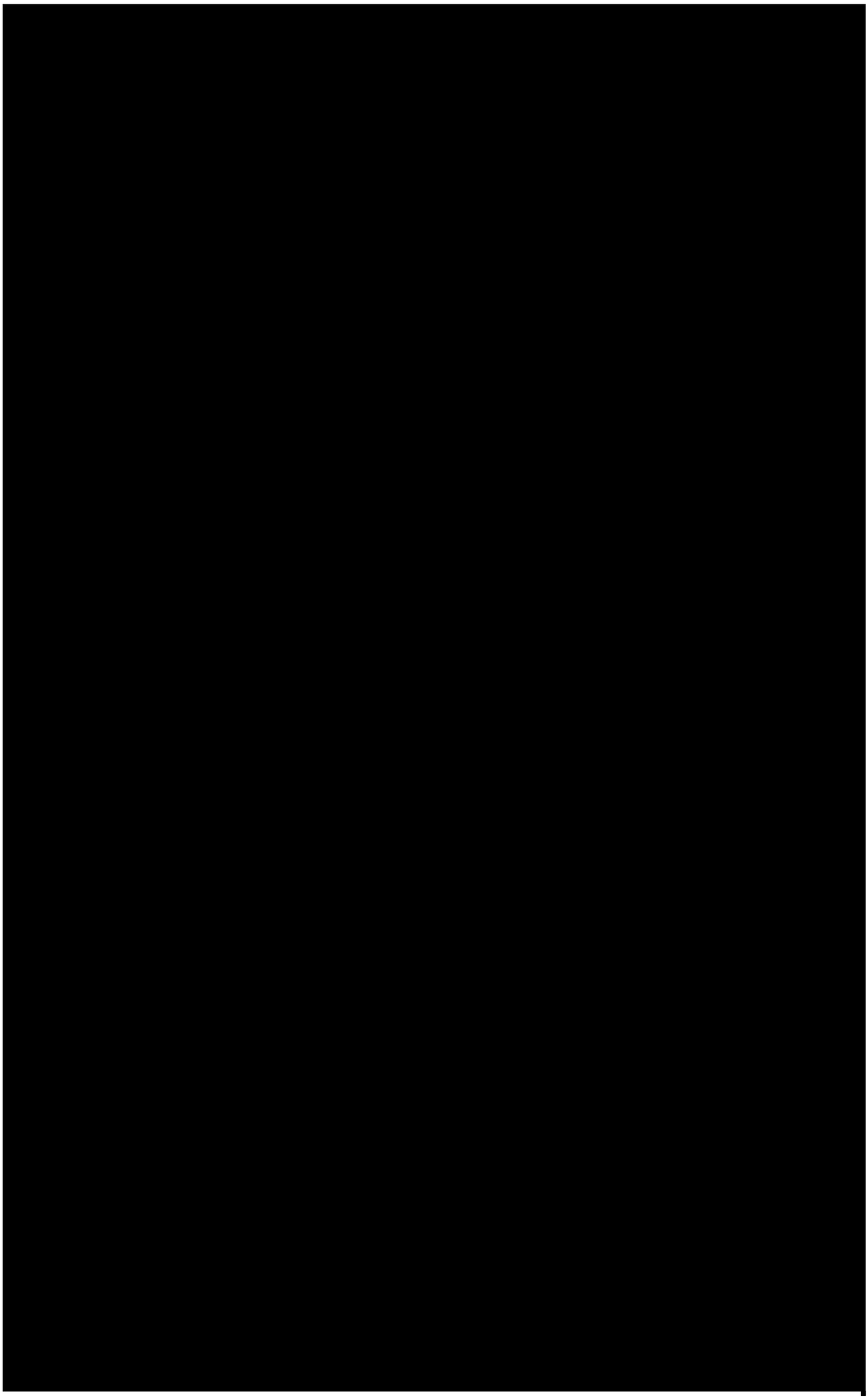
b) Se tome declaración al testigo [redacted]

c) Se tome declaración al testigo [redacted]

SEGUNDO OTROSÍ: A S.S. PIDO se sirva efectuar las notificaciones que correspondan a los siguientes correos electrónicos: [redacted]

<u>TERCER OTROSÍ:</u> Sírvase tener presente que nuestra personería para actuar en representación de ATACAMA MINERALS S.C.M. consta en mandato judicial autorizado ante Notario de fecha 30 de marzo del 2022, repertorio N° 3068-2022, el cual se acompaña a la presentación de la querella.

<u>CUARTO OTROSÍ</u>: Vengo en hacer presente a S.S., que en nuestra calidad de abogados habilitados para el ejercicio de la profesión nos reservamos el patrocinio y poder en estos autos.



Firmado digitalmente por:MARIA VIRGINIA WIELANDT COVARRUBIAS
Fecha: 01.04.2022 13:27 Razón: Notario Suplente
Ubicación: Santiago

[redacted]

[redacted]

Pag:

rtificado
3456856903
rifique validez
tp://www.fojas.