KIRKLAND & ELLIS

Informe a la Ciudad de Dallas Sobre el Incidente de la Pérdida de Datos en marzo de 2021

10 de febrero de 2022

Idioma predominante:
En caso de discrepancia entre la versión original en inglés de este informe y la traducción al español, prevalece la versión en inglés.
Prevailing Language:
In the event of any discrepancy between the English original version of this report and the Spanish language translation, the English version prevails.

Informe de Kirkland & Ellis LLP
a la Ciudad de Dallas sobre el Incidente de la Pérdida de Datos en marzo de 2021
10 de febrero de 2022

I. Resumen Ejecutivo

Este Informe está organizado en 12 secciones, comenzando con el alcance y la ejecución de nuestra Investigación, y de la siguiente manera:

- Describimos las políticas correspondientes que rigen la Ciudad de Dallas y la estructura de los departamentos correspondientes, así como los antecedentes técnicos relacionados con el Incidente de la Pérdida de Datos.

- A continuación, brindamos una descripción completa de los eventos que llevaron al Incidente de la Pérdida de Datos basado en entrevistas a testigos y documentos proporcionados por la Ciudad de Dallas.

- Luego proporcionamos un resumen detallado de las acciones y omisiones del técnico encargado de las copias de respaldo de ITS cuyo proceder causó el Incidente de la Pérdida de Datos, y la respuesta del personal de ITS y otros al evento.

- También analizamos los hallazgos relacionados con el origen del evento y otros factores sistémicos que se sumaron al posible impacto del Incidente de la Pérdida de Datos.

- Al final de este Informe, ofrecemos nuestras recomendaciones que se relacionan específicamente con los hallazgos de este Incidente de la Pérdida de Datos y, de manera más amplia, con los mayores problemas sistémicos que observamos durante esta Investigación.

A. Compromiso de Kirkland

Kirkland & Ellis LLP ("Kirkland") se comprometió el 1 de noviembre de 2021 (el "Compromiso") con la Ciudad de Dallas (la "Ciudad"), bajo la dirección del Concejo de la Ciudad de Dallas (el "Concejo de la Ciudad"), para llevar a cabo una investigación interna privilegiada e independiente (la "Investigación") sobre el Incidente de la Pérdida de Datos que ocurrió en la Ciudad a fines de marzo de 2021 y cerca de esa fecha (el "Incidente de la Pérdida de Datos"). En ese momento, la Ciudad informó que se habían perdido aproximadamente 22 terabytes de datos, posiblemente irrecuperables, y que la mayor parte de los datos posiblemente afectados estaban relacionados con el Departamento de Policía de Dallas (el "DPD") e incluían datos que constituían evidencia en juicios pendientes en la Oficina del Abogado del Distrito del Condado de Dallas (la “Oficina del Abogado del Distrito”).

De conformidad con nuestro Compromiso, contratamos a Stroz Friedberg LLC, una empresa Aon ("Stroz Friedberg"), para brindar servicios forenses. Nuestra Investigación involucró, entre otras cosas: (i) una revisión de documentos y datos puestos a disposición por los departamentos relevantes de la Ciudad, incluyendo el DPD y el departamento de Servicios de Tecnología de la Información ("ITS") de la Ciudad; (ii) entrevistas a 28 testigos de la Ciudad y de terceros, incluyendo varias entrevistas de seguimiento; y (iii) consulta con Stroz Friedberg sobre temas relevantes de tecnología de la información ("TI") y ciberseguridad.

Nuestros pasos de investigación se detallan a continuación. A continuación, se incluye un resumen de nuestros hallazgos y recomendaciones.

B. Hallazgos

- La causa inmediata del Incidente de la Pérdida de Datos fue una serie de acciones realizadas por un empleado de la Ciudad, un técnico de ITS responsable de las copias de seguridad y el archivo del sistema (el "técnico encargado de las copias de respaldo"), a fines de marzo de 2021.

- En el otoño de 2020 y la primavera de 2021, ITS transfirió los servidores de la Ciudad de una solución de almacenamiento en la nube a servidores locales ubicados en el Concejo de la Ciudad. ITS inició la transferencia del servidor en respuesta a los crecientes costos por uso de datos en la nube que excedían los requisitos presupuestarios. Los costos crecientes fueron en parte el resultado del aumento de los costos relacionados con la instalación secundaria de almacenamiento en la nube de la Ciudad ubicada en ese momento en Arizona.

- Como parte del proceso de transferencia, el técnico encargado de las copias de respaldo cometió los siguientes errores fundamentales:

    - Al transferir los servidores DPD, el técnico encargado de las copias de respaldo no copió correctamente los datos de los sistemas de almacenamiento en la nube actuales a los servidores del Concejo de la Ciudad recientemente implementados. Los datos en cuestión habían sido almacenados; por lo tanto, de acuerdo con los procedimientos del proveedor, el técnico encargado de las copias de respaldo debería haber restaurado los datos almacenados y luego haber copiado los datos restaurados en los servidores del Concejo de la Ciudad. En cambio, copió incorrectamente los archivos de marcador de posición que indican que los datos se habían almacenamiento. Pensando que los servidores se habían transferido correctamente de la nube al Concejo de la Ciudad, el técnico encargado de las copias de respaldo eliminó los datos almacenados de los servidores basados en la nube. Por lo tanto, los datos almacenados ya no estaban en los servidores basados en la nube. Debido a que los datos tampoco se copiaron correctamente en los servidores del Concejo de la Ciudad, ya no se pudieron recuperar.

    - En relación con la transferencia del servidor, el técnico encargado de las copias de respaldo también eliminó la configuración en el software Commvault de la Ciudad que controlaba el almacenamiento de datos de Violencia Familiar del DPD y FUSION. Estas eliminaciones provocaron la pérdida de datos adicionales, incluyendo aproximadamente 13,17 terabytes de datos de FUSION.

- Las acciones del técnico encargado de las copias de respaldo que causaron el Incidente de la Pérdida de Datos parecen haberse basado en su erróneo conocimiento de la plataforma de respaldo y archivo de la Ciudad, Commvault, y de los pasos necesarios para transferir correctamente los datos almacenados desde el almacenamiento en la nube de la Ciudad a los servidores del Concejo de la Ciudad.

    - Durante el curso de nuestra Investigación, no descubrimos ninguna evidencia de que el técnico encargado de las copias de respaldo tuviera una intención maliciosa o un propósito delictivo al eliminar los datos. En última instancia, cualquier conclusión a este respecto dependerá de la agencia de cumplimiento de la ley correspondiente encargada de investigar este asunto.

- El volumen total de datos perdidos en el Incidente de la Pérdida de Datos fue de aproximadamente 23.94 terabytes, de los cuales aproximadamente 3.26 terabytes se recuperaron de otras fuentes. En consecuencia, la pérdida neta de datos de la Ciudad fue de aproximadamente 20.68 terabytes. Según la investigación, estos aproximadamente 20.68 terabytes de datos se perdieron de forma permanente y todos los interesados deberían entender que no se pueden recuperar en su formato original.

- Hasta ahora, los efectos (aparte del costo) del Incidente de la Pérdida de Datos parecen ser relativamente

limitados. El DPD informó que, con una o dos excepciones menores, todos los archivos que identificó como posiblemente perdidos en el Incidente de la Pérdida de Datos se encontraron en otra ubicación (por ejemplo, correos electrónicos o discos duros individuales de los oficiales). La Oficina del Abogado del Distrito también informó que, a partir de enero de 2022, el Incidente de Pérdida de Datos no ha tenido un impacto sustancial en los enjuiciamientos. Sigue siendo posible que haya impactos adicionales en el futuro, aunque ITS, DPD y la Oficina del Abogado del Distrito están tomando medidas para minimizar cualquier impacto futuro.

- Los datos implicados en el Incidente de la Pérdida de Datos incluían ciertos datos almacenados en la nube a través de Commvault. No encontramos evidencia de que el Incidente de la Pérdida de Datos haya afectado negativamente a otros datos de la Ciudad.

C. Evaluación y Recomendaciones

- ITS debería haber implementado medidas de seguridad para garantizar la seguridad de los datos críticos de la Ciudad durante la transferencia del servidor. Dichas medidas de seguridad podrían haber incluido habilitar la función de "eliminación temporal" en la instalación de almacenamiento en la nube de la Ciudad para que los datos eliminados pudieran recuperarse. Además, ITS debería haberse asegurado de que se conservara una copia secundaria de los datos hasta que ITS confirmara que el proyecto de transferencia se completó y verificó con éxito.

- La comprensión y la capacitación del técnico encargado de las copias de respaldo sobre la plataforma Commvault eran erróneas. Dada su condición de profesional de TI y su responsabilidad de salvaguardar los datos críticos de la Ciudad, debería haber tomado la iniciativa de buscar capacitación adicional de ITS y Commvault. Del mismo modo, los directivos ITS debería haberse asegurado de tener un conocimiento suficiente de Commvault y/o traer expertos en la materia (incluyendo especialistas del equipo de Servicios Profesionales de Commvault) para ayudar en una transferencia de datos que implicaba datos críticos de la Ciudad.

- Dado el posible efecto en los casos penales activos, el Incidente de la Pérdida de Datos debería haber sido identificado como un incidente crítico en el momento en que ocurrió, y el Plan de Respuesta a Incidentes ("IRP") de la Ciudad debería haberse activado. Es probable que esto hubiera resultado en una evaluación más exhaustiva del problema en el momento en que se descubrió, así como en una comunicación más clara entre ITS y los interesados clave, incluyendo el DPD, la Oficina del Abogado del Distrito, el Administrador de la Ciudad y el Concejo de la Ciudad, con respecto al alcance de la pérdida de datos y los pasos que se están tomando para mitigar sus efectos.

- El esfuerzo actual de recuperación de datos de ITS se enfoca en identificar copias de documentos posiblemente afectados dentro de otros sistemas de la Ciudad mediante búsquedas de palabras clave para obtener información conocida sobre los casos afectados, como números de casos y nombres de oficiales. No es un esfuerzo por recuperar los datos originales, que ITS entiende perdidos de forma permanente. Hasta la fecha, ITS ha completado búsquedas de aproximadamente el 36% de los 17,484 casos afectados.

- Es incierto si valdrá la pena completar el esfuerzo de recuperación planificado, que no se prevé que finalice hasta fines de 2022, dado que, entre otras cosas, el esfuerzo no recuperará los datos perdidos en su formato original y que muchos archivos afectados puede que nunca se necesite en el futuro. ITS y otros interesados deben coordinarse para desarrollar un enfoque más eficiente y específico para recuperar los archivos afectados de forma prioritaria en el futuro.

- La Ciudad debe considerar al menos los siguientes pasos más amplios para mitigar el riesgo de que ocurra un evento similar en el futuro:

- ITS necesita desarrollar mejores procesos y procedimientos para (i) comprender los costos, beneficios y riesgos de los posibles esfuerzos de transferencia de datos y (ii) mapear todos los pasos de las transferencias propuestas y los riesgos potenciales que deben mitigarse con cada paso.

- La Ciudad debe tomar medidas para garantizar que los departamentos de ITS y de los interesados clave estén coordinados para que ITS pueda abordar adecuadamente todas las necesidades de TI departamentales, particularmente para departamentos como DPD que trabajan con datos críticos día tras día. Por ejemplo, y como se describe más detalladamente a continuación, el DPD y otros departamentos similares deben establecer un director de información departamental posicionado para comprender completamente las necesidades de TI del departamento y abogar por el departamento en el proceso de planificación y presupuestación.

Una evaluación integral de el origen y nuestras recomendaciones completas se establecen en detalle en las secciones VII y XI de este Informe.

II. Ímpetu a la Investigación Interna Independiente

Esta sección resume los eventos que llevaron a la contratación de Kirkland por parte de la Ciudad para llevar a cabo la Investigación del Incidente de la Pérdida de Datos.

A. Consulta del Abogado del Distrito y Comunicado de Prensa Consecuente

Como se describe con más detalle a continuación, la cadena de eventos que finalmente condujo al Incidente de Pérdida de Datos comenzó en el otoño de 2020. ITS descubrió el Incidente de Pérdida de Datos como resultado de las solicitudes de soporte de los usuarios del DPD y emprendió esfuerzos de reparación iniciales a principios de abril de 2021.[1] Aunque ITS proporcionó alguna información al DPD, ITS no informó a la Oficina del Abogado del Distrito sobre el Incidente de Pérdida de Datos en ese momento.[2]

La Oficina del Abogado del Distrito advirtió por primera vez de un posible Incidente de Pérdida de Datos el 30 de julio de 2021. Ese día, un Abogado Adjunto del Distrito del Condado de Dallas ("ADA") descubrió que ciertos archivos del DPD relacionados con un enjuiciamiento pendiente eran inaccesibles.[3] Los archivos en cuestión se había almacenado en la unidad "K", un recurso compartido de red del DPD asignado que consta de varios servidores de archivos subyacentes donde se almacenaba la evidencia del caso en cuestión.[4] Un detective del DPD le dijo al ADA que la Unidad de Almacenamiento K se había dañado y que como resultado, esos archivos ya no estaban disponibles.[5] El ADA luego informó al departamento de TI de la Oficina del Abogado del Distrito sobre el problema.[6]

A lo largo de la semana siguiente, la Oficina del Abogado del Distrito evaluó la situación e informó a sus directivos, incluyendo el Abogado del Distrito Penal del Condado de Dallas, John Creuzot (el "Abogado del Distrito" o "Abogado del Distrito Creuzot").[7] El 6 de agosto de 2021, luego de las consultas de la Oficina del Abogado del Distrito, ITS le informó a la Oficina del Abogado que, durante una transferencia de datos de rutina, "se habían eliminado varios terabytes de datos del DPD."[8] El 9 de agosto de 2021, ITS proporcionó detalles adicionales, informando a la oficina del Abogado del Distrito que entre el 21 de marzo de 2021 y el 5 de abril de 2021 se habían eliminado aproximadamente 22 terabytes de datos del DPD.[9] ITS también informó a la Oficina del Abogado del Distrito que se habían recuperado aproximadamente 14 terabytes de

datos, pero se creía que los ocho terabytes restantes eran irrecuperables.[10]

El 11 de agosto de 2021, Abogado del Distrito Creuzot publicó un comunicado de prensa titulado "Divulgación sobre Datos Faltantes de la Unidad de Red del Departamento de Policía de Dallas"[11] En el comunicado de prensa, el AD Creuzot declaró que la Ciudad se dio cuenta por primera vez del problema el 5 de abril de 2021, pero su oficina sólo había sido informada apenas el 6 de agosto de 2021.[12] Abogado del Distrito Creuzot también ordenó a todos los abogados que compararan los registros del DPD con los que mantiene la Oficina del AD para verificar que todas las pruebas del DPD se habían compartido a través del portal LEA (descrito a continuación).[13] La Oficina del AD luego comenzó a realizar divulgaciones a los abogados defensores y a las cortes que las pruebas podrían haber sido eliminadas.[14]

B. Discusión en el Concejo de la Ciudad

El 12 de agosto de 2021, el Alcalde Eric Johnson le dijo al Concejo de la Ciudad que había sido "sorprendido" el día anterior por la noticia de la pérdida de datos y solicitó que el concejo "convoque una sesión especial conjunta de sus comités para analizar la eliminación de datos, la preocupante falta de comunicación del personal de la Ciudad sobre lo que ocurrió y los pasos que se están tomando para resolver el asunto y prevenir futuras consecuencias".[16] En respuesta, el 18 de agosto de 2021, se informó al Concejo de la Ciudad sobre la una sesión ejecutiva a puertas cerradas.[16]

El 10 de septiembre de 2021, el Comité Ad Hoc sobre Investigación General y Ética (el "Comité Ad Hoc") consideró el asunto #2 de la agenda titulado "Considerar la contratación de un consultor externo para completar una investigación imparcial e integral e informar sobre el la pérdida de datos de la Ciudad".[17] El Presidente Mendelsohn explicó que las metas de cualquier investigación serían "comprender exactamente qué sucedió y por qué; lo que se perdió o recuperó; cómo se puede mejorar el proceso y asegurarse de que se implementen esos cambios".[18] El Comité Ad Hoc luego instruyó al Abogado de la Ciudad para que emitiera una solicitud pública de presentaciones de bufetes de abogados que pudieran realizar una investigación interna independiente.[19] La solicitud de presentaciones estaba abierta a cualquier bufete de abogados que desee presentar una propuesta.[20]

La Ciudad recibió doce propuestas en respuesta, las cuales fueron revisadas por un panel de abogados de la Ciudad compuesto por Tammy Palomino (Primera Abogada Adjunta de la Ciudad), Patricia DeLaGarza (Jefa de Litigios), Ayeh Powers (Abogada Administradora) y Stacey Rodriguez (Jefa de Litigios Generales).[21] El panel de revisión del Abogado de la Ciudad luego seleccionó tres bufetes de abogados para presentarlos al Comité Ad Hoc: Kirkland & Ellis LLP, Akin Gump Strauss Hauer & Feld LLP y Polsinelli. Los representantes de esas firmas, incluyendo a Erin Nealy Cox, socia de la oficina de Kirkland en Dallas, Texas, brindaron breves explicaciones de sus presentaciones y respondieron las preguntas de los miembros del Comité Ad Hoc.[22]

Luego de las presentaciones de los bufetes de abogados, los miembros del Comité Ad Hoc anunciaron individualmente a la firma que deseaban realizar la investigación interna independiente.[23] La presidente Mendelsohn, así como los concejales McGough, Blackmon y Schultz seleccionaron a Kirkland.[A]

El 1 de noviembre de 2021, Kirkland celebró un contrato de servicios profesionales con la Ciudad en virtud del cual se comprometía a investigar la pérdida de datos, contratar a una firma forense para analizar los datos electrónicos perdidos y proporcionar un informe: (1) que detalle cómo y por qué se perdieron los datos, (2) determine si los datos perdidos se recuperaron con éxito, (3) identifique cualquier problema con los sistemas y protocolos de TI de la Ciudad con respecto al mantenimiento y la transferencia de datos electrónicos, incluyendo, pero no limitándose a,

[A] Acta de la Reunión del Comité Ad Hoc de Investigación General y Ética (4 de noviembre de 2021). El concejal Atkins no estuvo presente en todas las presentaciones y, por lo tanto, optó por no participar en el proceso de selección. *Id.*

monitorear y supervisar las acciones de los empleados de ITS responsables de mantener y transferir datos electrónicos, (4) recomendar cambios para evitar que ocurran tales pérdidas de datos en el futuro, incluyendo las mejores prácticas, y (5) brindar cualquier otra recomendación que Kirkland considere necesaria en función de su experiencia en la realización de investigaciones similares.[24]

III. La investigación

A. Independencia de la Investigación

La Ciudad nos ordenó que siguiéramos los hechos dondequiera que condujeran y nos permitió realizar esta Investigación independientemente de interferencias o influencias. Si bien el mandato de investigación de Kirkland fue definido por el Concejo de la Ciudad, Kirkland ejerció su juicio independiente al realizar la Investigación, incluso con respecto a qué documentos necesitaba revisar, con qué testigos necesitaba hablar y qué temas eran relevantes para una investigación más profunda. El Abogado de la Ciudad y el Consejo de la Ciudad no fueron informados de la esencia o el proceso de la investigación de Kirkland, y solo se les dieron actualizaciones sobre el tiempo y el progreso general. A pesar de que el Abogado de la Ciudad nos contrató de conformidad con el privilegio abogado-cliente, diseñamos y realizamos la Investigación sin límites por parte de ellos. A nuestro exclusivo criterio, elegimos a quién entrevistar y qué materiales revisar. Se nos dio acceso rápido a documentos, empleados e información, incluyendo la información de contacto de empleados actuales y anteriores y contratistas externos.

Los hallazgos objetivos establecidos en este informe son presentados únicamente por Kirkland. La Ciudad no ejerció ninguna influencia sobre nuestro informe de los hechos y hallazgos.

Nuestra investigación no es una respuesta nuestra o de la Ciudad a ninguna demanda o investigación criminal pendiente. Kirkland no actúa como abogado de la Ciudad en ningún litigio civil relacionado con esta Investigación. Kirkland nunca antes había brindado representación legal a la Ciudad en ningún asunto relacionado con el Incidente de la Pérdida de Datos, y aunque la Ciudad pagó los honorarios legales de Kirkland incurridos durante la Investigación, el pago no depende de ningún hallazgo o resultado en particular.

B. Equipo de investigación

El equipo de investigación estuvo dirigido por la socia de Kirkland, Erin Nealy Cox, ex Abogada de los Estados Unidos para el Distrito Norte de Texas. Kirkland es una firma de abogados global que atiende a una amplia gama de clientes en todo el mundo y ayuda a las organizaciones a resolver sus problemas más complejos. El equipo de Kirkland que trabajó en la Investigación tiene una gran experiencia en la realización de investigaciones internas y gubernamentales, incluyendo una amplia experiencia en la representación de clientes que enfrentan desafíos de ciberseguridad y administración de datos. Además, Kirkland contrató a Stroz Friedberg, una empresa de consultoría técnica, para brindar asistencia forense y técnica en la Investigación. Stroz Friedberg ayudó en las entrevistas a testigos, realizó una revisión forense de todos los datos disponibles proporcionados por la Ciudad y sus proveedores, realizó recorridos con ITS de ciertos procesos relacionados con su esfuerzo actual de recuperación de datos y ayudó a preparar este informe. Los miembros del equipo de Stroz Friedberg tienen un total combinado de 55 años de experiencia en análisis forense digital y trabajo de respuesta a incidentes, además de antecedentes en leyes, investigaciones militares e investigaciones internas corporativas.

C. Proceso de Investigación

Comenzamos la investigación inmediatamente luego de involucrarnos y comenzamos a coordinarnos rápidamente con la Oficina del Abogado de la Ciudad, ITS, DPD, la Oficina del Abogado del Distrito y proveedores de servicios externos para programar entrevistas a testigos y obtener documentos. Durante un período de tres meses, entrevistamos a 28 testigos, incluyendo:

- El técnico encargado de las copias de respaldo, que ya no es empleado del Concejo de la Ciudad.
- Miembros del equipo ITS de la Ciudad, incluyendo los ejecutivos, supervisores y técnicos involucrados en la respuesta de la Ciudad al Incidente de la Pérdida de Datos. Entrevistamos a algunos miembros del equipo ITS más de una vez.
- Varios miembros del equipo de Seguridad de la Información de la Ciudad que se desempeñan en funciones de auditoría y cumplimiento.
- Un empleado contratado que trabaja en los esfuerzos de recuperación de datos de la Ciudad.
- Numerosos oficiales del DPD en varios niveles directivos y personal de mando.
- Miembros de la Oficina del Abogado del Distrito.
- Empleados de Commvault que tienen conocimiento personal relacionado con los sistemas de la Ciudad y el Incidente de la Pérdida de Datos.

Solicitamos y recibimos documentos y archivos de datos de ITS por un total aproximado de 211.000 páginas y 3.41 gigabytes. También recibimos documentos de la Oficina del Abogado del Distrito, DPD y Commvault. Cabe destacar que nuestra revisión abarcó los siguientes documentos y fuentes de datos clave:

- Memorándums, correos electrónicos y otra documentación que describa el Incidente de la Pérdida de Datos y sus posibles efectos.
- Solicitudes de soporte de Commvault creados como parte de la respuesta de la Ciudad al Incidente de la Pérdida de Datos.
- Informes de auditoría que identifican eliminaciones de políticas y clientes relevantes de Commvault.
- Instrucciones y materiales de apoyo de Commvault, incluyendo los titulados "Retirar un Cliente" y "Recuperar Datos Almacenados".
- Una copia de los archivos y datos de la unidad local del técnico encargado de las copias de respaldo.
- Informe inicial de ITS del 30 de septiembre de 2021 sobre el Incidente de la Pérdida de Datos (el "Reporte ITS").[B]

[B] Se pueden encontrar antecedentes técnicos adicionales sobre Commvault y los servidores de la Ciudad y los sistemas de almacenamiento en la nube en el Informe ITS.

- Un plan ITS para prevenir futuros incidentes de pérdida de datos.

IV. Antecedentes

A. Gobierno de la Ciudad de Dallas e ITS

La Ciudad de Dallas brinda una variedad de servicios gubernamentales a sus más de 1.3 millones de residentes. Para brindar estos servicios, la Ciudad cuenta con ITS, que es responsable de administrar los programas y operaciones de tecnología de los diversos departamentos de la Ciudad. Según ITS, actualmente atiende a 46 departamentos de clientes, incluyendo DPD, Bomberos-Rescate de Dallas, el Abogado de la Ciudad, la Oficina del Administrador de la Ciudad, Servicios Públicos de Agua de Dallas, el Departamento de Aviación y el Departamento de Obras Públicas.

Los departamentos de la Ciudad confían en ITS para los programas y el soporte de TI, incluyendo el almacenamiento, la copia de respaldo y el almacenamiento de datos.[25] Por ejemplo, el DPD confía en ITS para mantener el almacenamiento seguro y el archivo de las pruebas recopiladas para los procesos penales.[26] ITS ha contratado a dos personas para ayudar en sus esfuerzos para dar servicio a DPD: un Director de Relaciones Comerciales para DPD y un Director Sénior de TI para Seguridad Pública, quienes son responsables de servir de enlace con DPD con respecto a sus necesidades de TI.[27] La confianza en ITS se extiende más allá de los propios departamentos de la Ciudad, ya que DPD coordina con la Oficina del Abogado del Distrito en el enjuiciamiento de delitos cometidos en la Ciudad, y la pérdida de pruebas almacenadas por el DPD podría conducir a la incapacidad de mantener enjuiciamientos penales en curso.[28]

Históricamente, ITS ha contado con cinco subgrupos: (i) Infraestructura; (ii) Servidores y Redes; (iii) Redes de Radio; (iv) Servicio de Ayuda y Soporte a Usuarios; y (v) Contratos de Servicios Administrados.[29] Este informe se enfoca en el equipo de Servidores y Redes, que durante el período de tiempo relevante ha sido el grupo responsable de los servicios virtuales, locales, de almacenamiento en la nube y de respaldo, así como del soporte del servidor y servicios de recuperación. [C]

En junio de 2020, la Ciudad contrató a un nuevo Director de Información ("CIO").[30] El CIO tiene la responsabilidad y la supervisión de ITS.[31] Según el CIO, cuando llegó por primera vez a Dallas, notó una serie de deficiencias en ITS.[32] LA función de estos déficits en el Incidente de la Pérdida de Datos se analiza con más detalle a continuación.

B. La Oficina del Abogado del Distrito del Condado de Dallas

La Oficina del Abogado del Distrito es responsable de enjuiciar los delitos menores y graves que ocurren dentro del Condado de Dallas, incluyendo los que ocurren en la Ciudad.[33] A partir de 2020, hay aproximadamente 2.7 millones de residentes en el condado de Dallas,[34] lo que lo convierte en el noveno condado más grande de los Estados Unidos.[35] Esos residentes se distribuyen en más de 30 Ciudades incorporadas que están patrulladas por docenas de departamentos de policía y el Departamento del Aguacil del Condado de Dallas. La Oficina del Abogado del Distrito recibe informes, evidencia, fotografías, videos, grabaciones de audio y una gran cantidad de otros datos de estas entidades todos los días.[36] Para que los fiscales de la Oficina del Abogado del Distrito puedan desempeñar sus funciones correctamente, deben poder recibir y procesar evidencia digital en una manera eficiente y segura.

[C] Entrevista de Testigo el 5 de noviembre de 2021. Desde que comenzó esta investigación, se informa que la recuperación de copias de seguridad se ha trasladado a su propio equipo individual. Entrevista de testigo el 5 de enero de 2022.

C. El Departamento de Policía de Dallas

El DPD y sus más de 3100 oficiales juramentados y aproximadamente 650 empleados civiles requieren un inmenso soporte de TI para llevar a cabo su misión de realizar de la Ciudad un lugar seguro para vivir, trabajar y visitar.[37] Los oficiales construyen sus casos con evidencia como grabaciones de llamadas al 911, fotos y videos.[38] El DPD recopila o genera aproximadamente 800 terabytes de datos por año.[39] Ese número solo aumentará con el tiempo a medida que la evidencia digital, incluyendo cámaras corporales, cámaras de video, imágenes adicionales de drones y helicópteros, y otras fuentes de datos, estén en línea.[40] Naturalmente, las necesidades de TI del DPD incluyen el almacenamiento de una gran cantidad de pruebas en un lugar seguro. Y el DPD debe almacenar esta evidencia por largos períodos de tiempo, comenzando en el momento de la recolección, durante la investigación, hasta que el caso vaya a juicio y a través de cualquier apelación.[41] Para ciertos tipos de casos, no es inusual que este proceso tomar años.

1. Sistemas de Almacenamiento de Evidencia Digital

DPD actualmente se basa en varios sistemas para albergar su evidencia. En primer lugar, los oficiales pueden cargar todas las pruebas en una ubicación específica de la Unidad de Almacenamiento K.[42] El uso de una unidad compartida es importante porque, si un oficial en particular está en el campo, sus colegas o supervisores aún pueden localizar eficientemente los archivos de evidencia de la oficina.[43]

Los oficiales también pueden cargar pruebas en el Sistema de Administración de Registros ("RMS") del DPD, un sistema de administración de casos que puede albergar ciertos tipos de pruebas digitales, así como la cuenta de la Ciudad en Evidence.com.[44] Luego de cargar pruebas en RMS o Evidence.com , luego se espera que los oficiales transfieran el expediente del caso al portal de la Agencia de Cumplimiento de la Ley de Lumen ("LEA").[45] Desde allí, la Oficina del Abogado del Distrito puede acceder a cualquier evidencia en el portal LEA a través del programa TechShare.[D] Ninguna de estas plataformas fueron afectadas por el Incidente de la Pérdida de Datos. Finalmente, DPD tiene datos de teléfonos celulares almacenados en el servidor FUSION en el Concejo de la Ciudad.[46]

[D] *Ver en general* Entrevista de un testigo el 7 de diciembre de 2021. TechShare es una plataforma tecnológica propiedad del condado que aloja un software diseñado para ayudar a administrar la información a lo largo del ciclo de vida de un caso. Para obtener más información sobre el programa, consulte https://techsharetx.gov/./.

El siguiente diagrama resume en un alto nivel el flujo de datos del DPD a través de los sistemas de la Ciudad:

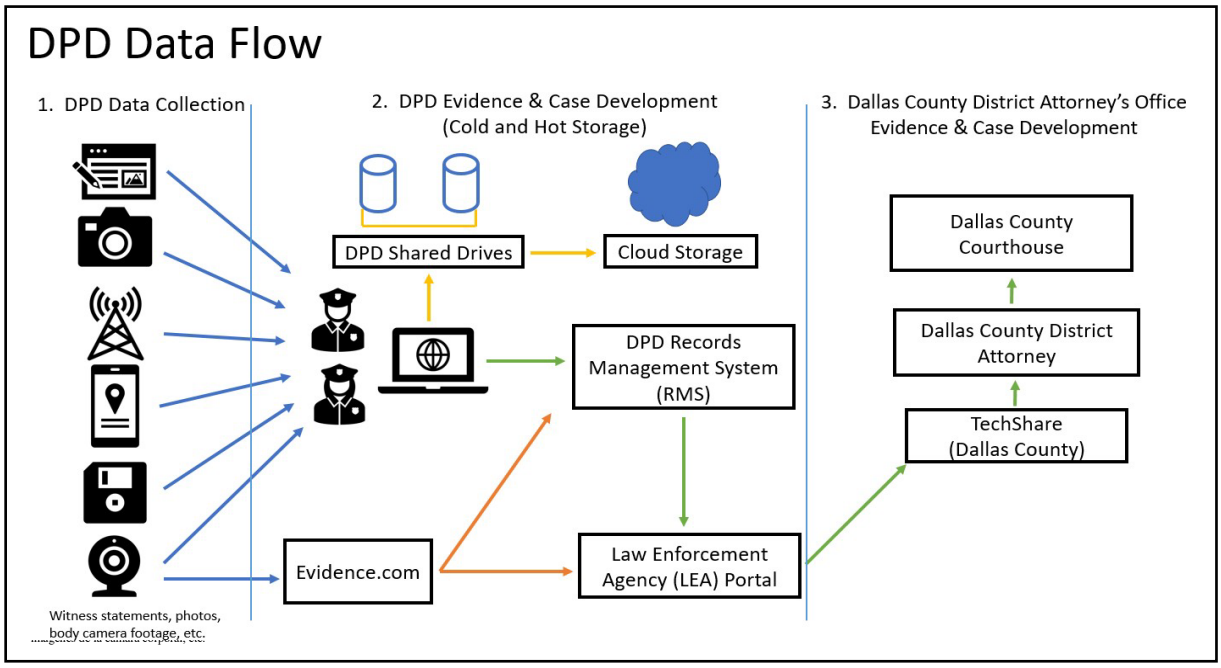

Fig. 1 – Flujo de Datos del DPD

2. Restricciones

Las plataformas Unidad de Almacenamiento K, RMS y LEA/TechShare tienen Restricciones. Dentro de la Unidad de Almacenamiento K, a cada unidad DPD solo se le asigna una cierta cantidad de datos por mes; no permite el almacenamiento ilimitado. [47] Las unidades DPD pueden solicitar espacio de almacenamiento adicional en la Unidad de Almacenamiento K de ITS, pero la solicitud puede demorar varios días en cumplirse, y las solicitudes a menudo se rechazan debido a las Restricciones generales de almacenamiento o al costo.[48] Según se informa, el proceso de carga a la Unidad de Almacenamiento K también suele ser lento, ya que el ancho de banda de la red de subida a la nube es limitado.[49] Los oficiales informan tiempos de carga y descarga en el rango de horas, días y semanas, no minutos.[50] Como resultado, algunos oficiales optan por omitir la Unidad de Almacenamiento K y, en su lugar, cargan la evidencia directamente a RMS desde sus unidades locales.[51] Otros oficiales almacenan sus datos en una computadora portátil local o dispositivos USB, y luego esperan para cargarlos en RMS cuando un caso está listo para presentarlo en la Oficina del Abogado del Distrito.[52]

Si bien RMS no tiene los mismos problemas de velocidad de carga, también tiene Restricciones de espacio de almacenamiento. Según se informa, los archivos de más de 20 megabytes no se pueden cargar en RMS y entendemos que ciertos archivos grandes (como videos en general) no se pueden colocar en RMS debido a Restricciones de espacio. En su lugar, estos datos se cargan en Evidence.com o se entregan personalmente en la Oficina del Abogado del Distrito.[53] El portal LEA también tiene sus límites. Se les ha dicho a los oficiales que solo carguen archivos de menos de cinco gigabytes de tamaño, ya que el sistema se vuelve problemático para el abogado defensor cuando se trata de archivos más grandes.[54]

Los datos del teléfono celular presentan otra complicación para el almacenamiento de evidencia DPD. Cellebrite es una de las herramientas forenses que utiliza DPD para recopilar datos de teléfonos celulares.[55] En el pasado, los datos de teléfonos celulares recopilados de Cellebrite se almacenaban en el servidor llamado FUSION. [E] Pero en 2020, el servidor FUSION se quedó sin capacidad y al DPD no se le

concedieron opciones de almacenamiento adicionales. Como resultado, DPD comenzó a utilizar almacenamientos alternativos. [56] DPD informa que desde que el centro Fusion se quedó sin espacio, han llenado aproximadamente 15 discos duros de dos terabytes con datos recopilados de teléfonos celulares.[57]

Como resultado de los diversos problemas presentados por la evidencia digital, y dada la necesidad de redundancia, parece que los oficiales individuales del DPD han desarrollado sus propias estrategias para almacenar y respaldar la evidencia recopilada.[58] Por ejemplo, los entrevistados del DPD afirmaron que es común que los oficiales mantengan copias duplicadas de evidencia en sus unidades locales o Microsoft OneDrive.[59]

V. Asuntos Técnicos

A. Servicios de TI de Almacenamiento y Copia de respaldo

En general, las copias de respaldo y el almacenamiento cumplen dos funciones distintas. El objetivo de crear copias de seguridad de los sistemas periódicamente es ayudar a recuperarse de un evento inesperado, como una falla de hardware o un desastre natural. Por el contrario, el propósito del almacenamiento es administrar los costos relacionados con el almacenamiento de datos de alta disponibilidad más costoso. El almacenamiento se logra moviendo archivos a los que no se ha accedido durante un período de tiempo (según lo definido por el cliente) a ubicaciones de almacenamiento de menor costo (a menudo denominadas almacenamiento inactivo).

El almacenamiento es más adecuado para los datos que ya no están en uso activo pero que aún no se pueden eliminar debido a requisitos operativos o reglamentarios.[60] Además de la rentabilidad, algunos de los beneficios del almacenamiento incluyen la eliminación de duplicación de datos (los elementos de datos idénticos, como los logotipos de la empresa, se almacenan una vez en lugar de varias) y la indexación de los datos almacenados para recuperarlos rápidamente.

Como se señaló, Commvault, una empresa de software empresarial que cotiza en la bolsa es el proveedor actual de soluciones de copia de respaldo y almacenamiento de la Ciudad. La Ciudad implementó originalmente Commvault en 2018 para reemplazar su solución de respaldo de entonces.[61] A partir de entonces, la Ciudad amplió su uso de Commvault para incluir el almacenamiento.[62]

En general, entendemos que los períodos de archivo establecidos por ITS para los datos relevantes para este Informe fueron los siguientes:

Fuente de Datos	Período de Archivo
Unidad de Almacenamiento K	18 meses[63]
Unidad de Almacenamiento K – Datos de Violencia Familiar	9 meses[64]
FUSION	10 meses[65]

[E] Entrevista de Testigo el 9 de noviembre de 2021. El servidor FUSION contiene una parte significativa de todos los datos de teléfonos celulares recopilados por DPD. La Unidad de Narcóticos y el ICAC tienen la capacidad de realizar y almacenar sus propios registros de teléfonos celulares. *Id.*

B. La Plataforma de Commvault

1. Información General

Dentro de la plataforma de Commvault, los clientes pueden determinar qué sistemas están sujetos a procesos de almacenamiento y/o copia de respaldo, así como la mecánica de dichos procesos, incluyendo qué datos deben almacenarse, cuándo deben almacenarse y dónde se almacenarán los datos almacenados.[66]

Commvault utiliza determinados términos para describir la funcionalidad de su plataforma, como se resume en la siguiente tabla.

Término	Definición	Ejemplo Hipotético
Cliente	En la terminología de Commvault, un "cliente" es un sistema informático que contiene datos que están sujetos a ser almacenados.	La Ciudad mantiene ciertos servidores en sus instalaciones para almacenar archivos digitales. Cada uno de los servidores se considera "clientes".
Política del Cliente	Una “política de cliente” rige los criterios y la mecánica de almacenamiento de datos en un cliente determinado, según la configuración del cliente.[67]	La Ciudad establece una política que requiere que, en servidores particulares, los datos de más de un año se archiven todos los viernes por la noche.
Política de Almacena-miento	Una “política de almacenamiento” es una entidad lógica a través de la cual se archivan los datos de los clientes deCommvault.[68] Más concretamente, una política de almacenamiento rige qué datos deben almacenarse, dónde deben almacenarse los datos almacenados, cuánto tiempo deben conservarse, etc.[69] Una la política de almacenamiento puede abarcar y gobernar datos de múltiples clientes y/o políticas de clientes.	Una política de almacenamiento podría exigir que los datos almacenados se conserven durante siete años antes de eliminarlos.

Término	Definición	Ejemplo Hipotético
Stub	Los stubs son archivos retenidos en un cliente que señalan a los datos almacenados, funcionalmente similares a un acceso directo de Windows.[70] Estos stubs actúan como un "puntero" al archivo almacenamiento y aparecen como archivos activos para el usuario final excepto que tienen un icono gris superpuesto que indica su estado de archivo, como en el siguiente ejemplo de la documentación de soporte de Commvault: DownloadSoftware_Job783170 DonwloadSOftware_Job783174	Utilizando el ejemplo anterior, el sistema retendría los archivos almacenados durante siete años. Cuando se archiva un archivo, se mueve desde la ubicación de almacenamiento original (por ejemplo, un servidor de archivos) a la nube de almacenamiento de Commvault y se reemplaza en el sistema original por un archivo de marcador de posición conocido como archivo stub. El archivo de marcador de posición tiene un icono gris con un logotipo X que indica que el archivo se ha almacenamiento.
Recuperación de Datos (Rehydration)	El proceso de revertir el proceso de almacenamiento extrayendo datos del archivo y reemplazando un stub con el contenido completo del archivo al que se hace referencia.[71]	Un técnico de la Ciudad puede ingresar un comando en el software de Commvault que realiza que el software vuelva a descargar archivos almacenados en un servidor de archivos y vuelva a colocar copias en el servidor.

2. Ubicaciones de Almacenamiento en la Nube

La Ciudad tiene dos instalaciones de almacenamiento en la nube. La instalación de almacenamiento en la nube principal de la Ciudad para Commvault es Microsoft Azure Government Cloud.[72] La Ciudad también tenía una instalación de almacenamiento en la nube secundaria que estaba ubicada en un centro de datos de Azure en Arizona desde aproximadamente abril de 2019 hasta enero de 2021. Desde aproximadamente enero de 2021, la instalación secundaria la instalación de almacenamiento en la nube se ha ubicado en el mismo centro de datos que la instalación de almacenamiento en la nube principal.[73]

3. Recuperación de un Archivo Almacenamiento

El proceso de abrir un archivo almacenamiento implica los siguientes pasos (consulte la Fig. 2 a continuación):

1. Un usuario realiza doble clic en un stub de un archivo que se ha almacenado (por ejemplo, File4.doc).

2. El software de Commvault busca en la nube la ubicación de almacenamiento del contenido almacenado del archivo.

3. El software de Commvault va a esa ubicación de almacenamiento y recupera el contenido almacenado del archivo.

4. El software de Commvault reemplaza el archivo stub con el contenido del archivo y abre ese archivo en el sistema del usuario.

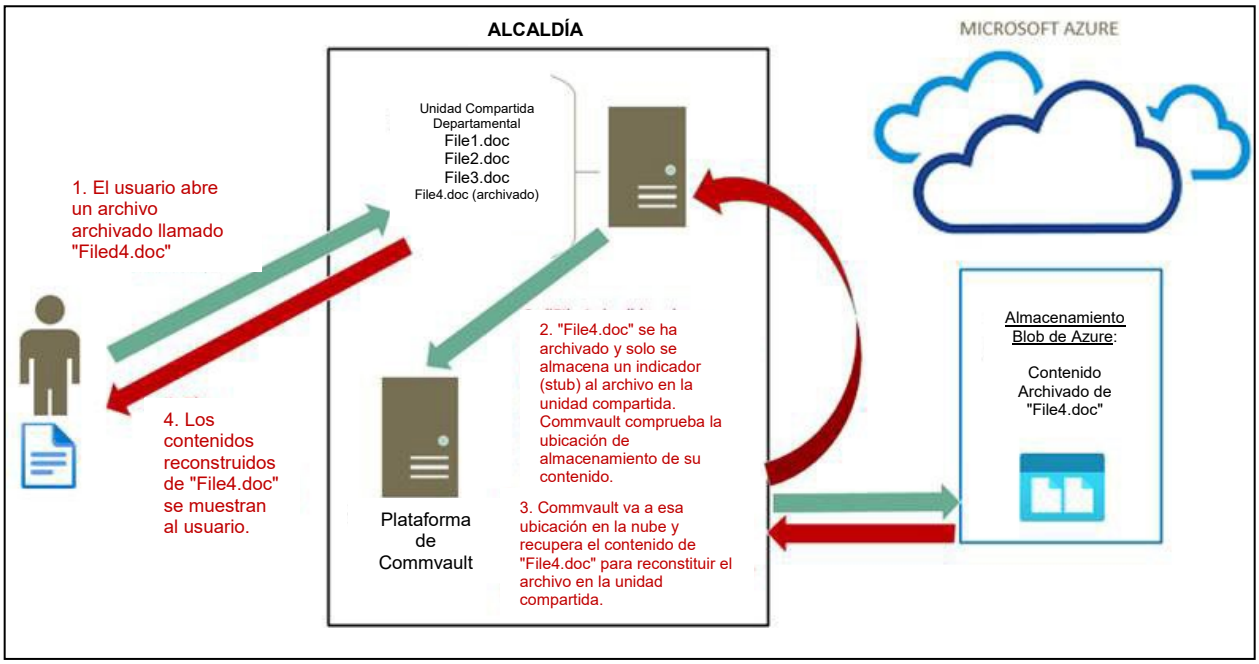

Fig. 2 – Representación del proceso para recuperar un archivo almacenamiento

VI. Conclusiones Objetivas

A. Cronología de Eventos Clave

La siguiente cronología de eventos clave identifica las fechas y los eventos más significativos relacionados con el Incidente de la Pérdida de Datos. En el Apéndice A se proporciona una cronología completa de los eventos relevantes.

Fecha/Horario*	Descripción del Evento
2018	ITS implementa Commvault como la solución de copia de respaldo de la Ciudad y, posteriormente, amplía el uso de Commvault para incluir el almacenamiento.[74]
Julio de 2020	Debates internos de ITS sobre los costos crecientes de entrada y salida de datos para la instalación auxiliar de Azure en Arizona, lo que lleva a la decisión de rediseñar la infraestructura.[75]
24 de agosto de 2020	Una Orden de Cambio que rige la transferencia de datos planificada para principios de 2021 desde la nube al almacenamiento local en el Concejo de la Ciudad de Dallas se envía a través del sistema de administración de cambios de ITS como un cambio "Normal".[76]

* Todos los horarios de CDT.

Fecha/Horario*	Descripción del Evento
Enero de 2021	El técnico encargado de las copias de respaldo comienza a lleva a cabo el plan de transferencia de datos al transferir cuatro servidores de la nube al Concejo de la Ciudad.[77] Mientras que el técnico encargado de las copias de respaldo intenta recuperar los datos de los archivos almacenados en los servidores antes de la transferencia, los errores en ese proceso dan como resultado una recuperación de datos incompleta, lo que significa que muchos archivos de los servidores no se transfirieron correctamente.[78]
Febrero de 2021	El técnico encargado de las copias de respaldo retira cuatro de los transferidos incorrectamente en Azure.[79] Tres de los servidores transferidos no fueron retirados.[80]
30 – 31 de marzo de 2021	El técnico encargado de las copias de respaldo trabaja para "limpiar" el sistema Commvault de la Ciudad mediante la realización de 17 eliminaciones permanentes de clientes y cinco eliminaciones de políticas de almacenamiento.[81] Como se describe en este documento, algunas de estas eliminaciones provocaron la pérdida de datos almacenados de Unidad de Almacenamiento K.
5 de abril de 2021	ITS recibe su primera solicitud de soporte del DPD con respecto a los archivos inaccesibles de la Unidad de Almacenamiento K.[82]
5 de abril de 2021 11:00 AM	El técnico encargado de las copias de respaldo suspende todas las eliminaciones de Commvault, lo que detiene el proceso de eliminación desencadenado por sus acciones de "limpieza".[83]
5 de abril de 2021 12:08 PM	El técnico de copia de respaldo crea una solicitud de soporte con Commvault con la descripción: "Los archivos almacenados y de stub no se recuperan".[84]
5 de abril de 2021 12:30 PM	El técnico encargado de las copias de respaldo notifica a su supervisor, el Director de TI para Servidores y Redes, que cometió un “error” durante la limpieza la semana anterior.[85]
5 de abril de 2021 6:22 PM	El soporte de Commvault identifica que “las recuperaciones de stubs estaban fallando porque los stubs estaban vinculados a clientes eliminados. . . que fueron borrados la semana pasada.”[86]
6 de abril de 2021 7:00 AM	El Director de TI para Servidores y Redes informa al Director Adjunto de Infraestructura del incidente.[87]
6 de abril de 2021 9:27 AM	El Director Adjunto de Infraestructura informa al CIO.[88]
9 de abril de 2021	ITS trabaja con el soporte de Commvault para confirmar el alcance de la pérdida de datos e identificar los posibles próximos pasos.[89]
10 de abril de 2021	El Director de TI para Servidores y Redes informa al Director Sénior de TI de Seguridad Pública y al equipo de TI que respalda a DPD que los archivos de varias divisiones se han eliminado y "podrían" ser irrecuperables.[90]

12 de abril de 2021	El Director Sénior de IT para Seguridad Pública anuncia en la reunión del personal de mando del DPD en la sede del DPD que ITS está trabajando para abordar un problema que afecta a la Unidad de Almacenamiento K. [91]

Fecha/Horario*	Descripción del Evento
13 de abril de 2021	El CIO notifica al Administrador Adjunto de la Ciudad por correo electrónico "sobre la posible pérdida masiva de datos que se produjo debido a un error durante la realización de transferencias de archivos de rutina desde el almacenamiento de Azure al almacenamiento del Concejo de la Ciudad de los archivos de archivos DPD. Estamos organizando una reunión con la directiva del DPD esta tarde."[92]
19 de abril de 2021	El Jefe de Policía del DPD publica un memorándum interno para todo el personal del departamento, en el que se indica: "Los servicios de TI han recibido informes de archivos o carpetas que faltan en las unidades de red. Se solicita a todo el personal del departamento que verifique si faltan archivos o carpetas en sus unidades de red. Si le faltan archivos o carpetas, siga los pasos en el archivo adjunto para restaurar los archivos o carpetas que faltan."[93]
Mayo-Agosto de 2021	El técnico encargado de las copias de respaldo continúa con las eliminaciones manuales de los clientes de Commvault.[94]
30 de julio de 2021	Los oficiales informan a un ADA que ciertos archivos DPD relacionados con un enjuiciamiento pendiente ya no están disponibles en Unidad de Almacenamiento K.[95]
Principios a mediados de agosto de 2021	DPD comienza a descubrir problemas con la recuperación de datos de FUSION.[96]
6 de agosto de 2021	ITS informa a la Oficina del Abogado del Distrito de los datos borrados.[97]
11 de agosto de 2021	Abogado del Distrito Creuzot emite un memorándum y comunicado de prensa sobre la pérdida de datos.[98]
12 de agosto de 2021	El técnico encargado de las copias de respaldo y el Director de TI se reúnen para una "entrevista de licencia administrativa".[99]
Mediados de agosto de 2021	Commvault realiza una auditoría de políticas y clientes eliminados y determina que el servidor FUSION también se ha visto afectado debido a una política de almacenamiento eliminada.[100]
26 de agosto de 2021 6:25 PM	El CISO activa el IRP para realizar un análisis de la pérdida de datos, elevándolo a un nivel de gravedad de P1.[101]
27 de agosto de 2021	Se envía un Notificación formal de la posible pérdida de datos a la Oficina del Administrador de la Ciudad, la Oficina del Alcalde, el Concejo de la Ciudad y la Oficina del Abogado del Distrito.[102]
30 de agosto de 2021	El técnico encargado de las copias de respaldo recibe una notificación de audiencia previa al despido.[103]
22 de octubre de 2021	El técnico encargado de las copias de respaldo es despedido.[104]

B. La transferencia de Datos 2020-2021

1. Impulso y Planificación

El advenimiento del sistema Commvault de la Ciudad se remonta a 2017. Luego de recibir una gran factura ese año del proveedor de respaldo de la Ciudad en ese momento, ITS decidió cambiarse a Commvault en algún momento durante el año siguiente.[105] El técnico encargado de las copias de respaldo llegó a tener responsabilidad en ITS para Commvault en esta época.[106] Otro administrador de sistemas sénior actuó como suplente para la cobertura de Commvault, pero nunca estuvo destinado a servir como un recurso de respaldo completo, y no recibió capacitación sobre Commvault hasta agosto de 2021. [107] Commvault fue contratado para asesorar a ITS en la configuración o implementación de la plataforma de la Ciudad, ni la Ciudad contrató al equipo de Servicios Profesionales de Commvault para brindar orientación sobre la implementación, las estrategias de transferencia.[108]

En 2020, y nuevamente debido al aumento costos, ITS decidió implementar otro cambio y alejarse del almacenamiento en la nube a favor de alojar nuevamente los datos de la Ciudad en el Concejo de la Ciudad.[109] En relación con este proceso, ITS decidió retirar los servidores actuales de la Ciudad en la nube.[110] La decisión de ITS de transferir los servidores de la Ciudad del almacenamiento en la nube a sus instalaciones fue impulsada por el costo: específicamente, los crecientes costos mensuales relacionados con el uso de datos en la nube, principalmente, pero no exclusivamente, relacionados con la instalación secundaria de almacenamiento en la nube, que en ese momento estaba ubicado en un centro de datos en Arizona.[F]

ITS envió la Orden de Cambio que rige la transferencia de datos (la "Orden de Cambio") a través de su sistema de administración de cambios el 24 de agosto de 2020, caracterizando el cambio como un cambio "Normal".[111] La Orden de Cambio enumeró al técnico encargado de las copias de respaldo como responsable de la transferencia de datos, y proporcionó la siguiente descripción del cambio:

> Implemente nuevas bibliotecas de almacenamiento de Azure para eliminar los costos de salida entre regiones. Las bibliotecas nuevas solo existirán en la región de Texas. La transferencia será gradual para poder controlarlo.[112]

De conformidad con la Orden de Cambio, ITS planeó realizar la transferencia (incluyendo la consolidación de ciertos servidores) y luego realizar una transición donde los servidores antiguos se desconectarían y los servidores nuevos se conectarían en su lugar.[113] Luego de operar en esa condición durante treinta días sin problemas, el plan era retirar los antiguos servidores en la nube, incluyendo la detención de las copias de seguridad de esos sistemas, la detención de los servicios de monitoreo y aplicación de parches, y la eliminación de los servidores.[114] La Orden de Cambio fue aprobada por el Director de TI para Servidores y Redes y el Director Adjunto de Infraestructura.[115]

Uno de los documentos adjuntos a la Orden de Cambio, "Plan de Implementación para las Nuevas Bibliotecas de Almacenamiento Blob de Commvault", fue escrito por el técnico encargado de las copias de respaldo y contiene una lista de los pasos que se deben realizar en relación con la transferencia del servidor.[116] El primer elemento

[F] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 15 de diciembre de 2021; Entrevista de Testigo el 5 de enero de 2022; Entrevista de Testigo el 5 de enero de 2022. El cambio a la nube se describió como un esfuerzo de "elevar y cambiar" en el que todo, desde los servidores de impresión y de bases de datos hasta los servidores de archivos, se trasladaron a la nube sin rediseño; su ubicación simplemente se cambió de la nube al Concejo de la Ciudad. Entrevista de testigo el 5 de noviembre de 2021.

en la lista dice "eliminar biblioteca de Arizona", lo que significa que los datos almacenados en la instalación de almacenamiento en la nube secundaria se eliminarían como parte del proceso de transferencia.[117] Los otros pasos en el documento recorren ciertos datos de Commvault que se transferirían y eliminarían.[118] El técnico encargado de las copias de respaldo declaró que, aunque recibió información general de Commvault sobre el proceso de transferencia en varios puntos, el Soporte técnico de Commvault no revisó la Orden de Cambio ni la lista de pasos adjunta.[119]

2. Realización

En enero de 2021, el técnico encargado de las copias de respaldo comenzó a realizar el "Plan de Implementación". De acuerdo con el orden de los pasos en el "Plan de Implementación", el técnico encargado de las copias de respaldo eliminó los datos de Commvault en la instalación secundaria de almacenamiento en la nube en Arizona. [G] El técnico encargado de las copias de respaldo luego intentó transferir varios servidores con datos almacenados desde la ubicación principal de almacenamiento en la nube de la Ciudad a los nuevos servidores de almacenamiento de la Ciudad en el Concejo de la Ciudad, y luego realizó la transición para activar los nuevos servidores.[120] Treinta días luego de completar la transferencia, no se informaron errores ni problemas a ITS.[121]

En este punto, el técnico encargado de las copias de respaldo creía que todos los datos en los servidores de archivos de la Ciudad que estaban previamente ubicados en las instalaciones de almacenamiento en la nube de la Ciudad se habían reubicado con éxito a los nuevos servidores en el Concejo de la Ciudad.[122] El técnico encargado de las copias de respaldo aparentemente no advirtió de que los archivos transferidos incluía millones de stubs, que representan archivos almacenados, y que los datos almacenados subyacentes no se habían transferido correctamente dentro de Commvault a través de un proceso de recuperación de datos adecuado. El técnico encargado de las copias de respaldo procedió a eliminar cuatro de los clientes de servidor transferidos de Commvault[123], así como una política de almacenamiento de Commvault que rige el almacenamiento de datos de FUSION y Violencia Familiar.[124]

3. Análisis

Identificamos varios problemas en la realización del "Plan de Implementación". Primero, según el técnico encargado de las copias de respaldo, ITS confió en los usuarios finales relevantes para verificar que aún podían acceder a

[G] Los relatos de los testigos difieren con respecto a algunos detalles relacionados con la eliminación de la instalación secundaria en Arizona. Primero, cuando se le preguntó sobre el hecho de que la lista de pasos en el documento del "Plan de Implementación" está numerada y el primer paso dice "eliminar la biblioteca de Arizona", el técnico encargado de las copias de respaldo afirmó que el documento simplemente tenía la intención de servir como una lista de verificación de pasos, eso debería tomarse en algún punto de la transferencia, no una secuencia ordenada de pasos. Entrevista de Testigo el 15 de diciembre de 2021. Por el contrario, el Director del técnico encargado de las copias de respaldo, que participó en la revisión de la Orden de Cambio y la documentación de respaldo, afirmó que entendía que el documento enumeraba los pasos de transferencia en el orden en que debían realizase. según lo identificado por el técnico encargado de las copias de respaldo. Entrevista del testigo el 5 de enero de 2022. En segundo lugar, según el técnico encargado de las copias de respaldo, el ingeniero de ventas de Commvault responsable de la cuenta de la Ciudad recomendó no eliminar la ubicación de almacenamiento secundario en Arizona. Entrevista de Testigo el 15 de diciembre de 2021. El técnico encargado de las copias de respaldo también declaró que transmitió esta recomendación a sus supervisores y que, a pesar de sus objeciones y las de Commvault, le ordenaron que continuara y eliminara los servidores almacenados en las instalaciones de Arizona. *Id*. Por el contrario, el ingeniero de ventas de Commvault, cuando fue entrevistado, afirmó que no expresó ninguna objeción. Entrevista de Testigo el 5 de enero de 2021. Dijo que siempre le decía al técnico encargado de las copias de respaldo que mantuviera los datos de archivo en la ubicación más barata y alentó la redundancia general de datos, ya sea en diferentes regiones o en diferentes medios. El ingeniero de ventas de Commvault afirmó que, según su entendimiento, el sistema de la Ciudad cumplía con estos requisitos al pasar de Azure a las instalaciones. *Id.* A pesar de estos detalles diferentes, todos los testigos coincidieron en que el técnico encargado de las copias de respaldo eliminó la instalación secundaria en Arizona antes de llevar a cabo el resto de la transferencia. Entrevista de testigo el 15 de diciembre de 2021; Entrevista de testigo el 5 de noviembre de 2021; Entrevista de Testigo el 5 de enero de 2022; Entrevista de testigo el 22 de noviembre de 2021.

todo lo que necesitaban y enviar una solicitud de soporte en caso de cualquier problema.[125] Por lo tanto, cuando el técnico encargado de las copias de respaldo no escuchó los informes de problemas de accesibilidad del DPD durante 30 días luego de la transición, creyó que el proyecto de transferencia se validó adecuadamente y no tomó algún paso de Confirmación adicional. [H] Por ejemplo, el técnico encargado de las copias de respaldo no realizó un informe para determinar que los nuevos stubs hacían referencia a sus ubicaciones previstas para garantizar que todos los datos se habían transferido correctamente.[126] Además, el técnico encargado de las copias de respaldo no pudo retener una copia de los datos que intentó transferir en caso de que algo saliera mal en el proceso de transferencia. La falta de una copia duplicada creó consecuencias graves cuando se cometieron errores. Debido a que los datos de archivo de Commvault se almacenan en un almacenamiento sin duplicados especial, no es posible reconstruir los archivos eliminados a través de la recuperación forense, como se puede realizar con frecuencia en una computadora de escritorio típica u otros tipos de almacenamiento. [I] Cuando las actividades de "limpieza" del técnico encargado de las copias de respaldo elimina el mapeo entre los stubs de Commvault y los archivos correspondientes, esto hizo imposible reconstruir los datos eliminados. Esto provocó la eliminación de aproximadamente 23.94 terabytes de datos de la Ciudad.

El técnico encargado de las copias de respaldo tampoco pudo recuperar datos de los archivos en los sistemas de los usuarios que se habían almacenamiento. Según Commvault, uno de los pasos necesarios para transferir un servidor con archivos almacenados por Commvault es "recuperar" los datos que se han almacenamiento, es decir, revertir el proceso de almacenamiento y reemplazar los stubs con los datos subyacentes.[127] En este caso , sin embargo, el técnico encargado de las copias de respaldo no completó el proceso de recuperación para todos los servidores antes de la transferencia, lo que significa que para algunos servidores, solo se transfirieron los stubs a la nueva ubicación local en lugar del contenido completo del archivo.[128] Debido a que esos servidores se transfirieron de forma incompleta, la eliminación de las políticas de almacenamiento y los clientes de Commvault relevantes resultó en la pérdida de sus datos.[129] No identificamos evidencia de que alguien en ITS haya tomado medidas para validar que los datos transferidos estaban presentes y accesibles, aparte de esperar 30 días para que los usuarios informaran por sí mismos acerca de los problemas.[130] El Director de TI afirmó que confió en el técnico encargado de las copias de respaldo para validar la transferencia de datos, pero no pudo dar más detalles sobre el método de verificación utilizado.[131]

[H] Entrevista de Testigo el 15 de diciembre de 2021. El técnico encargado de las copias de respaldo también afirmó que nunca tuvo tiempo de tomar pasos de Confirmación adicionales, debido a las Restricciones de tiempo impuestas como resultado del trabajo constante del proyecto requerido por el departamento de ITS. *Id.*

[I] En un sistema de almacenamientos de Windows, cada archivo se escribe en una ubicación disponible en la unidad de almacenamiento correspondiente y el sistema de almacenamientos rastrea la ubicación de cada archivo en esa unidad en una tabla. Cuando se elimina un archivo, la entrada de la tabla que indica a la ubicación del archivo en la unidad se elimina y la ubicación donde reside el contenido del archivo queda disponible para su uso. Sin embargo, el espacio de almacenamiento del archivo en sí mismo normalmente no se borra ni se sobrescribe, dejando el contenido del archivo intacto en la unidad, a menos y hasta que se escriba otro archivo en el mismo espacio de almacenamiento. Como resultado, es posible recuperar más tarde un archivo eliminado, en parte o en su totalidad, examinando el contenido del espacio no asignado (espacio no relacionado con un archivo) en la unidad. Examinar el espacio no asignado para intentar recuperar archivos eliminados es el proceso típico de primera línea empleado en un esfuerzo de recuperación de datos forenses.

Por el contrario, Commvault almacena datos en lo que se conoce como formato sin duplicado. Cuando se añaden archivos, el sistema de almacenamientos verifica cualquier coincidencia de contenido total o parcial entre los archivos que ya están en el almacenamiento correspondiente y luego simplemente asigna esos contenidos a la ubicación de almacenamiento correspondiente. Dada la cantidad de duplicación que a menudo se encuentra en los tipos típicos de datos, como correos electrónicos y documentos, este proceso de comparar archivos nuevos con datos actuales puede resultar en reducciones significativas en el volumen total de datos almacenados. Sin embargo, puede añadir ciertos riesgos: en particular, debido a que los datos no están duplicados, eliminar un solo archivo simplemente significa eliminar la entrada de índice relevante para ese archivo. No existe un espacio de almacenamiento único desde el cual se pueda recuperar el archivo y, por lo general, la entrada de índice en sí misma no es recuperable. Como resultado, una vez que los archivos se eliminan de un almacenamiento de Commvault sin duplicado, no se pueden recuperar mediante técnicas forenses tradicionales.

C. Los Eventos de Marzo y Abril de 2021

1. Cómo Ocurrieron las Eliminaciones de Marzo

Según todos los informes, el acuerdo dentro de ITS era que, a partir del 30 de marzo de 2021, la transferencia de datos estaba completa y el software de Commvault ahora estaba almacenando y recuperando datos de los servidores de almacenamiento en las instalaciones del Concejo de la Ciudad.[132] Por lo tanto, el martes 30 de marzo de 2021, el técnico encargado de las copias de respaldo comenzó el proceso de "limpieza" de los clientes y políticas de Commvault que creía que ya no eran necesarios luego de la transferencia.[133]

El 30 y 31 de marzo de 2021, el técnico encargado de las copias de respaldo ejecutó una serie de eliminaciones que afectaron a 17 políticas de clientes y cinco políticas de almacenamiento.[134] Juntas, estas políticas gobernaron principalmente el almacenamiento de datos que los empleados del DPD habían almacenado en la Unidad de Almacenamiento K del DPD.[135] Como resultado de eliminar estas políticas, Commvault eliminó automáticamente de la nube cualquier archivo creado bajo esas políticas. Por lo tanto, los stubs relacionados con los archivos almacenados en la Unidad de Almacenamiento K del DPD y que el técnico encargado de las copias de respaldo había transferido sin darse cuenta a los nuevos servidores de almacenamiento en el Concejo de la Ciudad ya no podían recuperarse, porque los archivos habían sido eliminados.

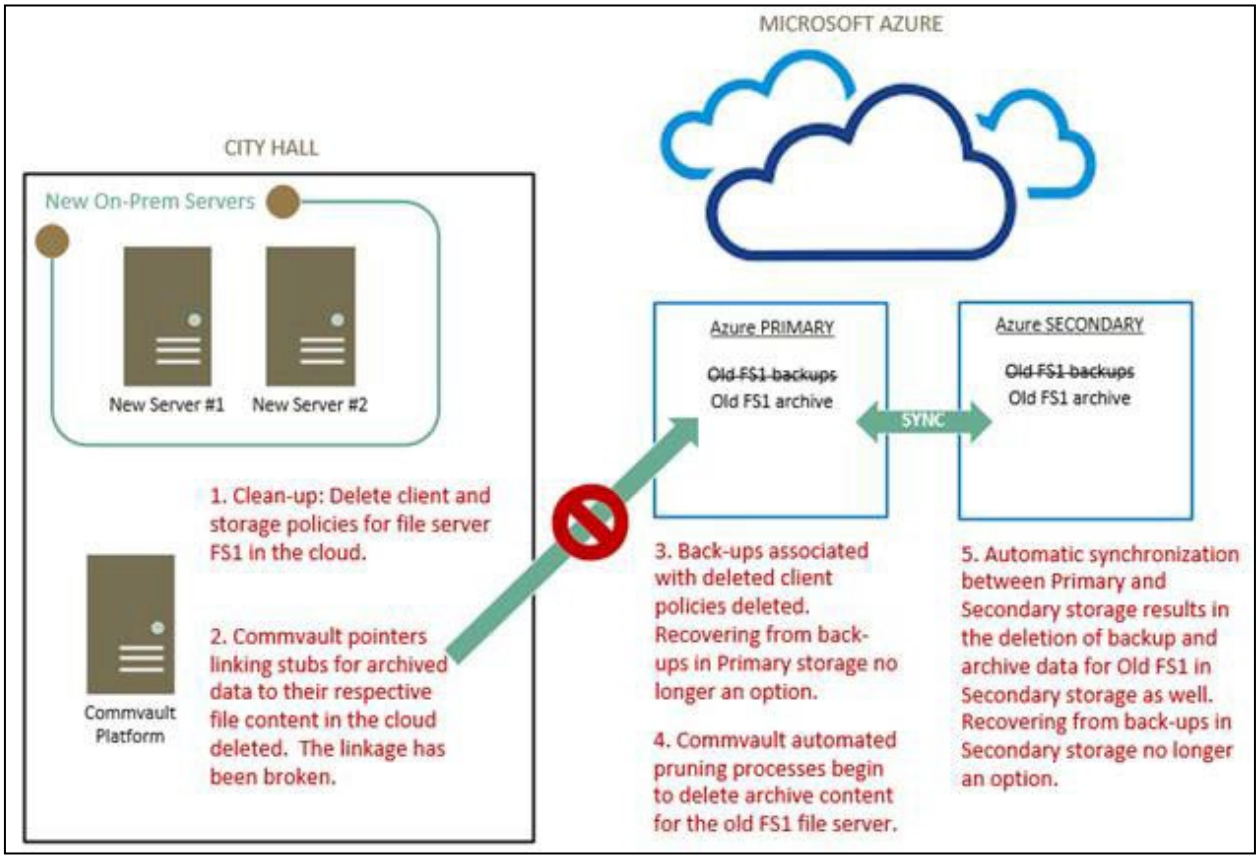

Fig. 3 –Representación de eventos de eliminación

Existen protecciones dentro del sistema Commvault para mitigar el riesgo de eliminación no intencional de datos. Por ejemplo, para eliminar una política de almacenamiento, Commvault preguntará al usuario final si desea continuar. Si el usuario desea eliminar, debe escribir manualmente la frase "borrar y reutilizar medios" como se muestra en la figura a continuación.[136]

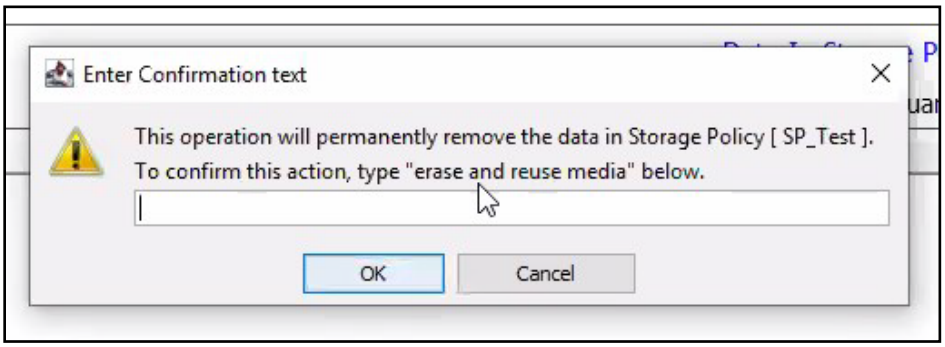

Fig. 4 – Mensaje de Confirmación de Eliminación de la Política de Commvault

Commvault proporciona advertencias similares para la eliminación de un cliente.[137] En este caso, el software de Commvault notificó al técnico encargado de las copias de respaldo dos veces que continuar con las eliminaciones permanentes de cliente resultaría en la eliminación de datos.[138] La documentación de soporte de Commvault establece que dichos datos se vuelven irrecuperables a menos que haya una copia de respaldo que contiene información sobre la entidad eliminada (es decir, la política de almacenamiento o el cliente).[139] El técnico encargado de las copias de respaldo procedió con las eliminaciones, a pesar de las advertencias.

Cuando fue entrevistado, el técnico encargado de las copias de respaldo confirmó que entendía que la instalación de almacenamiento en la nube secundaria en Arizona ya no existía en el momento en que procedió con las eliminaciones de clientes y políticas de almacenamiento anteriores porque se había transferido al servidor local. También confirmó que sabía que ejecutar el comando de eliminación permanente podría resultar en la eliminación de los datos almacenados.[140] Sin embargo, el técnico encargado de las copias de respaldo declaró que no prestó atención a estas notificaciones porque pensó que los datos ya se habían movido, y estas alertas pertenecían solo al archivo antiguo que, en su opinión, ya había sido transferido a su nueva ubicación.[141] Por lo tanto, creía que era seguro borrarlo.[142] Reconoció que no entendió en ese momento que el proceso de recuperación no se había completado correctamente para los cuatro servidores retirados (lo que resultó en la pérdida de los datos almacenados de esos servidores).[143]

2. Descubrimiento del Problema Dentro de ITS

La primera notificación a ITS de cualquier dato almacenamiento inaccesible ocurrió en la mañana del lunes 5 de abril de 2021, cuando ITS comenzó a recibir solicitudes de soporte del DPD con respecto a archivos de la Unidad de Almacenamiento K inaccesibles.[144] Una vez que el técnico encargado de las copias de respaldo advirtió de un posible problema, inmediatamente detuvo el proceso de “limpieza” que comenzó el 30 de marzo de 2021.[145]

Esa tarde, el técnico encargado de las copias de respaldo creó una solicitud de soporte con Commvault que tenía la descripción: "Los archivos almacenados y de stub no se recuperaron".[146] El técnico encargado de las copias de respaldo luego notificó a su supervisor, el Director de TI para Servidores y Redes, que había cometido un "error” la semana anterior.[147] Específicamente, informó a su supervisor que había eliminado una cantidad de clientes vinculados a servidores antiguos, lo que podría haber resultado en la eliminación de un volumen significativo de archivos.[148]

dijo que le informó a su Director que DPD había estado llamando para informar sobre la imposibilidad de acceder a los datos, que el técnico encargado de las copias de respaldo ahora creía que era el resultado de las eliminaciones de sus clientes.[149]

A lo largo de la semana siguiente, el técnico encargado de las copias de respaldo y el administrador de la nube de ITS trabajaron con Commvault y Microsoft, respectivamente, en posibles vías de corrección y/o recuperación.[150] Entre otras cosas, el administrador de la nube de ITS se comunicó con Microsoft para determinar si la "eliminación temporal" La función se habilitó para las cuentas de almacenamiento de la Ciudad. [J] Microsoft confirmó que la función de eliminación temporal no estaba disponible cuando la Ciudad cambió inicialmente a la nube de Azure y nunca se añadió posteriormente, por lo que no era una opción para la recuperación.[151]

En la mañana del martes 6 de abril de 2021, el Director de TI para Servidores y Redes informó al Director Adjunto de Infraestructura sobre el incidente y el alcance del impacto conocido en ese momento.[152] El Director Adjunto de Infraestructura se comunicó con el Director de Información de la Ciudad en la noche del martes 6 de abril de 2021.[153] En ese momento, el técnico encargado de las copias de respaldo estaba trabajando activamente con Commvault para intentar recuperar los datos perdidos.[154]

El Director Sénior de TI de seguridad pública fue notificado por el Director de TI para servidores y redes el 8 de abril de 2021 sobre el problema.[155] En ese momento, un detective del DPD envió una solicitud de soporte de alta prioridad que indicaba que no podía acceder a ciertos archivos en el Unidad de Almacenamiento K.[156] Nadie dentro de ITS activó el IRP de la Ciudad en ese momento.

Durante una reunión el 10 de abril de 2021, se notificó al DPD que los archivos de varias divisiones se habían eliminado y podrían ser irrecuperables.[157] Luego, el equipo del servidor proporcionó una hoja de cálculo para comenzar a reducir el alcance de lo que se había perdido.[158] La seguridad y el Director de relaciones comerciales de ITS para DPD no tomaron más medidas iniciales más allá de establecer una fila individual y priorizada para las solicitudes de soporte enviadas por DPD relacionadas con Unidad de Almacenamiento K.[159]

Luego de consultar con Commvault y Microsoft, el equipo del servidor ITS proporcionó un desglose de los eventos al CIO.[160] Posteriormente, el 13 de abril de 2021, el CIO informó al Administrador Adjunto de la Ciudad por correo electrónico sobre una "pérdida masiva de datos debido a un error". durante la realización de transferencias de archivos de rutina desde el almacenamiento de Azure al almacenamiento del Concejo de la Ciudad de los archivos almacenados del DPD."[161]

3. Notificación a los Directivos del DPD

El Director Sénior de TI de Seguridad Pública asistió a una reunión del personal de mando del DPD el lunes 12 de abril de 2021 en la sede del DPD que incluyó a todos los jefes, los comandantes de las subestaciones y oficinas, y el equipo de TI que apoya al DPD.[162] El Director Sénior de TI de Seguridad Pública anunció en la reunión del Personal de mando que ITS estaba trabajando en un problema que afectaba a Unidad de Almacenamiento K y ordenó a los empleados del DPD que enviaran una solicitud de soporte si se necesitaba un archivo que se creía inaccesible en Unidad de Almacenamiento K para un caso judicial.[163] El Director sénior de TI de Seguridad Pública luego

[J] Entrevista de Testigo el 5 de noviembre de 2021. La eliminación temporal es una función disponible en Azure que protege los archivos de eliminaciones o sobreescrituras accidentales al mantener los datos eliminados en el sistema durante un período de retención específico (entre uno y 365 días) seleccionado por el cliente. Durante el período de retención, un objeto eliminado temporalmente puede restaurarse a su estado en el momento de la eliminación. Una vez que ha expirado el período de retención, el objeto se elimina de forma permanente. Consulte Eliminación temporal de blobs, Microsoft Azure (27 de enero de 2022), https://docs.microsoft.com/en-us/azure/storage/blobs/soft-delete-blob-overview.

proporcionó al DPD un memorándum que detallaba un proceso de dos pasos que involucraba (1) el envío de una solicitud a ITS con respecto a archivos y/o carpetas faltantes, y (2) proporcionar una lista de archivos y/o carpetas faltantes para ser "restaurados".[164] Se enviaron once solicitudes al final de esa semana laboral, y para el lunes siguiente, había 23 solicitudes pendientes.[165]

El 19 de abril de 2021, y debido al creciente número de problemas para acceder a los archivos de Unidad de Almacenamiento K, el Jefe de Policía del DPD emitió un memorándum interno a todo el personal del departamento en el que se indica:

> Los servicios de TI han recibido informes de archivos o carpetas que faltan en las unidades de red. Se solicita a todo el personal del departamento que verifique si faltan archivos o carpetas en sus unidades de red. Si le faltan archivos o carpetas, siga los pasos en el archivo adjunto para restaurar los archivos o carpetas que faltan.[166]

Incluido con el memorándum del Jefe estaba el memorándum antes mencionado escrito por el Director Sénior de TI de Seguridad Pública que describe los pasos que los oficiales podrían tomar para "restaurar [sus] archivos o carpetas faltantes".[167] Está claro de todas nuestras conversaciones con DPD y de la redacción utilizada en la notificación a los empleados del Director Sénior de TI, como "restaurar", que DPD no entendió en ese momento que los datos eran irrecuperables.[168]

4. Función del Soporte Técnico de Commvault

Como se describió anteriormente, el técnico encargado de las copias de respaldo abrió una solicitud de soporte de Commvault en la tarde del 5 de abril de 2021. En unas pocas horas, el ingeniero de soporte de Commvault asignado identificó la causa del problema: que "las recuperaciones de stub estaban fallando porque los stubs estaban vinculados a clientes eliminados que se eliminaron la semana pasada".[169] El ingeniero de soporte de Commvault explicó además que la pérdida de datos parecía haber sido causada por una falla en la "recuperación" adecuada de los datos relevantes:

> De la discusión, los stubs de los clientes en cuestión se transfirieron a un nuevo hardware, sin embargo, no todos los datos se recuperaron, lo cual es necesario para volver a colocar en stub los datos para relacionarlos con el nuevo cliente. Como resultado, algunos de los antiguos stubs todavía estaban relacionados con el cliente anterior y, al eliminar los clientes, se eliminaron los metadatos de la base de datos de Commserve y también se activó la eliminación del almacenamiento en la nube. . . los datos necesarios para reconstruir el índice se han eliminado de la biblioteca de la nube de Azure, por lo que los datos son físicamente inaccesibles en este momento.[170]

En otras palabras, Commvault explicó que el técnico encargado de las copias de respaldo había copiado los stubs del marcador de posición en lugar del contenido del archivo, y que esto resultó en la eliminación automática de los datos almacenados luego de que el técnico encargado de las copias de respaldo eliminó los clientes relevantes y las políticas de almacenamiento en Commvault.

El soporte de Commvault trabajó con el técnico encargado de las copias de respaldo durante las próximas semanas para brindar una mejor noción del impacto de la eliminación. El 15 de abril de 2021, el ingeniero de soporte de Commvault confirmó que 4.1 millones de archivos de código auxiliar se habían visto afectados; estos archivos de código auxiliar estaban "ubicados en los servidores de archivos de destino que estaban vinculados a los clientes de origen eliminados, que se eliminaron el 31 de marzo". El martes 20 de abril de 2021, el ingeniero de soporte de Commvault confirmó además que "los trabajos vinculados a los clientes eliminados antes del momento en que ocurrió el incidente [el 31 de marzo] todavía han fallado en la verificación [de datos] hasta el momento, lo que significa que ninguno de los datos de los trabajos afectados es recuperable."[172]

En la solicitud de soporte relacionado con el Incidente de la Pérdida de Datos, Commvault envió en un memorándum posteriormente la siguiente "Resolución de Incidentes":

> El cliente, sin saberlo, transfirió los stubs sin recuperar los datos y luego eliminó los clientes originales, por lo que los datos se eliminaron y no se pueden recuperar. Se trabajó con el departamento de desarrollo para proporcionar [una] lista de stubs afectados y los pasos/documentación adecuada para los escenarios de transferencia de stub solicitados para evitar que [el] problema siga adelante.[173]

Además, el soporte de Commvault concluyó que la causa subyacente del incidente fue "Commvault (Configuración y Producto)", mientras que la causa secundaria fue "Conocimiento General/Capacitación"[174]

5. Eliminaciones en Curso hasta agosto de 2021

A pesar de los problemas derivados de la eliminación de clientes y políticas de almacenamiento, el técnico encargado de las copias de respaldo continuó con la eliminación permanente de clientes desde el viernes 7 de mayo de 2021 hasta el jueves 5 de agosto de 2021.[175] En el **Apéndice B** se proporciona una lista completa de estas eliminaciones. Estas eliminaciones indican que el técnico encargado de las copias de respaldo no pudo apreciar la magnitud del incidente y que su eliminación de los clientes y políticas de almacenamiento no fue consistente con la directriz de Commvault. Sin embargo, en última instancia, los datos sujetos a estas eliminaciones se respaldaron en otro lugar o Commvault no los archivó, por lo que no se perdió ningún dato.

6. Evidencia del Motivo

Si bien examinar los motivos del técnico encargado de las copias de respaldo no es un propósito central de esta Investigación, vale la pena señalar que no descubrimos ninguna evidencia que sugiera que el técnico encargado de las copias de respaldo tuvo una intención maliciosa o un propósito delictivo al eliminar los datos de la Ciudad. Múltiples testigos ofrecieron su opinión de que no hubo malicia en las acciones del técnico encargado de las copias de respaldo, y ninguna evidencia documental o testamentaria sugirió que el técnico encargado de las copias de respaldo tuviera un motivo oculto para sus acciones. Sin embargo, en última instancia, las conclusiones de la investigación en cuanto a la intención del técnico encargado de las copias de respaldo serán competencia de los organismos encargados de realizar el cumplimiento de la ley que investigan el Incidente de la Pérdida de Datos, quienes pueden tener acceso a fuentes adicionales de evidencia y herramientas de investigación.

D. Descubrimiento y Auditoría de Agosto de 2021

1. Memorándum y Comunicado de Prensa del Abogado del Distrito Creuzot

El martes 3 de agosto de 2021, el Jefe de División del Gran Jurado y la División de Admisión de la Oficina del Abogado del Distrito se comunicó con un Jefe del DPD porque algunos fiscales habían oído hablar de una posible pérdida de datos.[176] El viernes 6 de agosto de 2021, ITS le dijo a la Oficina del Abogado del Distrito que la Ciudad había descubierto que se habían eliminado varios terabytes de datos del DPD durante una transferencia de datos en marzo.[177]

A esa reunión virtual asistieron el CIO de la Ciudad, el Director Adjunto de Infraestructura, varios Jefes del DPD y Abogado del Distrito Creuzot, junto con otros miembros del personal del Abogado del Distrito.[178] Abogado del Distrito Creuzot solicitó información precisa sobre la eliminación, y en la tarde del miércoles El 9 de agosto de 2021, DPD transmitió la siguiente información de ITS: que se habían eliminado aproximadamente 22 terabytes de datos del DPD, se recuperaron aproximadamente 14 terabytes y faltaban aproximadamente ocho terabytes y se creía que eran irrecuperables.[179]

Poco después, el Abogado del Distrito Creuzot publicó un memorándum interno a su personal y una carta a los jueces revelando los datos faltantes de la unidad de red del DPD.[180]

2. Auditoría de Agosto y Activación del Plan de Respuesta a Incidentes

Luego de la reunión con la Oficina del Abogado y el descubrimiento de archivos de FUSION inaccesibles por parte del DPD, el CIO de la Ciudad determinó que era necesaria una mayor evaluación.[182] Esta mayor evaluación también incluyó un mayor equipo, incluyendo el equipo del Oficial Principal de Seguridad de la Información de la Ciudad ("CISO") e individuos más allá de ITS, como consultores externos y soporte de Commvault. A mediados de agosto de 2021, Commvault realizó una revisión amplia de los servidores de la Ciudad.[183] Durante esta revisión, Commvault descubrió que el servidor FUSION de la Ciudad también se había visto afectado, no por la transferencia de datos o la eliminación de marzo, sino por una política de almacenamiento individual que el técnico encargado de las copias de respaldo había eliminado en enero de 2021.[184]

Debido a que Commvault descubrió que había habido una pérdida de datos adicional además del descubrimiento inicial, el 26 de agosto de 2021, el CISO activó el IRP de la Ciudad para realizar un análisis más exhaustivo de la pérdida de datos.[185] Una vez que se activó el IRP, el Director de IR trabajó con DPD e ITS para evaluar el incidente utilizando la matriz de riesgo descrita en IRP.[186] El Director de IR luego contrató a Commvault, al equipo de seguridad de ITS y al DPD.[187]

E. Esfuerzos de Recuperación de Datos

El CIO identificó dos conjuntos diferentes de esfuerzos de recuperación: uno que ocurrió antes del viernes 6 de agosto de 2021 y el otro luego del 6 de agosto de 2021.[188] En la fase inicial de recuperación, el técnico encargado de las copias de respaldo y el administrador de la nube trabajaron con Commvault y Microsoft durante las primeras semanas para evaluar y determinar opciones, métodos y enfoques para recuperar datos.[189] Commvault identificó entre 8.5 y 8.7 millones de stubs relevantes a través de su investigación, e ITS, en coordinación con DPD, determinó que mapearon a 17,484 casos DPD y 966,018 archivos relacionados con casos.[190] Muchos stubs relacionados con archivos que no estaban vinculados a un caso, como memorándums u otros documentos administrativos.[191] El equipo de recuperación trabajó con DPD para correlacionar los 17,484 casos con oficiales.[192]

Luego del 6 de agosto de 2021, ITS adoptó un enfoque diferente para la recuperación.[193] El CISO estuvo a cargo de las reuniones semanales de los viernes con el DPD y la Oficina del Abogado del Distrito a partir del 20 de agosto de 2021,[194] donde proporcionó actualizaciones sobre el esfuerzo de recuperación y qué datos se encontraron.[195] El CISO también solicitó que su Director Sénior de Cumplimiento, Riesgo y Descubrimiento Electrónico reúna un equipo (el "Equipo de Recuperación") para comenzar el proceso de determinar qué datos se perdieron y recuperarlos.[196] El DPD y la Oficina del Abogado del Distrito proporcionaron la CISO con dos listas de casos prioritarios para revisar: una lista inicial que contiene aproximadamente 600 casos priorizados y una segunda lista que contiene aproximadamente 1,100 casos priorizados.[197] El esfuerzo de recuperación no se centró en recuperar los archivos que se eliminaron, sino en buscar posibles duplicados de los datos en otras ubicaciones, como Office 365, OneDrive, SharePoint, Teams o cualquier otra ubicación secundaria.[198] El Equipo de Recuperación buscó en el Centro de Cumplimiento de Microsoft Office 365 de la Ciudad[199] para términos clave posiblemente relevantes para cada caso, como el nombre del acusado, la fecha del delito, la dirección, el nombre de la víctima, el tipo de caso, el número de caso o el nombre del oficial. [200] Si se encuentra una coincidencia en el contenido de un archivo, el archivo se copió en un almacenamiento individual que se creó específicamente para el esfuerzo de recuperación.[201]

Hasta la fecha, el equipo de recuperación continúa rastreando e informando las métricas sobre el esfuerzo de búsqueda de documentos al DPD y luego comparte las métricas con la Oficina del Abogado del Distrito. Actualmente, el Equipo de recuperación ha realizado búsquedas para aproximadamente el 36% de los 17,484 casos.[202] El Equipo de recuperación completa aproximadamente entre 100 y 200 búsquedas a la semana, a cuyo ritmo el CISO estima que el proyecto estará completo a fines de 2022.[203] Hasta la fecha, el Equipo de recuperación ha identificado 4,137,272 archivos que posiblemente coinciden con uno de los 966,018 archivos relacionados con los archivos perdidos relacionados con el caso.[204]

La siguiente tabla resume el estado actual del proceso de búsqueda del Equipo de Recuperación:[205]

Categoría	Volumen Total	Volumen completado hasta la fecha	Porcentaje completado hasta la fecha
Casos Prioritarios del Abogado del Distrito	1,081	1,081	100%
Todos los Casos	17,494	6,253	35.7%

VII. Evaluación del Origen

A. Teoría de la Imputación

Como se detalla en este Informe, la Investigación confirmó que la causa más inmediata de la pérdida de datos fueron los comandos de eliminación de Commvault que el técnico encargado de las copias de respaldo ejecutó durante la transferencia de datos. El técnico encargado de las copias de respaldo declaró que tomó estas medidas en un esfuerzo por "limpiar" los datos luego de transferir los servidores de la Ciudad de Azure al centro de datos local en el Concejo de la Ciudad de Dallas.[206] Cuando fue entrevistado, el técnico encargado de las copias de respaldo reconoció que había cometido un error, eliminando clientes relevantes sin verificar que sus datos estuvieran duplicados en otro lugar, y que no comprendía completamente las implicaciones de sus acciones.[207] No descubrimos ninguna indicación de que el técnico encargado de las copias de respaldo intentara causar la pérdida de datos u otro daño a los sistemas de la Ciudad; más bien, parece haber estado intentando llevar a cabo la transferencia de datos de acuerdo con su entendimiento sincero, aunque erróneo, del software Commvault. Las consecuencias de sus acciones fueron gravísimas. El técnico encargado de las copias de respaldo reconoció, y todos los demás entrevistados relevantes estuvieron de acuerdo, que las acciones del técnico encargado de las copias de respaldo dieron como resultado la eliminación de al menos 22 terabytes de datos almacenados. [K] Además, tanto el Director de TI como el Director Adjunto de Infraestructura indicaron que durante su investigación del Incidente de Perdida de Datos, llegaron a comprender que el proceso de "limpieza" del técnico encargado de las copias de respaldo no se realizó de acuerdo con el proceso de Commvault apropiado, ni fue requerido por la Orden de Cambio aprobada para el proyecto de transferencia.[208]

A pesar de tener la responsabilidad principal dentro de ITS para Commvault, la evidencia sugiere que el técnico encargado de las copias de respaldo no tenía suficiente experiencia con la plataforma para comprender sus complejidades y matices. El técnico encargado de las copias de respaldo completó un curso de capacitación de nivel básico de cinco días

[K] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 22 de noviembre de 2021; Entrevista de testigo el 15 de diciembre de 2021; Entrevista de Testigo el 5 de enero de 2022. Según nuestro trabajo de Confirmación, la pérdida inicial total de datos fue de aproximadamente 23.94 terabytes y la pérdida neta total de datos fue de aproximadamente 20.68 terabytes luego de la recuperación de 3.26 terabytes. Véase la Sección IX. Veintidós terabytes representan el volumen aproximado de la pérdida de datos que ITS y DPD habían identificado a principios de agosto de 2021. Entrevista de testigo el 22 de noviembre de 2021.

en 2018 cuando la Ciudad hizo la transición a Commvault. Esta capacitación abarcó temas como implementación, configuración de almacenamiento, políticas de almacenamiento, monitoreo, seguridad y administración de datos.[209] Sin embargo, el técnico encargado de las copias de respaldo no recibió capacitación adicional de Commvault hasta casi tres años luego, en 2021.[210] El Director Adjunto de Infraestructura instruyó al Director de TI enviar al técnico encargado de las copias de respaldo a la capacitación de Commvault debido a un incidente que ocurrió en 2019 en el que las copias de seguridad de Commvault dejaron de realizase luego de un cambio en la configuración del cortafuegos.[211] Aunque este incidente ocurrió en 2019, el técnico encargado de las copias de respaldo no recibió la capacitación adicional hasta enero 2021. De los tres cursos de capacitación complementarios a los que asistió, dos fueron repeticiones de cursos de nivel de entrada tomados en 2018.[212] En resumen, el conocimiento y la comprensión de Commvault del técnico encargado de las copias de respaldo eran inadecuados para su función y responsabilidades en ITS. En el futuro, el directorio de ITS debe garantizar que el conocimiento y las habilidades de los empleados sean acordes con sus funciones en el departamento.

Además, debería haberse implementado un proceso de autenticación de dos personas para los pasos clave en la transferencia de datos, como la eliminación de políticas y clientes. Esto podría haber dado lugar a preguntas sobre las eliminaciones por parte de una segunda persona capacitada. En términos más generales, se podría haber designado a una segunda persona en ITS como experto en la materia en Commvault para que evalúe y proporcione información sobre todos los pasos de transferencia de datos, incluyendo la Orden de Cambio y el proceso para implementarla. Se necesitaba más experiencia en Commvault dentro de ITS tanto a nivel de pares como de directivos. Si bien no hay garantía de que estos pasos, si se aplicaran, hubieran evitado la pérdida de datos, casi con certeza habrían reducido el riesgo.

B. Colaboradores Sistémicos

Si bien las acciones del técnico encargado de las copias de respaldo fueron la causa más inmediata de la pérdida de datos, hubo otros factores de riesgo presentes.

Primero, ITS no había implementado ningún plan de redundancia de datos antes del Incidente de la Pérdida de Datos, lo que podría haber permitido la recuperación de los datos perdidos. Por ejemplo, si hubiera existido una función de "eliminación temporal", todos los datos eliminados habrían permanecido disponibles y recuperables luego de la eliminación. Del mismo modo, si se hubiera utilizado un almacenamiento de datos secundario, la mayoría de los datos, si no todos, probablemente habrían sido recuperables. [L] Los entrevistados diferían en sus relatos sobre exactamente por qué los datos almacenados en la nube secundaria se eliminaron antes de las actividades de eliminación del técnico encargado de las copias de respaldo en Commvault. [M] Pero el punto más amplio y significativo es que ninguna de las partes responsables en ITS, incluyendo el técnico encargado de las copias de respaldo y sus supervisores, tomó medidas para garantizar que existiera *algún* tipo de redundancia de datos antes de realiza comandos en Commvault que planteó posibles consecuencias adversas para múltiples terabytes de datos críticos de la Ciudad.

Más allá de la necesidad de redundancia de datos, la Investigación identificó deficiencias en los procedimientos de ITS para revisar y aprobar Órdenes de Cambio y otros cambios en los sistemas de la Ciudad. La Ciudad cuenta con un proceso de administración de cambios para revisar los cambios propuestos[213] que incluye una Junta Asesora de Cambios ("CAB") compuesta por representantes de la empresa y de ITS[214] y una junta de revisión técnica que emite las aprobaciones finales.[215] Sin embargo, las personas que entrevistamos

---

[L] Esta capacidad de recuperación dependería precisamente de cómo se configuró el almacenamiento secundario, que nuevamente habría estado sujeto a la determinación en ITS para maximizar la redundancia y la capacidad de recuperación en caso de cualquier incidente.

[M] *Ver* nota al pie G.

quienes revisaron la Orden de Cambio reconocieron que no tenían mucha comprensión de la complejidad de Commvault, y esencialmente confiaban en el técnico encargado de las copias de respaldo para identificar y realiza los pasos apropiados.[216] También parece que se prestó poca atención a la identificación de posibles riesgos, como como falta de redundancia de datos, antes de realiza la Orden de Cambio. En el futuro, ITS debe evaluar de manera más cuidadosa y sistemática la necesidad de cambios significativos y cómo deben implementarse. La realización de la transferencia de datos de 2020-2021 parece haber sido un síntoma de una mayor falta de estrategia y planificación en torno a cómo la Ciudad pretendía utilizar la nube para satisfacer sus necesidades de tecnología de la información.

Las deficiencias en la comunicación y coordinación entre departamentos parecen haber contribuido al impacto de la pérdida de datos en toda la Ciudad. Por ejemplo, el almacenamiento de datos del servidor FUSION fue una sorpresa para el personal del DPD que administraba ese sistema, y solo se descubrió cuando el DPD necesitaba acceder a la evidencia de teléfonos celulares. [N] También escuchamos de varios interesados dentro del DPD que no hay suficiente consulta con el DPD en relación con la idoneidad y los criterios para almacenar datos para el departamento.[217] La mayoría de los entrevistados no sabían que el almacenamiento había comenzado, y aquellos que dijeron que no habían podido proporcionar información significativa en la determinación de los criterios de almacenamiento.[218] Además, existe una pregunta más amplia en torno a la conveniencia de almacenar los datos de los casos del DPD en los horarios actuales dado que, a diferencia de los archivos internos típicos que se vuelven obsoletos luego de un período de tiempo, estos datos se recopilan en el curso de investigaciones policiales activas que pueden tomar meses o años para ir a juicio. Estos ejemplos indican a una importante falta de coordinación, colaboración e intercambio de información entre ITS y los clientes internos a los que debe respaldar.

Además, como se detalló anteriormente, ITS advirtió de la posibilidad de una pérdida de datos a gran escala a más tardar el 5 de abril de 2021. El técnico encargado de las copias de respaldo sabía desde el 9 de abril de 2021 que los datos eliminados de las instalaciones de almacenamiento en la nube como resultado de las eliminaciones de su cliente y de la política de almacenamiento eran irrecuperables. [219] Según todos los informes, ITS, DPD, el CIO y el Administrador Adjunto de la Ciudad fueron informados en algún nivel sobre la supuesta pérdida de datos en las semanas siguientes. Sin embargo, es incierto si las partes ajenas a ITS entendieron completamente el posible alcance o las implicaciones de la pérdida de datos. Durante varios meses, la pérdida de pruebas se abordó esencialmente de manera fragmentada fuera de ITS, con oficiales individuales del DPD que enviaban solicitudes de apoyo para ayudar a localizar archivos individuales inaccesibles. Los mensajes a DPD con respecto a la capacidad de recuperación de los datos afectados siguieron siendo ambiguos en las semanas posteriores al descubrimiento de la pérdida de datos a pesar de que Commvault le informó a ITS el 9 de abril de 2021 que los datos relevantes eran irrecuperables en su formato original (es decir, desde el almacenamiento en la nube). Las discusiones entre ITS y Commvault a principios de abril indican un cambio de enfoque para obtener una comprensión detallada de los datos de Unidad de Almacenamiento K afectados.[O] Por el contrario, hasta que ITS compartió el impacto total de la pérdida de datos a principios de agosto, varios testigos del DPD creían que los datos no se perdieron de forma permanente, sino que fueron inaccesibles temporalmente pero posiblemente recuperables en el futuro.[220]

[N] Entrevista de testigo el 2 de diciembre de 2021; Entrevista del testigo el 8 de diciembre de 2021. Afortunadamente, debido a que el registro de teléfonos celulares en cuestión todavía estaba bajo custodia policial, los detectives pudieron solicitar una nueva orden de registro y recuperar la imagen forense. Entrevista de testigo el 9 de noviembre de 2021.

[O] El director de atención al cliente de Commvault confirmó que trabajaron con la Ciudad durante un período de tiempo para determinar el impacto de la eliminación y determinaron que los datos habían desaparecido. Entrevista de testigo el 20 de diciembre de 2021.

Finalmente, a pesar de la comprensión inicial de ITS del alcance de la pérdida de datos, la Ciudad no activó su IRP en abril de 2021 en respuesta al Incidente de la Pérdida de Datos. [221] El IRP de la Ciudad no se convocó hasta agosto, aproximadamente cuatro meses y medio luego se produjo la pérdida de datos. Existe un amplio acuerdo dentro de ITS de que esto debería haberse hecho en abril de 2021.[222] Es incierto con precisión y en qué medida convocar el IRP habría afectado la capacidad de la Ciudad para recuperar datos posiblemente, pero como mínimo, realizarlo habría ayudado a aclarar el alcance de la pérdida de datos. Además de ayudar a aclarar el alcance de la pérdida de datos, convocar el IRP en abril de 2021 podría haber permitido una mejor comunicación entre departamentos con respecto a los próximos pasos.

C. Evaluaciones de Informes de ITS

En relación con esta Investigación, revisamos el Informe ITS en profundidad y realizamos entrevistas detalladas con sus autores. La mayoría de las recomendaciones del Informe de ITS se relacionan integral con el desarrollo de los sistemas y procesos de ITS, en lugar de específicamente con el Incidente de la Pérdida de Datos.[223] Las recomendaciones específicas del Informe de ITS relacionadas con el Incidente de la Pérdida de Datos, como habilitar la función de "eliminación temporal" en el futuro—son generalmente consistentes con los de este Informe.

Si bien los desafíos más amplios e integrales de ITS no son el enfoque central de esta Investigación, la información que revisamos valida la necesidad de continuar con el desarrollo organizacional dentro de ITS, de acuerdo con los estándares reconocidos de la industria y las mejores prácticas. En octubre de 2020, el CIO contrató a Forrester, una empresa de investigación y asesoría, para realizar una evaluación de desarrollo de TI empresarial para la Ciudad luego de que observó ciertas deficiencias en su funcionamiento.[224] Forrester descubrió, en parte, que "existen desafíos importantes en la cultura de la organización, comunicaciones y colaboración. Un panorama complejo, la falta de procesos operativos desarrollados y la creciente deuda técnica plantean riesgos importantes que crean impedimentos para comprender el valor de aumentar la inversión en tecnología." [225]

La falta de desarrollo organizacional de ITS es el panorama en el que se desarrollaron los procesos y acciones específicos que llevaron al Incidente de la Pérdida de Datos. Abordar estos problemas integrales no tiene la misma urgencia inmediata que los orígenes específicos del Incidente de la Pérdida de Datos. Dicho esto, la Ciudad se vería beneficiada por el continuo desarrollo de ITS en esta área.

VIII. Efectos del Incidente de la Pérdida de Datos

A. Efectos en el DPD

Como se analizó anteriormente, los entrevistados indicaron que debido a la latencia de la red y los problemas de capacidad de almacenamiento, DPD históricamente no tenía un proceso consistente en todas las divisiones para almacenar evidencia digital.[226] Irónicamente, esta falta de una práctica consistente de almacenar archivos probablemente evitó el Incidente de la Pérdida de Datos tener consecuencias mucho más significativas en todo el DPD.[227] La Ciudad tiene la fortuna de que los datos del DPD se almacenaron en otros sitios, como por ejemplo los escritorios de los oficiales, correos electrónicos y discos duros y dispositivos USB externos del DPD.[228]

Desafortunadamente, la Unidad de Violencia Familiar del DPD parece ser inusual en el sentido de que fue la única unidad en la que los oficiales siguieron consistentemente un protocolo específico para almacenar evidencia digital en el Unidad de Almacenamiento K.[229] La intención detrás de esto es lógica y razonable. La Unidad de Violencia Familiar tiene miles de casos por año (más que cualquier otra unidad que investiga delitos contra las personas)[230] y numerosos oficiales que se transfieren dentro y fuera de la Unidad.[231] En consecuencia

el mantenimiento de una estricta adhesión a un protocolo de pruebas electrónicas coherente resultó muy beneficioso. Inesperadamente (y trágicamente), debido a que la Unidad de Violencia Familiar siguió un protocolo estricto para almacenar evidencia en la Unidad de Almacenamiento K, la Unidad de Violencia Familiar se vio afectada de manera desproporcionada por las eliminaciones de la Unidad de Almacenamiento K del Incidente de la Pérdida de Datos.[232] Esta pérdida se vio exacerbada por la transición de la Unidad de Violencia Familiar a un sistema de almacenamiento no en papel en 2019.[233]

Sin embargo, el personal del DPD expresó su escepticismo de que la pérdida de datos tendría un efecto significativo en el enjuiciamiento de casos penales que caen dentro de la jurisdicción de la Unidad de Violencia Familiar.[234] Esta creencia se basa en el hecho de que los casos de violencia familiar rara vez se suspenden porque las decisiones sobre si un caso será presentado a la Oficina del Abogado del Distrito se realizan con relativa rapidez en comparación con otros tipos de casos.[235] Un miembro de la Unidad de Violencia Familiar explicó que "prácticamente siempre sabemos quién es el sospechoso y podemos convertir nuestros casos en mucho más rápido [que otras divisiones]. A diferencia del robo en el que quizás nunca conozcan [al perpetrador], nosotros el 99,9 % de las veces, tenemos un sospechoso".[236] Como la pérdida de datos se restringió únicamente a los datos almacenados, que no incluirían datos de casos activos (y por lo tanto recientes) de violencia familiar, muchos en el DPD creen que cualquier dato perdido no fue probablemente se necesitarán en cualquier caso judicial activo.[237] Dicho esto, si bien es poco probable que se necesiten datos almacenados para un caso activo, esto no significa que los datos perdidos no tuvieran un posible valor probatorio actual o futuro. Dado que los delincuentes de violencia familiar tienen una alta tasa de reincidencia y, a menudo, cometen delitos violentos, la evidencia archivada perdida puede ser útil en casos futuros o ser necesaria para mantener una condena en la apelación de un caso.[238]

B. Efectos sobre la Oficina del Abogado del Distrito y el Sistema de Justicia Penal

Como se señaló anteriormente, la Oficina del Abogado del Distrito no tuvo conocimiento de la pérdida de datos hasta el 30 de julio de 2021.[239] Al principio, la Oficina del Abogado del distrito estaba muy preocupada por los casos que podrían haber sido afectados por el Incidente de la Pérdida de Datos.[240] También existía la preocupación de que la Oficina del Abogado del Distrito cumpliera con sus obligaciones bajo la Ley Michael Morton.[241] Esta Ley requiere que el Estado entregue evidencia exculpatoria y haga un registro de la evidencia que ha sido revelada a la defensa.

Afortunadamente, esas preocupaciones no se han materializado. La incertidumbre acerca de qué datos se perdieron realmente puede, en algunos casos limitados, estar ralentizando el ritmo de la acusación debido a las mociones del abogado defensor.[242] Un ADA también identificó un caso de asesinato en el que la fiscalía no pudo obtener una verificación rápida del DPD de que no faltaba ningún dato. Como resultado, la Oficina del Abogado del Distrito tuvo que anunciar que no estaba lista para ir a juicio y el sospechoso fue puesto en libertad bajo fianza de palabra.[243] Sin embargo, en general, los entrevistados de la Oficina del Abogado del Distrito confirmaron que la pérdida de datos no ha tenido un impacto sustancial hasta la fecha en la capacidad de la Oficina del Abogado del Distrito para procesar casos activos. [P] Tanto el DPD como la Oficina del Abogado del Distrito sintieron que la pérdida de datos no afectará sustancialmente la capacidad de la Oficina del Abogado del Distrito para llevar a cabo su misión de "mejorar la seguridad pública y el bienestar de la comunidad apoyando a las víctimas, responsabilizando a los a las personas que cometen delitos y haciendo participar a la comunidad en la prevención de daños".[244]

[P] Entrevista de testigo el 7 de diciembre de 2021; Entrevista de testigo el 7 de diciembre de 2021; Entrevista de Testigos el 25 de enero de 2022; Entrevista de un testigo el 25 de enero de 2022. Si bien la pérdida de datos no ha impedido que los fiscales presenten casos, en algunos casos los abogados defensores penales han citado el evento de la pérdida de datos al presentar mociones solicitando que una parte independiente revise el archivo del caso para verificar que esté completo. Entrevista de testigo el 7 de diciembre de 2021; Entrevista de testigo el 25 de enero de 2022. Hasta ahora, la mayoría, si no todas, de tales mociones han sido negadas. Entrevista de testigo el 7 de diciembre de 2021; Entrevista de testigo el 25 de enero de 2022.

IX. Volumen de Datos Perdidos

La Investigación validó el volumen de datos perdidos en el Incidente de la Pérdida de Datos. Los detalles de este trabajo se establecen en el **Apéndice C**, pero en un alto nivel, nuestro proceso de Confirmación incluyó conversaciones con ITS y una revisión de la documentación y los datos relevantes, incluyendo los registros de Commvault y los informes del panel de Azure de la Ciudad. Validamos que la Ciudad perdió un total neto de aproximadamente 20.68 terabytes de datos almacenados en su formato original, luego de recuperar aproximadamente 3.26 terabytes que inicialmente se creían perdidos. Todos los datos perdidos provinieron del Unidad de Almacenamiento K de la Ciudad (incluyendo la Violencia Familiar) y los servidores FUSION.

La siguiente tabla resume los datos brutos y netos aproximados perdidos de cada categoría de servidor:

Servidores	Pérdida de Datos Inicial	Volumen Recuperado	Pérdida Neta de Datos
Unidad de Almacenamiento K	10.77 TB[245]	3.26 TB[246]	7.51 TB[247]
FUSION	13.17 TB[248]	0 TB[249]	13.17 TB
Total:	23.94 TB	3.26 TB	20.68 TB

Como se ha señalado, en el **Apéndice C** se proporcionan más detalles.

X. Datos Perdidos Anteriormente

Revisamos documentos e interrogamos a testigos con respecto a las políticas y procedimientos históricos de la Ciudad para el almacenamiento, respaldo y archivo de sus datos.[250] La Investigación no identificó ningún Incidente de Pérdida de Datos notable que no sea el Incidente de la Pérdida de Datos en cuestión aquí.

XI. Recomendaciones

Basado en esta Investigación, la Ciudad debe considerar al menos los siguientes pasos para mitigar el riesgo de que ocurran eventos similares de pérdida de datos en el futuro.

A. Protección de Datos y Redundancia

Es necesario establecer controles de redundancia adecuados, particularmente en lo que respecta a los datos almacenados. Las oportunidades de mejora incluyen las siguientes:

- Diseñar e implementar un proceso de prueba y verificación para la transferencia de datos. Esto debe incluir un proceso para probar y verificar el proceso de transferencia de datos antes de cualquier transferencia o eliminación de datos. El proceso de verificación debe incluir un entorno de prueba con datos de prueba que se puedan utilizar para minimizar el riesgo para el entorno de producción.

- Requerir la autorización de dos personas para cualquier proceso que pueda tener un impacto importante en el ámbito si no se realiza de manera adecuada o de acuerdo con la política (como las eliminaciones de la política de almacenamiento y el cliente).

- Implementar la función de "eliminación temporal" en Azure. Entendemos que esto se ha hecho y recomendamos que ITS mantenga la funcionalidad de "eliminación temporal" en su lugar. ITS también debe asegurarse de que cualquier característica de protección análoga esté habilitada en cualquier sistema futuro de copia de respaldo y archivo que la Ciudad pueda establecer.

B. Consultar a los Expertos del Proveedor según Sea Necesario

ITS debe planificar (y presupuestar) la consulta con expertos externos al emprender proyectos fundamentales, como la transferencia de datos y la implementación de soluciones tecnológicas en toda la empresa.

- Independientemente del sistema de copia de respaldo y archivo que se utilice, ITS debe involucrar a expertos en la materia durante la planificación de la transferencia de datos y, si es posible, durante cualquier transferencia de datos críticos. La consulta debe incluir la Confirmación de cambios relevantes o impactantes o modificaciones específicas propuestas a los clientes y políticas adjuntas a los datos del servidor transferidos.

- ITS debe involucrar a otros expertos proveedores, como expertos en la materia, cuando sea necesario en relación con proyectos futuros.

C. Recursos y Personal del DPD

Como se describió anteriormente, la falta de recursos de TI adecuados en DPD constituyó un factor que contribuyó al Incidente de la Pérdida de Datos. En el futuro, la Ciudad debe tomarse el tiempo para evaluar cuidadosamente las necesidades presupuestarias, de recursos y de personal del DPD con la meta de remediar los problemas identificados en este Informe. En particular:

- Como se describe de manera más general a continuación, la Ciudad debería considerar establecer un CIO Departamental en DPD.

- Se debe asignar a DPD un presupuesto adecuado para desarrollar su infraestructura de TI, lo que incluye añadir almacenamiento adicional en las instalaciones y/o en la nube, capacidad de Evidence.com y rendimiento/ancho de banda de la red, según sea necesario.

- Además de la asignación presupuestaria, el proceso de adquisición de infraestructura crítica debe reflejar los aportes de las personas que entienden las necesidades únicas de datos y almacenamiento del DPD. También debe reflejar los resultados de cualquier evaluación de infraestructura de TI (discutida a continuación) y/o plan estratégico que DPD pueda establecer para su futuro desarrollo de TI a largo plazo.

- La Ciudad debe considerar realizar una evaluación completa de la infraestructura de TI para el DPD a fin de identificar completamente todas las necesidades de recursos (incluyendo las que pueden estar más allá del alcance de este Informe). Esto podría establecer proyectos y objetivos específicos para implementar cualquier recomendación que surja de la evaluación.

D. Necesidades de Capacitación y Personal de ITS

ITS debe considerar expandir y perfeccionar la capacitación de sus empleados para garantizar que adquieran y mantengan la experiencia adecuada en la materia con respecto a los sistemas fundamentales.[Q] En particular, la Ciudad debe:

- Asegurarse de que el personal de ITS designado como expertos en la materia técnica tenga la capacitación adecuada con la tecnología que se utiliza.

- Solicitar información de proveedores clave (como Commvault y Microsoft) sobre qué habilidades y capacitación se necesitarían para tener uno o más expertos en la materia completamente calificados en el personal de ITS.

- Capacitar suficientemente a los empleados para garantizar que no haya un solo punto de fallo para los sistemas clave si un recurso ITS en particular no está disponible.

E. Cuestiones Presupuestarias y Asignación

ITS indicó que actualmente cuenta con un presupuesto adecuado para las necesidades actuales. [251] Sin embargo, los aportes de importantes interesados, como el DPD y la Oficina del Abogado, no parecen ser tomados en cuenta en su totalidad. Según se informa, las solicitudes de asuntos necesarios se rechazan habitualmente debido a la falta de presupuesto. Si bien el proceso general de adquisición y presupuestación de la Ciudad está más allá del alcance de este Informe, las recomendaciones preliminares para el futuro incluyen:

- La Ciudad debe garantizar un proceso de adquisiciones más fluido y optimizado que funcione bien para los diferentes interesados al permitirles aprovechar de manera eficiente el gasto disponible en TI.

- En la medida en que las restricciones presupuestarias sean un problema, las necesidades presupuestarias adicionales relevantes para la copia de respaldo/transferencia de datos deben evaluarse adecuadamente y se les debe dar la importancia adecuada considerando los eventos descritos en este Informe.

- El control y la planificación presupuestarios deben incluir aportes de los interesados en la administración de datos de ITS. Por ejemplo, esta Investigación reveló que la persona propietaria de la partida presupuestaria para la transferencia a la nube no formaba parte de la toma de decisiones en torno a la transferencia y, por lo tanto, no podía proporcionar información valiosa.[252] Tales interesados deben participar en las conversaciones sobre el establecimiento del presupuesto para garantizar que las necesidades de datos de la Ciudad se satisfagan adecuadamente.

[Q] Estas recomendaciones no abordan la sustitución del puesto de técnico encargado de las copias de respaldo en ITS, ya que entendemos que el departamento ha contratado a dos nuevos expertos desde el Incidente de la Pérdida de Datos para que sean expertos en la materia y lideren los esfuerzos de ITS con respecto a Commvault.

F. Protocolos y Prácticas de Administración de TI

Según nuestras entrevistas, parece que el modelo operativo dentro de ITS ha sido tradicionalmente de naturaleza reactiva y en gran medida aislado de los departamentos de clientes. ITS debería tratar de cambiar a un modelo operativo más estratégico y proactivo. En particular:

- La Ciudad debe desarrollar una visión cohesiva de dónde quiere estar a corto, mediano y largo plazo (planificación de al menos 3 a 5 años). En relación con ese proceso, ITS debe trabajar con los diversos interesados para comprender lo que necesitan en términos de tecnología y personal. Entre otras cosas, esto ayudará a informar las decisiones sobre gastos y priorización para resolver conflictos de recursos.

- La Ciudad debe implementar un plan claramente definido y cuidadosamente pensado basado en un enfoque estratégico para construir una arquitectura de respaldo que funcione para el estado actual y el crecimiento planificado. Este plan tendría que tener en cuenta sistemáticamente todas las consideraciones correspondientes. Por ejemplo, la Investigación descubrió un patrón de toma de decisiones dentro de ITS que parece haberse basado únicamente en el costo. En el futuro, ITS debe encontrar formas de evaluar las necesidades teniendo en cuenta al crecimiento estratégico, con aportes en torno a las necesidades comerciales de los interesados apropiados en los departamentos afectados, y considerando las posibles implicaciones de primer y segundo orden de los cursos de acción alternativos.

- Como parte de la planificación del crecimiento estratégico, se debe prestar atención adicional a la identificación y búsqueda de soluciones de almacenamiento más extensibles. El volumen de datos de la Ciudad ha crecido a un ritmo vertiginoso y seguirá haciéndolo. ITS debe investigar opciones de almacenamiento de datos que sean fácilmente extensibles para satisfacer las necesidades cambiantes de la Ciudad, particularmente el DPD y otros departamentos de seguridad pública que necesitan administrar grandes volúmenes de datos críticos.

G. Protocolos y Prácticas Departamentales

La Ciudad debe realizar una revisión de las políticas y procedimientos departamentales relacionados con el almacenamiento y respaldo de datos. En particular:

- Esto debe incluir garantizar que los departamentos almacenen los datos de manera constante en almacenamientos con debidas copias de respaldo.

- En relación con una revisión de las prácticas de almacenamiento de datos, se necesita una revisión de la infraestructura y el ancho de banda para los departamentos de alta prioridad (como el DPD). Como se analizó, varios entrevistados del DPD se quejaron de las velocidades excesivamente lentas de carga y descarga, lo que desalentó el cumplimiento de las directrices de almacenamiento actuales. La atención no puede centrarse únicamente en crear políticas y procedimientos más consistentes en torno al almacenamiento de datos si la infraestructura subyacente no permite que los departamentos esenciales implementen esas políticas de manera eficiente.

H. Comunicación y Coordinación Interdepartamental

Basado en esta Investigación, las dificultades de comunicación tanto particularizadas como sistémicas entre ITS y sus departamentos de clientes (principalmente DPD) afectaron el Incidente de la Pérdida de Datos y posteriores esfuerzos de corrección. Por ejemplo, los departamentos

fuera de ITS aparentemente no tenían conocimiento de cómo funcionaba el sistema de almacenamiento de Commvault y qué datos se almacenarían. En consecuencia, estos departamentos no estaban en condiciones de comprender el posible alcance o las implicaciones del Incidente de la Pérdida de Datos en el momento en que ocurrió. En particular, a pesar de la disponibilidad de enlaces de ITS, parece haber una desconexión sustancial entre ITS y DPD. Numerosos entrevistados, no limitados solo a los entrevistados por DPD, se quejaron de que ITS carece de una mentalidad de servicio al cliente y no comprende las herramientas tecnológicas que el DPD necesita para funcionar con éxito.[253] Por lo tanto, en el futuro:

- Los interesados en los datos deben proporcionar los requisitos comerciales/requisitos de retención de datos e ITS debe realizar recomendaciones para satisfacer esas necesidades. Por ejemplo, la mayoría de los datos del DPD son pruebas electrónicas que respaldan las investigaciones penales, lo cual es muy diferente de los archivos comerciales típicos y debe tratarse con mucho cuidado en estrecha colaboración con el DPD. Además, como se señaló, parece que el DPD no siguió de manera consistente los protocolos para el almacenamiento de evidencia digital debido a problemas de latencia de red y ancho de banda. Cualquier problema de este tipo debe plantearse y abordarse de manera integral como parte del proceso de coordinación interdepartamental.

- La Ciudad debe desarrollar procesos generalizados para mejorar la comunicación/coordinación interdepartamental y la visibilidad para todos los interesados. Por ejemplo, cuando ITS eliminó la instalación secundaria de almacenamiento en la nube en Arizona, el responsable de recuperación en caso de desastres y otros propietarios de aplicaciones no estaban al tanto de estas decisiones, lo que hizo que la Ciudad fuera vulnerable desde la perspectiva de la recuperación de datos.

I. CIO Departamentales de TI

Como se mencionó anteriormente, la Ciudad debe considerar establecer funciones específicas de Director de Información ("CIO") dentro de los departamentos (como el DPD) que almacenan datos críticos para la Ciudad. Estas personas reportarían a los jefes de departamento, como el Jefe de Policía del DPD. Si bien ITS actualmente tiene enlaces que son responsables de comunicarse con los departamentos de clientes, son empleados de ITS y no parecen estar muy familiarizados con la infraestructura de TI, los procesos o los casos de uso específicos de los datos de los departamentos. Establecer funciones de CIO formalizados en departamentos clave como el DPD podría servir como un paso significativo para mitigar el riesgo de que ocurra un evento de pérdida de datos similar en el futuro. Los CIO departamentales también podrían tener la tarea de abogar por sus departamentos en relación con las discusiones presupuestarias de TI y educar a los responsables de ITS sobre las necesidades específicas del departamento.

J. Evaluación de la Criticidad de los Datos en Toda la Ciudad

La Ciudad debe realizar una evaluación de la clasificación y la criticidad de los datos en toda la Ciudad, en consonancia con las recomendaciones del Informe de ITS y el trabajo que ya está realizando el equipo del CISO para el desarrollo de TI de la Ciudad.

- La evaluación debe involucrar a ITS, representantes de otros departamentos relevantes y cualquier otro interesado clave. Los representantes departamentales deben ser personas que tengan una comprensión técnica adecuada de los sistemas de TI de la Ciudad y estén bien entendidos en las necesidades de TI de sus departamentos, así como en las metas de crecimiento estratégico.

- Dicha evaluación puede tener un alcance estratégico, pero debe centrarse en ayudar a determinar, entre otras cosas, los tipos de datos que almacena cada departamento, los sistemas relevantes y los custodios de datos, si los datos se respaldan y cuánto tiempo se necesita respaldar el impacto si se pierden los datos y los límites aceptables de recuperación ante desastres para el Objetivo de Tiempo de Recuperación ("RTO") y el Objetivo de Punto de Recuperación ("RPO") para sistemas fundamentales como los que utilizan los departamentos de seguridad pública. Esta información se puede utilizar para informar el proceso de presupuestación y planificación para el desarrollo del sistema de TI de la Ciudad en el futuro.

K. Reformulación del Esfuerzo de Recuperación de Datos

Actualmente, la Ciudad ha invertido una cantidad considerable de tiempo y recursos, tanto en empleados como en dólares totales, en su esfuerzo de búsqueda de descubrimiento electrónico, y el CISO estima que gastará $750,000 en su totalidad.[254] Si bien el esfuerzo de búsqueda es admirable por su minuciosidad, el beneficio de las búsquedas continuas de descubrimiento electrónico caso por caso hasta fines de 2022 es posiblemente cuestionable dado el costo relativo. Recomendamos que la Ciudad considere más a fondo los posibles enfoques para priorizar los casos que son el objetivo del esfuerzo de descubrimiento electrónico, identificando y almacenando posibles datos relacionados con casos de una manera menos intensiva en mano de obra, y considerar seriamente la posibilidad de detener el esfuerzo en algún momento antes de identificar los expedientes de los 17,484 casos identificados.

XII. Conclusión

Es fundamental que el DPD y sus oficiales puedan recopilar y mantener pruebas de manera segura que proteja la integridad de cada investigación.[255] Es igualmente crítico que se mantenga y proteja la integridad de las pruebas digitales en las que se basa la Oficina del Abogado del Distrito para sus procesamientos. Las pruebas digitales son un factor clave en muchos, si no en la gran mayoría, de los casos actuales, y la falta de una administración de datos fiable podría poner en peligro el éxito de la aplicación de la ley en la comunidad de Dallas. [256] La Oficina del Abogado del Distrito debe ser capaz de recibir grandes cantidades de datos de entidades encargadas del cumplimiento de la ley a las que sirve, almacenando esos datos de forma segura y adecuada, y luego convirtiéndolos en evidencia que se puede presentar en ante una corte de justicia sujeto a estrictos estándares probatorios. Cuando la evidencia digital se elimina, se extravía o se manipula incorrectamente, puede llevar a la desestimación de los costos penales o evitar que un jurado vea evidencia valiosa que necesita para determinar la culpabilidad o la inocencia.

Desafortunadamente, el Incidente de la Pérdida de Datos puso en peligro directamente la misión de cumplimiento de la ley de la Ciudad y es un síntoma de desafíos mucho más amplios que tienen el potencial de plantear desafíos significativos en el futuro. La Ciudad tiene la fortuna de que el impacto del Incidente de la Pérdida de Datos no haya sido más significativo.

Nuestro informe ha identificado tanto los orígenes específicos como los factores sistémicos que contribuyeron al Incidente de la Pérdida de Datos, así como recomendaciones de medidas correctivas y oportunidades para el desarrollo continuo de las funciones y procesos de TI de la Ciudad. Nuestra evaluación a este respecto se basa en nuestra experiencia y juicio independiente aplicado a las declaraciones de los testigos que entrevistamos, y el voluminoso registro que nos ha proporcionado la Ciudad.

Si bien este Informe puede ayudar a confirmar las circunstancias y el origen del Incidente de la Pérdida de Datos, queda mucho trabajo por realizar para abordar los problemas que hicieron posible el Incidente de la Pérdida de Datos. Esperamos que este Informe sea útil para la Ciudad, ya que continúa evaluando los próximos pasos en los esfuerzos de corrección, así como la estrategia a largo plazo con respecto a los datos relacionados con el DPD.

XIII. Apéndices

A. Apéndice A: Cronología de Eventos Clave Relacionados con el Incidente de Pérdida de Datos

Fecha/Horario*	Descripción del Evento
2018	ITS implementa Commvault como su solución de copia de respaldo y eventualmente expande su uso de Commvault para incluir el almacenamiento.[257]
Abril de 2019	ITS crea su cuenta de almacenamiento de Microsoft Azure en Arizona.[258]
Junio de 2020	La Ciudad contrata a un nuevo Director de Información ("CIO").[259]
23 - 28 de julio de 2020	El Director de TI para Servidores y Redes envía un correo electrónico a un representante de Microsoft solicitando ayuda para comprender la configuración de almacenamiento y los centros de datos de la Ciudad, particularmente en relación con los grandes costos del ancho de banda.[260]
21 de agosto de 2020	El Director de TI para Servidores y Redes envía un correo electrónico al Director Adjunto de Infraestructura con respecto al costo del almacenamiento en la nube de Azure y las posibles alternativas.[261]
24 de agosto de 2020	Una Orden de Cambio que rige la transferencia de datos planificada para principios de 2021 desde la nube de Azure al almacenamiento local en el Concejo de la Ciudad de Dallas se presenta como un cambio "Normal".[262]
Octubre de 2020	El CIO contratado por Bewly contrata a la firma de investigación y asesoría Forrester para realizar una evaluación de desarrollo de TI de ITS.[263]
Septiembre de 2020	ITS realiza ciertos ajustes técnicos en sus cuentas de almacenamiento de Microsoft Azure en Arizona para reducir los costos de salida.[264]
16 de diciembre de 2020	Forrester comparte los resultados de su evaluación de desarrollo de TI con los directivos de ITS. La evaluación enumera las fortalezas, las oportunidades clave, los desafíos y las recomendaciones para ITS, incluyendo las recomendaciones relacionadas con la recuperación ante desastres y el desarrollo de TI.[265]
10 de enero de 2021	El Director de TI para Servidores y Redes envía un correo electrónico al Director Adjunto de Infraestructura y señala que el almacenamiento en Arizona se eliminará al final de la semana.[266]
23 de enero de 2021	ITS desactiva el archivo antes de la transferencia de datos.[267]
Enero de 2021	El técnico encargado de las copias de respaldo lleva a cabo el plan de transferencia de datos y transfiere todos los datos del servidor en la nube de Azure a una ubicación local en el Concejo de la Ciudad de Dallas.[268]

* Todos los horarios de CDT.

Fecha/Horario*	Descripción del Evento
Febrero de 2021	El técnico encargado de las copias de respaldo retira cuatro de los servidores transferidos en Azure, lo que da como resultado que no se reportaran errores o problemas en ese momento.[269]
4 de marzo de 2021	El técnico encargado de las copias de respaldo envía un correo electrónico al administrador de la nube de ITS para informarle que ha puesto fuera de funcionamiento el antiguo almacenamiento en la nube del DPD desde el día anterior, y que supervisará y confirmará cuándo podría eliminarse el almacenamiento antiguo. Él escribe que probablemente sería una buena idea esperar al menos una o dos semanas para asegurarse de que ningún usuario intentara acceder a los archivos (aparentemente para asegurarse de que todos los archivos aún estuvieran accesibles).[270]
30 - 31 de marzo de 2021	El técnico encargado de las copias de respaldo comienza el proceso de "limpieza" de los datos que cree que ya no son necesarios luego de la transferencia mediante la realización de una serie de eliminaciones de clientes y políticas de almacenamiento. En el transcurso de dos días, el técnico encargado de las copias de respaldo realiza un total de 17 eliminaciones permanentes de clientes y cinco eliminaciones de políticas de almacenamiento.[271]
5 de abril de 2021	ITS comienza a recibir solicitudes de soporte del DPD con respecto a archivos de la Unidad de Almacenamiento K inaccesibles.[272]
5 de abril de 2021 11:00 AM	El técnico encargado de las copias de respaldo cancela todas las eliminaciones de datos de Commvault y detiene el proceso de "limpieza".[273]
5 de abril de 2021 12:08 PM	El técnico encargado de las copias de respaldo crea una solicitud de soporte con Commvault con la descripción: "Los archivos almacenados y de stub no se recuperan".[274]
5 de abril de 2021 12:30 PM	El técnico encargado de las copias de respaldo notifica a su supervisor, el Director de TI para Servidores y Redes, que cometió un error durante la limpieza la semana anterior.[275]
5 de abril de 2021 5:22 PM	El soporte de Commvault identifica que "las recuperaciones de stubs estaban fallando porque los stubs estaban vinculados a clientes eliminados que se eliminaron la semana pasada".[276]
6 de abril de 2021 7:00 AM	El Director de TI para Servidores y Redes informa al Director Adjunto de Infraestructura sobre el incidente.[277]
6 de abril de 2021 6:08 PM	Un ingeniero de soporte de Commvault realizó una búsqueda de stubs averiados en los servidores de la Ciudad. El ingeniero de soporte de Commvault también aconseja al técnico encargado de las copias de respaldo que "no elimine ningún cliente, ya que ahí es donde se encuentran los datos de la copia de respaldo".[278]
6 de abril de 2021 9:27 AM	El Director Adjunto de Infraestructura informa al CIO de la situación.[279]
7 de abril de 2021 (mañana)	El Director Adjunto de Infraestructura y el CIO discuten por teléfono la transferencia de datos y los posibles impactos.[280]

Fecha/Horario*	Descripción del Evento
9 de abril de 2021 4:58 PM	El ingeniero de soporte de Commvault le informa al técnico encargado de las copias de respaldo que la solicitud se derivará al equipo de desarrollo de Commvault para que "puedan ayudar a proporcionar los pasos a seguir para compilar una lista de stubs irrecuperables".[281]
9 de abril de 2021 5:14 PM	El soporte de Commvault confirma que "gran parte de los datos parecen ser irrecuperables ya que se deshabilitó la 'eliminación temporal' en la cuenta de almacenamiento de Azure, y ahora el cliente está buscando un informe [sic] de todos los archivos afectados".[282]
10 de abril de 2021	El Director de TI para Servidores y Redes informa al Director Sénior de TI de Seguridad Pública y al equipo de TI que asiste al DPD que, debido a un paso omitido en la transferencia de datos, los archivos de varias divisiones se eliminaron y es posible que no se puedan recuperar. El equipo de ITS desarrolla una hoja de cálculo para comenzar a reducir el alcance de lo que se perdió.[283]
12 de abril de 2021	El Director Sénior de IT para Seguridad Pública anuncia en la reunión del personal de mando del DPD en la sede del DPD que ITS está trabajando para solucionar un problema que afecta al Unidad de Almacenamiento K.[284]
13 de abril de 2021 2:53 PM	El CIO notifica al Administrador Adjunto de la Ciudad por correo electrónico sobre una "pérdida masiva de datos que se produce debido a un error durante la realización de transferencias de archivos de rutina desde el almacenamiento de Azure al almacenamiento del Concejo de la Ciudad de los archivos del DPD… Estamos organizando una reunión con los directivos del DPD esta tarde."[285]
13 de abril de 2021	El CIO organiza una reunión con los responsables del DPD para trabajar en el proceso de informar cualquier problema relacionado con esta pérdida de datos.[286]
15 de abril de 2021 11:43 AM	El ingeniero de soporte de Commvault confirma que 4.1 millones de archivos de stub se han visto afectados.[287]
19 de abril de 2021	El Jefe de Policía del DPD publica un memorándum interno para todo el personal del departamento, pidiéndole a todo el personal que verifique si faltan archivos o carpetas y siga los pasos identificados para "restaurar" esos archivos o carpetas.[288]
20 de abril de 2021 1:14 PM	El ingeniero de soporte de Commvault confirma que "los trabajos relacionados a los clientes eliminados antes del momento en que se produjo el incidente [el 31 de marzo] han fallado todos en la verificación [de datos] hasta ahora, lo que significa que ninguno de los datos de los trabajos afectados es recuperable."[289]
22 de abril de 2021	El CIO solicita la asistencia del DPD para investigar la pérdida de datos.[290]
27 de abril de 2021 3:28 PM	El técnico encargado de las copias de respaldo escribe un documento titulado "Escenarios de Transferencia de Datos de la Ciudad de Dallas", en el que describe el proceso que siguió al transferir los datos almacenados. El técnico encargado de las copias de respaldo proporciona el documento al soporte de Commvault.[291]

Fecha/Horario*	Descripción del Evento
28 de abril - 7 de mayo de 2021	El ingeniero de soporte de Commvault revisa el documento "Escenarios de Transferencia de Datos de la Ciudad de Dallas" con miembros de los equipos de soporte, desarrollo y servicios profesionales de Commvault. El ingeniero de soporte de Commvault señala que el documento contiene "pasos incorrectos". El soporte de Commvault mejora los pasos para la transferencia de archivos y entrega una copia editada del documento al técnico encargado de las copias de respaldo.[292]
7 de mayo de 2021	El técnico encargado de las copias de respaldo lleva a cabo una eliminación permanente de cliente.[293]
14 de mayo de 2021	El técnico encargado de las copias de respaldo se comunica con Commvault y solicita una demostración con Servicios Profesionales de los procedimientos y pasos exactos para la transferencia de datos.[294]
18 de mayo de 2021	El técnico encargado de las copias de respaldo realiza un seguimiento con Commvault y nuevamente solicita programar una demostración con Servicios Profesionales.[295]
19 de mayo de 2021	El técnico encargado de las copias de respaldo lleva a cabo una eliminación permanente de cliente.[296]
7 de junio de 2021	El técnico encargado de las copias de respaldo lleva a cabo una eliminación permanente de cliente.[297]
Alrededor del 17 de junio de 2021	Ocurre la demostración de escenarios de transferencia con Servicios Profesionales. [298]
21 de junio de 2021	El técnico encargado de las copias de respaldo lleva a cabo nueve eliminaciones permanentes de cliente.[299]
23 de junio de 2021	El técnico encargado de las copias de respaldo lleva a cabo 19 eliminaciones permanentes de cliente.[300]
24 de junio de 2021	El técnico encargado de las copias de respaldo lleva a cabo cuatro eliminaciones permanentes de cliente.[301]
25 de junio de 2021	El técnico encargado de las copias de respaldo lleva a cabo una eliminación permanente de cliente.[302]
23 de junio de 2021	El técnico encargado de las copias de respaldo lleva a cabo 19 eliminaciones permanentes de cliente.[303]
29 de junio de 2021	El técnico encargado de las copias de respaldo lleva a cabo dos eliminaciones permanentes de cliente.[304]
30 de julio de 2021	Los oficiales informan al Abogado Adjunto del Distrito del condado de Dallas que ciertos archivos del DPD relacionados con un enjuiciamiento pendiente ya no estaban disponibles en Unidad de Almacenamiento K.[305]
Principios a mediados de agosto de 2021	DPD informa a ITS que no puede acceder a los archivos de FUSION.[306]
3 de agosto de 2021 3:56 PM	Un Jefe de División de la Oficina del Abogado del Distrito se comunica con un Jefe Adjunto Ejecutivo del DPD para obtener más información sobre la pérdida de datos.[307]

Fecha/Horario*	Descripción del Evento
4 de agosto de 2021	DPD envía una solicitud de la Oficina del Abogado del Distrito para obtener más información sobre la pérdida de datos a ITS. El Director de Relaciones Comerciales de ITS reenvía el correo electrónico al Equipo Ejecutivo de ITS.[308]
5 de agosto de 2021	El técnico encargado de las copias de respaldo lleva a cabo 11 eliminaciones permanentes de cliente.[309]
6 de agosto de 2021	DPD e ITS informan a la Oficina del Abogado del Distrito que, en abril de 2021, la Ciudad descubrió que se habían eliminado varios terabytes de datos del DPD durante una transferencia de datos de una unidad de red del DPD.[310]
9 de agosto de 2021	ITS informa a DPD, quien luego informa a la Oficina del Abogado del Distrito, que entre el 21 de marzo de 2021 y el 5 de abril de 2021, se eliminaron aproximadamente 22 terabytes de datos del DPD en el transcurso de unos días, y aproximadamente ocho terabytes siguen faltando y se cree que son irrecuperable.[311]
11 de agosto de 2021	El Abogado del Distrito Penal del Condado de Dallas, John Creuzot, emite un memorándum sobre la pérdida de datos.[312]
11 de agosto de 2021	El problema de la pérdida de datos comienza a recibir la atención de los medios.
12 de agosto de 2021	El alcalde Eric Johnson envía un memorándum a los concejales de la Ciudad B. Adam McGough y Cara Mendelsohn, afirmando que estaba "sorprendido" por la noticia de la pérdida de datos y solicitó que los miembros del concejo "convoquen una reunión especial conjunta de sus comités para analizar la eliminación de datos, la preocupante falta de comunicación por parte del personal de la Ciudad sobre lo ocurrido y los pasos que se están tomando para resolver el asunto y prevenir futuras consecuencias."[313]
12 de agosto de 2021	El técnico encargado de las copias de respaldo y el Director de TI se reúnen para una "entrevista de licencia administrativa".[314]
13 de agosto de 2021	Varios medios de comunicación, incluyendo ABC News, Fox News, *Dallas Morning News* y *New York Post*, informan que Jonathan Pitts, un sospechoso de asesinato que estaba programado para ir a juicio esa misma semana, fue liberado bajo fianza de palabra de la cárcel del Condado de Dallas luego de que se determinó que la evidencia en su contra podría haberse perdido.[315]
18 de agosto de 2021	Se informa al Concejo de la Ciudad de Dallas sobre la pérdida de datos durante una sesión ejecutiva a puertas cerradas.[316]
Mediados de agosto de 2021	Commvault realiza una auditoría de políticas y clientes eliminados, lo que implica investigar otros servidores. Commvault determina que el servidor FUSION también se ha visto afectado debido a una política de almacenamiento eliminada en enero de 2021.[317]
20 de agosto de 2021	El CISO comienza a organizar reuniones semanales regulares con el DPD y la Oficina del Abogado del Distrito, brindando actualizaciones sobre el esfuerzo de recuperación de datos.[318]

Fecha/Horario*	Descripción del Evento
26 de agosto de 2021 6:25 PM	El CISO activa el Plan de respuesta a incidentes para realizar un análisis de la pérdida de datos, elevándolo al nivel de gravedad más alto según el Plan.[319]
26 de agosto de 2021 6:30 PM	El Director de Respuesta a Incidentes comienza la clasificación con DPD e ITS y evalúa el Incidente de la Pérdida de Datos utilizando la matriz de riesgo descrita en el IRP.[320]
26 de agosto de 2021	El Director Sénior de TI de Seguridad Pública envía un correo electrónico a los Jefes del DPD con un desglose de los servidores en las instalaciones y las acciones tomadas por ITS en apoyo de esos servidores.[321]
26 de agosto de 2021	Lynn Richardson, Defensora Pública del Condado de Dallas, pide una auditoría independiente de 18 casos distintos de asesinato.
27 de agosto de 2021	Se envía una notificación formal de una posible pérdida de datos a la Oficina del Administrador de la Ciudad, la Oficina del Alcalde, el Concejo de la Ciudad y la Oficina del Abogado del Distrito.[322]
30 de agosto de 2021	Al técnico encargado de las copias de respaldo se le emite una notificación de audiencia previa al despido.[323]
31 de agosto de 2021	El CIO envía un correo electrónico que contiene respuestas a las preguntas planteadas por la Oficina del Abogado del Distrito con respecto al Incidente de la Pérdida de Datos.[324]
1 de septiembre de 2021	Se contrata al proveedor externo Birch Cline para desarrollar un protocolo de corrección para intentar localizar y recuperar datos perdidos.[325]
10 de septiembre de 2021	El Comité Ad Hoc sobre Investigación General y Ética consideró el asunto #2 de la agenda con respecto a la posibilidad de contratar a un consultor externo para completar una investigación independiente del Incidente de la Pérdida de Datos. Luego, el Comité instruye al Abogado de la Ciudad para que emita una solicitud de presentación de firmas de abogados que podrían realizar una investigación interna independiente. [326]
14 de octubre de 2021	De conformidad con el asunto de la agenda "A 21-1991", el Comité Ad Hoc de Investigación General y Ética entrevista a los tres principales bufetes de abogados propuestos para realizar una investigación independiente en nombre de la Ciudad. El Comité selecciona a Kirkland & Ellis LLP.[327]
22 de octubre de 2021	El técnico encargado de las copias de respaldo recibe una notificación de despido. [328]
27 de octubre de 2021	De conformidad con el asunto 47 de la agenda, el Concejo de la Ciudad autoriza la realización de un contrato de servicios profesionales con Kirkland & Ellis LLP para realizar una investigación del Incidente de la Pérdida de Datos.[329]
1 de noviembre de 2021	Kirkland & Ellis LLP realiza un contrato de servicios profesionales con la Ciudad de Dallas en virtud del cual se compromete a investigar la pérdida de datos, contratar a una firma forense para analizar los datos electrónicos perdidos y proporcionar un informe.[330]

B. Apéndice B: Eliminaciones Permanentes de Cliente en Commvault entre abril de 2021 y agosto de 2021

La siguiente tabla resume todos los comandos de eliminación de clientes que el técnico encargado de las copias de respaldo ejecutó en el software Commvault de la Ciudad entre abril de 2021 y agosto de 2021. Las eliminaciones que causaron el Incidente de la Pérdida de Datos están designadas con filas grises.

Fecha/Horario	Descripción
03/30/2021 21:34:55 UTC (16:34:55 CDT)	Eliminación permanente de cliente
03/30/2021 21:44:36 UTC (16:44:36 CDT)	Eliminación permanente de cliente
03/30/2021 21:47:47 UTC (16:47:47 CDT)	Eliminación permanente de cliente
03/30/2021 21:49:51 UTC (16:49:51 CDT)	Eliminación permanente de cliente
03/30/2021 21:50:28 UTC (16:50:28 CDT)	Eliminación permanente de cliente
03/31/2021 15:14:50 UTC (10:14:50 CDT)	Eliminación permanente de cliente
03/31/2021 15:28:49 UTC (10:28:49 CDT)	Eliminación permanente de cliente
03/31/2021 22:03:57 UTC (17:03:57 CDT)	Eliminación permanente de cliente
03/31/2021 22:14:10 UTC (17:14:10 CDT)	Eliminación permanente de cliente
03/31/2021 22:27:19 UTC (17:27:19 CDT)	Eliminación permanente de cliente
03/31/2021 22:29:05 UTC (17:29:05 CDT)	Eliminación permanente de cliente
03/31/2021 22:29:36 UTC (17:29:36 CDT)	Eliminación permanente de cliente
03/31/2021 22:30:08 UTC (17:30:08 CDT)	Eliminación permanente de

	cliente
03/31/2021 22:30:37 UTC (17:30:37 CDT)	Eliminación permanente de cliente
03/31/2021 22:31:06 UTC (17:31:06 CDT)	Eliminación permanente de cliente
03/31/2021 22:31:38 UTC (17:31:38 CDT)	Eliminación permanente de cliente
03/31/2021 22:37:15 UTC (17:37:15 CDT)	Eliminación permanente de cliente
05/07/2021 16:31:39 UTC (11:31:39 CDT)	Eliminación permanente de cliente
05/19/2021 16:42:50 UTC (11:42:50 CDT)	Eliminación permanente de cliente
06/07/2021 14:27:14 UTC (09:27:14 CDT)	Eliminación permanente de cliente

Fecha/Horario	**Descripción**
06/21/2021 15:44:42 UTC (10:44:42 CDT)	Eliminación permanente de cliente
06/21/2021 15:46:55 UTC (10:46:55 CDT)	Eliminación permanente de cliente
06/21/2021 15:47:16 UTC (10:47:16 CDT)	Eliminación permanente de cliente
06/21/2021 15:47:35 UTC (10:47:35 CDT)	Eliminación permanente de cliente
06/21/2021 15:47:57 UTC (10:47:57 CDT)	Eliminación permanente de cliente
06/21/2021 15:48:15 UTC (10:48:15 CDT)	Eliminación permanente de cliente
06/21/2021 15:48:15 UTC (10:48:34 CDT)	Eliminación permanente de cliente

06/21/2021 15:49:11 UTC (10:49:11 CDT)	Eliminación permanente de cliente
06/21/2021 15:49:36 UTC (10:49:36 CDT)	Eliminación permanente de cliente
06/23/2021 14:48:49 UTC (09:48:49 CDT)	Eliminación permanente de cliente
06/23/2021 15:16:26 UTC (10:16:26 CDT)	Eliminación permanente de cliente
06/23/2021 15:18:22 UTC (10:18:22 CDT)	Eliminación permanente de cliente
06/23/2021 15:18:39 UTC (10:18:39 CDT)	Eliminación permanente de cliente
06/23/2021 15:18:56 UTC (10:18:56 CDT)	Eliminación permanente de cliente
06/23/2021 15:19:15 UTC (10:19:15 CDT)	Eliminación permanente de cliente
06/23/2021 15:19:30 UTC (10:19:30 CDT)	Eliminación permanente de cliente
06/23/2021 15:19:48 UTC (10:19:48 CDT)	Eliminación permanente de cliente
06/23/2021 15:20:04 UTC (10:20:04 CDT)	Eliminación permanente de cliente
06/23/2021 16:28:13 UTC (11:28:13 CDT)	Eliminación permanente de cliente
06/23/2021 20:18:43 UTC (15:18:43 CDT)	Eliminación permanente de cliente
06/23/2021 20:21:02 UTC (15:21:02 CDT)	Eliminación permanente de cliente
06/23/2021 20:22:15 UTC (15:22:15 CDT)	Eliminación permanente de cliente
06/23/2021 20:22:23 UTC (15:22:33 CDT)	Eliminación

	permanente de cliente

Fecha/Horario	Descripción
06/23/2021 20:22:52 UTC (15:22:52 CDT)	Eliminación permanente de cliente
06/23/2021 20:25:35 UTC (15:25:35 CDT)	Eliminación permanente de cliente
06/23/2021 20:32:50 UTC (15:32:50 CDT)	Eliminación permanente de cliente
06/23/2021 21:41:46 UTC (16:41:36 CDT)	Eliminación permanente de cliente
06/23/2021 21:41:56 UTC (16:41:56 CDT)	Eliminación permanente de cliente
06/24/2021 14:04:42 UTC (09:04:42 CDT)	Eliminación permanente de cliente
06/24/2021 14:05:07 UTC (09:05:07 CDT)	Eliminación permanente de cliente
06/24/2021 14:29:49 UTC (09:29:49 CDT)	Eliminación permanente de cliente
06/24/2021 14:30:07 UTC (09:30:07 CDT)	Eliminación permanente de cliente
06/25/2021 17:17:35 UTC (12:17:35 CDT)	Eliminación permanente de cliente
07/26/2021 17:24:39 UTC (12:24:39 CDT)	Eliminación permanente de cliente
07/26/2021 17:25:13 UTC (12:25:13 CDT)	Eliminación permanente de cliente
07/26/2021 17:26:04 UTC (12:26:04 CDT)	Eliminación permanente de cliente
07/26/2021 17:26:36 UTC (12:26:36 CDT)	Eliminación permanente de cliente

07/26/2021 17:27:56 UTC (12:27:56 CDT)	Eliminación permanente de cliente
07/26/2021 17:28:55 UTC (12:28:55 CDT)	Eliminación permanente de cliente
07/26/2021 17:29:18 UTC (12:29:18 CDT)	Eliminación permanente de cliente
07/26/2021 17:29:40 UTC (12:29:40 CDT)	Eliminación permanente de cliente
07/26/2021 17:30:17 UTC (12:30:17 CDT)	Eliminación permanente de cliente
07/26/2021 17:30:52 UTC (12:30:52 CDT)	Eliminación permanente de cliente
07/26/2021 17:31:55 UTC (12:31:55 CDT)	Eliminación permanente de cliente
07/26/2021 17:32:21 UTC (12:32:21 CDT)	Eliminación permanente de cliente
07/29/2021 14:42:03 UTC (09:42:03 CDT)	Eliminación permanente de cliente

Fecha/Horario	**Descripción**
07/29/2021 16:42:34 UTC (11:42:34 CDT)	Eliminación permanente de cliente
08/05/2021 17:07:25 UTC (12:07:25 CDT)	Eliminación permanente de cliente
08/05/2021 17:07:47 UTC (12:07:47 CDT)	Eliminación permanente de cliente
08/05/2021 17:08:04 UTC (12:08:04 CDT)	Eliminación permanente de cliente
08/05/2021 17:08:33 UTC (12:08:33 CDT)	Eliminación permanente de cliente
08/05/2021 17:08:49 UTC (12:08:49 CDT)	Eliminación permanente de

	cliente
08/05/2021 17:09:05 UTC (12:09:05 CDT)	Eliminación permanente de cliente
08/05/2021 17:09:20 UTC (12:09:20 CDT)	Eliminación permanente de cliente
08/05/2021 17:09:36 UTC (12:09:36 CDT)	Eliminación permanente de cliente
08/05/2021 17:09:52 UTC (12:09:52 CDT)	Eliminación permanente de cliente
08/05/2021 17:10:13 UTC (12:10:13 CDT)	Eliminación permanente de cliente
08/05/2021 17:10:32 UTC (12:10:32 CDT)	Eliminación permanente de cliente

C. Apéndice C: Confirmación del Volumen de la Pérdida de Datos

1. Proceso General de Confirmación

Como parte de esta Investigación, utilizamos varios métodos para validar el volumen de la pérdida de datos informado por ITS.[331] Según las fuentes de datos disponibles, el volumen de la pérdida de datos sufrido por la Ciudad como resultado de las eliminaciones de marzo de 2021 es el siguiente:

- Aproximadamente 13 terabytes de datos FUSION.

- Inicialmente se perdieron 11 TB de datos de la Unidad de Almacenamiento K y se recuperaron 3.5 terabytes de datos de tres servidores que el técnico encargado de las copias de respaldo no había retirado. Un total de 7.51 terabytes de datos se consideraron irrecuperables.

En el transcurso de la auditoría de agosto, se creía que los servidores de CAPERS y del Secretario de la Ciudad también estaban posiblemente implicados, pero posteriormente se confirmó que se habían mantenido copias duplicadas de sus datos. Por lo tanto, la pérdida neta de datos fue la siguiente:

Ubicación	Volumen Perdido	Número de Archivos
Unidad de Almacenamiento K	7.51 TB	4.1 millones de archivos
Servidor FUSION	13.167 TB	4.6 millones de archivos
Servidor CAPERS	N/A	No se perdieron datos
Secretario de la Ciudad	N/A	No se perdieron datos

Según su auditoría de políticas y clientes eliminados realizada en agosto de 2021, Commvault concluyó que solo cuatro servidores se vieron afectados por la pérdida de datos:[332]

Servidor Afectado*	Categorización en Informe	Causa de la Pérdida de Datos
DPD FUSION	FUSION	Política de almacenamiento eliminada
Violencia Familiar	Unidad de Almacenamiento K	Política de almacenamiento eliminada
Servidor de Archivos DPD 1	Unidad de Almacenamiento K	Cliente eliminado
Servidor de Archivos DPD 2	Unidad de Almacenamiento K	Cliente eliminado

* Nombres de servidores anónimos.

2. Confirmación de la Pérdida de Datos de la Unidad de Almacenamiento K

Como se analizó anteriormente, la Unidad de Almacenamiento K es una red compartida mapeada donde los oficiales, detectives y otro personal del DPD de varias divisiones almacenan archivos de casos (es decir, evidencia) y datos administrativos. Antes del cambio a la nube de Azure, la Unidad de Almacenamiento K consistía en 6-8 servidores de archivos locales en el Concejo de la Ciudad y la sede del DPD.[333] A partir de entonces, en 2021 y debido a los sobrecostos causados por la cantidad de servidores, el uso activo de datos almacenados en almacenamiento inactivo y el aumento de los costos de salida, ITS decidió transferir los servidores de archivos nuevamente al Concejo de la Ciudad, como se detalló anteriormente.

Según las entrevistas, el volumen total de datos que inicialmente se creía que se habían perdido a partir de la eliminación del 31 de marzo de 2021 varió de 8 terabytes a 11 terabytes a 14 terabytes.[334] La cantidad de 22 terabytes se informó en agosto luego de una evaluación adicional.[335] El volumen neto de la pérdida de datos de Unidad de Almacenamiento K de aproximadamente 7.51 terabytes se validó al revisar el resultado del registro Azure de la Ciudad. El siguiente gráfico muestra la pérdida de datos inicial el 1 de abril de 10.77 terabytes (65.47 terabytes menos 54.7 terabytes) y la recuperación posterior de 3.26 terabytes (aumento de 54.7 terabytes el 1 de abril a 57.96 terabytes el 12 de abril), lo que da como resultado una pérdida de datos neta de 7.51 terabytes (65.47 terabytes menos 57.96 terabytes):

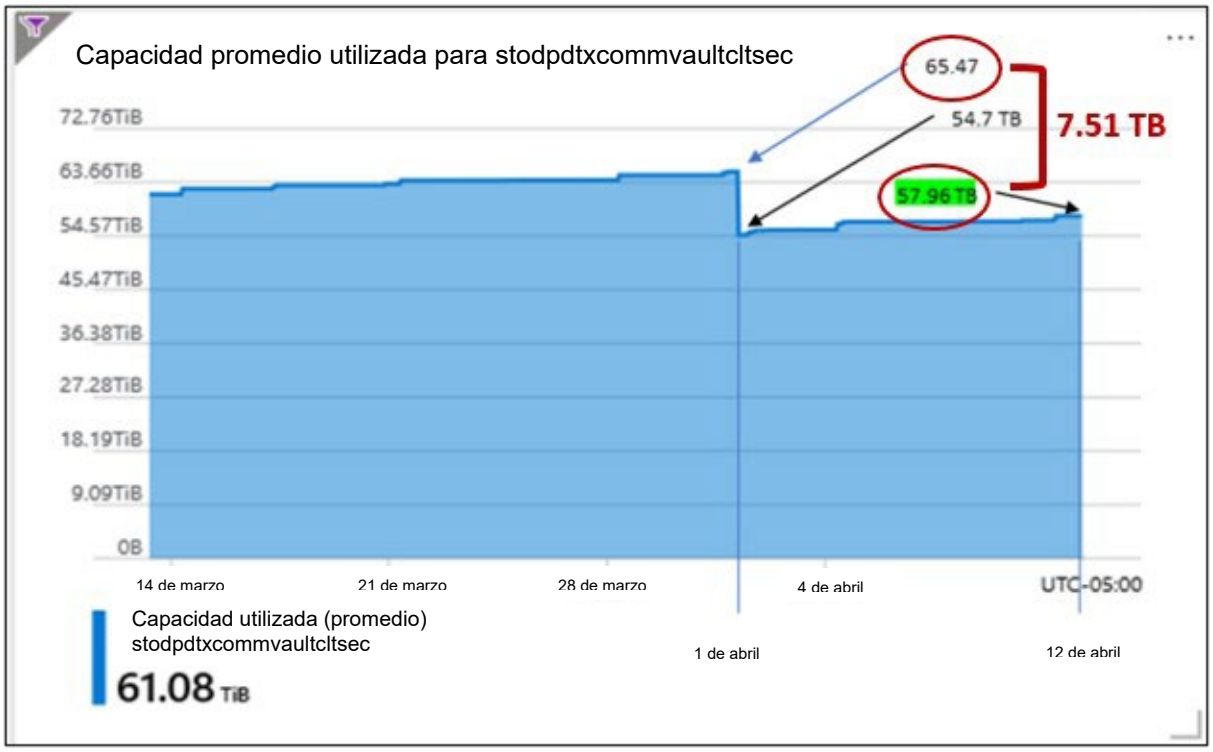

Fig. 5 – Captura de Pantalla del Registro de Microsoft Azure que Muestra el Volumen de Datos Perdidos

Hasta la fecha, todavía hay partes de los servidores de archivos de la Unidad de Almacenamiento K y DPD en Azure, específicamente: 15 unidades que almacenan alrededor de 10 terabytes cada una.[336] Tras la conclusión de la investigación, ITS planea completar una recuperación de datos masiva y trasladar estos sistemas restantes a la Alcaldía.[337]

3. Confirmación de la Pérdida de Datos de FUSION

El servidor FUSION es un servidor local de 14 terabytes que almacena principalmente imágenes de dispositivos móviles recopiladas por Center FUSION del DPD. [338] El servidor tenía aproximadamente 10 terabytes en uso (es decir, el área de almacenamiento donde ya residen los archivos) y 4 terabytes de espacio libre (es decir, el área de almacenamiento donde se pueden almacenar nuevos archivos).[339] Debido al tamaño de las imágenes de los teléfonos celulares y la rapidez con que llenaron el servidor FUSION, ITS habilitó el almacenamiento de Commvault en el servidor.[340]

Confirmamos que todo el servidor de 14 terabytes se vio afectado por el Incidente de la Pérdida de Datos, ya que los archivos nuevos no se habían almacenado en el servidor FUSION desde aproximadamente septiembre de 2020, lo que significa que la mayoría de los datos en FUSION ya se habían almacenamiento cuando la política de almacenamiento relevante de Commvault se eliminó en enero de 2021.[341] El servidor tiene una capacidad total de 14.6 terabytes y 14.5 terabytes de ese almacenamiento estaban en uso, como se muestra en la siguiente imagen.[342] Debido a que todos los datos tenían más de 18 meses, todos los datos se almacenaron. Por lo tanto, cuando se eliminó el archivo, se eliminaron todos los datos de FUSION.

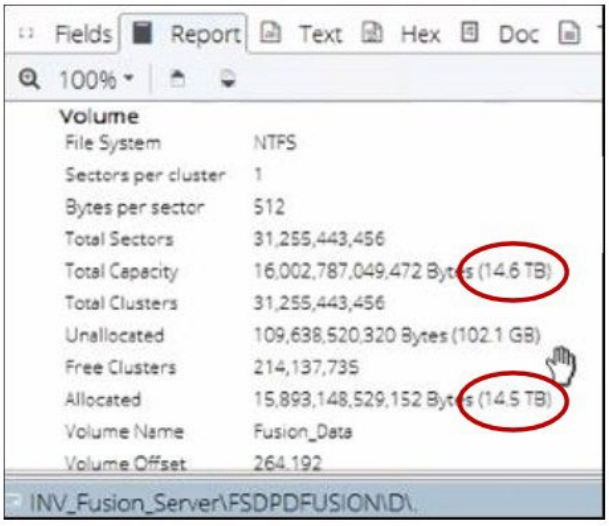

Fig. 6 –Captura de Pantalla que Muestra el Tamaño de la Imagen Forense del Servidor FUSION

4. Evaluación de la Secretaria de la Ciudad y CAPERS

La Ciudad, con la ayuda de Commvault, determinó que el técnico encargado de las copias de respaldo eliminó varias políticas para CAPERS y la oficina del Secretario de la Ciudad. Sin embargo, los archivos del Secretario de la Ciudad y CAPERS se almacenaron en otra parte de la red. Como resultado de esta redundancia, estos servidores no sufrieron ninguna pérdida final de datos.[343]

[1] *Por ejemplo,* entrevista de testigo el 5 de noviembre de 2021.

[2] Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 7 de diciembre de 2021; Entrevista de Testigo y Testigo el 25 de enero de 2022; Memorándum, John Creuzot, Abogado del Distrito Penal del Condado de Dallas, Divulgación sobre Datos Faltantes de la Unidad de Red del Departamento de Policía de Dallas (11 de agosto de 2021) [Memorándum de Creuzot], https://www.dallascounty.org/Assets/uploads/docs/district -abogado/pólizas/Memorándum% 20re% 20DPD% 20Data% 20Loss.pdf.

[3] Entrevista de testigo el 7 de diciembre de 2021; Entrevista de Testigo y Testigo el 25 de enero de 2022.

[4] Entrevista de testigo el 7 de diciembre de 2021; Entrevista de Testigo y Testigo el 25 de enero de 2022; Entrevista de testigo el 22 de noviembre de 2021.

[5] Entrevista de testigo el 7 de diciembre de 2021; Entrevista de Testigo y Testigo el 25 de enero de 2022.

[6] Entrevista de testigo el 7 de diciembre de 2021; Entrevista de Testigo y Testigo el 25 de enero de 2022.

[7] Entrevista de testigo el 7 de diciembre de 2021; Memorándum de Creuzot (11 de agosto de 2021).

[8] Memorándum de Creuzot (11 de agosto de 2021).

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] Carta de Eric Johnson, Alcalde de Dallas, a Adam McGough y Cara Mendelsohn, Concejales de la Ciudad de Dallas (12 de agosto de 2021).

[16] Acta de la Reunión del Consejo de la Ciudad de Dallas (18 de agosto de 2021).

[17] Acta de la Reunión del Comité Ad Hoc de Investigación General y Ética (10 de septiembre de 2021).

[18] Acta de la Reunión del Comité Ad Hoc de Investigación General y Ética (14 de octubre de 2021).

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] Acta de la Reunión del Comité Ad Hoc de Investigación General y Ética (4 de noviembre de 2021).

[23] *Id.*

[24] Solicitud de presentaciones, Ciudad de Dallas (17 de septiembre de 2021).

[25] *Servicios de Información y Tecnología: Sobre de Nosotros,* Ciudad de Dallas, https://dallascityhall.com/departments/ciservices/ Pages/About-Us.aspx.

[26] *Ver en general* Entrevista de testigo el 9 de diciembre de 2021; Entrevista de testigo el 5 de noviembre de 2021.

[27] Entrevista de testigo el 5 de noviembre de 2021.

[28] Entrevista de testigo el 7 de diciembre de 2021.

[29] Entrevista de testigo el 22 de noviembre de 2021.

[30] Entrevista de testigo el 5 de noviembre de 2021.

[31] *Servicios de información y tecnología: Sobre de Nosotros,* Ciudad de Dallas, https://dallascityhall.com/departments/ciservices/Pages/About-Us.aspx.

[32] Entrevista de testigo el 5 de noviembre de 2021.

[33] *Nuestra Misión,* Abogado del Distrito Penal del Condado de Dallas, https://www.dallascounty.org/government/district-abogado/mission.php.

[34] *Datos Breves:* Condado de Dallas, Texas, EE. UU. Oficina del Censo, https://www.census.gov/quickfacts/fact/table/dallascountytexas/POP010220.

[35] *Poblaciones de los Condados de EE. UU. 2021,* Revisión de la población mundial, https://worldpopulationreview.com/us-counties.

[36] Entrevista de testigo el 7 de diciembre de 2021.

[37] *Historia,* Departamento de Policía de Dallas, https://dallaspolice.net/abouts/dpdhistory.

[38] Entrevista de testigo el 2 de diciembre de 2021.

[39] Entrevista de testigo el 2 de diciembre de 2021.

[40] *Id.*

[41] *Ver* Entrevista de testigo el 2 de diciembre de 2021.

[42] Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 21 de diciembre de 2021; Entrevista de testigo el 21 de diciembre de 2021.

[43] Entrevista de testigo el 21 de diciembre de 2021; Entrevista de testigo el 21 de diciembre de 2021.

[44] Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 21 de diciembre de 2021.

[45] Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 2 de diciembre de 2021.

[46] *Por Ejemplo,* entrevista de testigo el 2 de diciembre de 2021.

[47] Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 21 de diciembre de 2021.

[48] Entrevista de testigo el 2 de diciembre de 2021.

[49] *Ver* Entrevista de testigo el 2 de diciembre de 2021.

[50] *Ver id.*

[51] *Id.*

[52] *Id.*; Entrevista de testigo el 21 de diciembre de 2021.

[53] Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 21 de diciembre de 2021.

[54] Entrevista de testigo el 7 de diciembre de 2021; Entrevista de testigo el 7 de diciembre de 2021.

[55] Entrevista de testigo el 9 de noviembre de 2021.

[56] Entrevista de testigo el 9 de noviembre de 2021.

[57] Entrevista de testigo el 9 de noviembre de 2021.

[58] *Ver* Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 21 de diciembre de 2021; Entrevista de testigo el 21 de diciembre de 2021; Entrevista de testigo el 2 de diciembre de 2021.

[59] Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 21 de diciembre de 2021; Entrevista de testigo el 21 de diciembre de 2021.

[60] *Ver, por ejemplo,* 6 Normas: Para el Almacenamiento de Datos, Iron Mountain, https://www.ironmountain.com/resources/whitepapers/d/6-dos-and-donts-for-data-archiving.

[61] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de Testigo el 5 de enero de 2022; Entrevista de testigo el 3 de diciembre de 2021.

[62] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 3 de diciembre de 2021.

[63] Entrevista de testigo el 5 de noviembre de 2021.

[64] Entrevista de testigo el 2 de diciembre de 2021.

[65] Entrevista de testigo el 9 de noviembre de 2021.

[66] *Ver* Creación de un Plan de Archivo, Commvault (21 de octubre de 2021), https://documentation.commvault.com/11.26/essential/127324_creating_archive_plan.html.

[67] Entrevista de testigo el 5 de enero de 2021; *ver Glosario*: Política de Subclientes, Commvault, https://documentación.commvault.com/11.24/essential/50021_glossary.html.

[68] *Glosario: Política de Almacenamiento,* Commvault, https://documentation.commvault.com/11.24/essential/50021_glossary.html.

[69] Entrevista de testigo el 20 de diciembre de 2021.

[70] *Glosario: Stubs,* Commvault, https://documentation.commvault.com/11.24/essential/50021_glossary.html.

[71] Entrevista de testigo el 5 de enero de 2021; Entrevista de testigo el 20 de diciembre de 2021.

[72] Entrevista de Testigo el 5 de enero de 2022; Entrevista de testigo el 5 de enero de 2021; Entrevista de testigo el 15 de diciembre de 2021; Entrevista de testigo el 22 de noviembre de 2021.

[73] Entrevista de Testigo el 5 de enero de 2022; Entrevista de testigo el 8 de noviembre de 2021; Entrevista de testigo el 15 de diciembre de 2021; Entrevista de testigo el 22 de noviembre de 2021.

[74] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de Testigo el 5 de enero de 2022; Entrevista de testigo el 3 de diciembre de 2021.

[75] Cadena de correo electrónico ITS con fecha del 23 de julio de 2020 al 28 de julio de 2020.

[76] *Detalle de Orden de Cambio:* 116670, ITS (disponible el 24 de agosto de 2020).

[77] Entrevista de testigo el 5 de noviembre de 2021.

[78] *Ver* Entrevista de testigo el 15 de diciembre de 2021.

[79] Entrevista de testigo el 5 de noviembre de 2021.

[80] *Id.*

[81] *Informe de seguimiento de auditoría: eliminación permanente de cliente, C*ommvault (generado el 26 de agosto de 2021*); Informe de Seguimiento de Auditoría: Eliminar Política de Almacenamiento, Commvault (*generado el 26 de agosto de 2021).

[82] Memorándum de Creuzot (11 de agosto de 2021); Cadena de Correo Electrónico ITS y DPD fecha 9 de agosto de 2021.

[83] Informe inicial de la pérdida de datos de ITS, en 10.

[84] *Detalles del incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021).

[85] Entrevista de testigo el 5 de noviembre de 2021.

[86] *Detalles del incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021).

[87] Entrevista de testigo el 22 de noviembre de 2021.

[88] Informe inicial de pérdida de datos de ITS, en 11.

[89] *Detalles del incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021).

[90] Entrevista de testigo el 2 de diciembre de 2021.

[91] *Id.*

[92] Correo electrónico de la cadena de correo electrónico de ITS con fecha del 13 de abril de 2021.

[93] *Actualización del Jefe: Documento 21-2015,* Departamento de Policía de Dallas (19 de abril de 2021).

[94] *Informe de Seguimiento de Auditoría: Eliminación permanente de Cliente,* Commvault (generado el 26 de agosto de 2021).

[95] Entrevista de testigo el 7 de diciembre de 2021; Entrevista de Testigo y Testigo el 25 de enero de 2022.

[96] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 5 de noviembre de 2021.

[97] Memorándum de Creuzot (11 de agosto de 2021).

[98] *Id.*

[99] Carta del representante legal a ITS de fecha 1 de noviembre de 2021.

[100] Entrevista de testigo el 22 de diciembre de 2021; Entrevista de testigo el 20 de diciembre de 2021.

[101] Informe inicial de la pérdida de datos de ITS, en 11; Entrevista de testigo el 9 de diciembre de 2021.

[102] Informe inicial de la pérdida de datos de ITS, en 11; Entrevista de testigo el 9 de diciembre de 2021.

[103] *Notificación de audiencia previa al despido al técnico encargado de las copias de respaldo,* Ciudad de Dallas (30 de agosto de 2021).

[104] *Notificación de despido al técnico encargado de las copias de respaldo,* Ciudad de Dallas (22 de octubre de 2021).

[105] Entrevista de testigo el 5 de noviembre de 2021.

[106] Entrevista de testigo el 15 de diciembre de 2021.

[107] *Ver* Entrevista de testigo el 5 de enero de 2022.

[108] Entrevista de testigo el 5 de enero de 2021.

[109] Entrevista de testigo el 5 de noviembre de 2021.

[110] *Id.*

[111] *Detalle de Orden de Cambio: 116670, ITS* (disponible el 24 de agosto de 2020).

[112] *Id.*

[113] Entrevista de testigo el 5 de noviembre de 2021.

[114] *Id.*

[115] *Detalle de Orden de Cambio: 116670, ITS* (inaugurado el 24 de agosto de 2020).

[116] Entrevista de testigo el 15 de diciembre de 2021.

[117] *Ver* Plan de implementación para las nuevas bibliotecas de almacenamiento blob de Commvault (adjunto a la Orden de Cambio del 24 de agosto de 2020).

[118] *Ver id.*

[119] *Detalles del incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021); Entrevista de testigo el 15 de diciembre de 2021.

[120] Entrevista de testigo el 5 de noviembre de 2021.

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] Entrevista de testigo el 9 de diciembre de 2021.

[125] Entrevista de testigo el 15 de diciembre de 2021.

[126] *Id.*

[127] Entrevista de testigo el 5 de enero de 2021; Entrevista de testigo el 20 de diciembre de 2021.

[128] Entrevista de Testigo el 5 de enero de 2022; Entrevista de testigo el 20 de diciembre de 2021.

[129] Entrevista de Testigo el 5 de enero de 2022.

[130] Entrevista de testigo el 15 de diciembre de 2021.

[131] Entrevista de Testigo el 5 de enero de 2022.

[132] Entrevista de testigo el 5 de noviembre de 2021.

[133] Entrevista de testigo el 15 de diciembre de 2021; Cadena de correo electrónico de ITS y DPD con fecha del 9 de agosto de 2021.

[134] *Informe de seguimiento de auditoría: eliminación permanente de cliente,* Commvault (generado el 26 de agosto de 2021); *Informe de seguimiento de auditoría: Eliminar política de almacenamiento,* Commvault (generado el 26 de agosto de 2021).

[135] *Informe de seguimiento de auditoría: eliminación permanente de cliente,* Commvault (generado el 26 de agosto de 2021); *Informe de seguimiento de auditoría: Eliminar política de almacenamiento,* Commvault (generado el 26 de agosto de 2021).

[136] Entrevista de testigo el 20 de diciembre de 2021.

[137] Directriz de Commvault de 24 de enero de 2022.

[138] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 20 de diciembre de 2021.

[139] *Recuperación de datos relacionados con clientes y políticas de almacenamiento eliminados,* Commvault (28 de octubre de 2021), https://documentation.commvault.com/11.21/essential/43719_recovering_data_associated_with_deleted_clients_and_storage_policies.html.

[140] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 22 de noviembre de 2021.

[141] Entrevista de testigo el 15 de diciembre de 2021.

[142] *Id.*

[143] *Id.*

[144] Memorándum de Creuzot (11 de agosto de 2021); cadena de correo electrónico ITS y DPD con fecha del 9 de agosto de 2021; Entrevista de testigo el 5 de noviembre de 2021.

[145] Informe inicial de la pérdida de datos de ITS, en 10.

[146] *Detalles del incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021).

[147] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 15 de diciembre de 2021.

[148] Entrevista de testigo el 5 de noviembre de 2021.

[149] *Ver* Entrevista de testigo el 15 de diciembre de 2021.

[150] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 15 de diciembre de 2021.

[151] Entrevista de testigo el 5 de noviembre de 2021.

[152] Entrevista de testigo el 22 de noviembre de 2021.

[153] Entrevista de testigo el 5 de noviembre de 2021.

[154] *Id.*

[155] Entrevista de testigo el 9 de diciembre de 2021.

[156] *Id.*

[157] Entrevista de testigo el 2 de diciembre de 2021.

[158] Entrevista de testigo el 5 de noviembre de 2021.

[159] *Id.*; Entrevista de testigo el 2 de diciembre de 2021.

[160] Entrevista de testigo el 5 de noviembre de 2021.

[161] *Ver* cadena de correo electrónico ITS con fecha del 13 de abril de 2021.

[162] Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 5 de noviembre de 2021.

[163] Entrevista de testigo el 2 de diciembre de 2021.

[164] *Ver* Memorándum de seguridad pública sobre archivos y carpetas faltantes, Ciudad de Dallas.

[165] Entrevista de testigo el 2 de diciembre de 2021.

[166] *Ver Actualización del Jefe: Documento 21-2015,* Departamento de Policía de Dallas (19 de abril de 2021).

[167] *Ver* Memorándum de seguridad pública sobre archivos y carpetas faltantes, Ciudad de Dallas.

[168] Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 9 de noviembre de 2021.

[169] *Detalles del Incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021).

[170] *Id.*

[171] *Id.*

[172] *Id.*

[173] *Id.*

[174] *Id.*

[175] *Informe de seguimiento de auditoría: eliminación permanente de cliente, Commvault (generado el 26 de agosto de 2021).*

[176] Entrevista de testigo el 7 de diciembre de 2021.

[177] Memorándum de Creuzot (11 de agosto de 2021).

[178] Entrevista de testigo el 5 de noviembre de 2021.

[179] Memorándum de Creuzot (11 de agosto de 2021).

[180] *Id.*

[181] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 2 de diciembre de 2021.

[182] Entrevista de testigo el 5 de noviembre de 2021.

[183] Entrevista de testigo el 20 de diciembre de 2021.

[184] *Id.*

[185] Entrevista de testigo el 9 de diciembre de 2021.

[186] Entrevista de testigo el 3 de diciembre de 2021.

[187] *Id.*

[188] Entrevista de Testigo el 5 de enero de 2022.

[189] Entrevista de testigo el 8 de noviembre de 2021.

[190] Entrevista de testigo el 9 de diciembre de 2021; Entrevista de testigo el 3 de diciembre de 2021; Entrevista de testigo del 9 de febrero de 2022.

[191] *Ver* Entrevista de testigo el 9 de diciembre de 2021; Entrevista de testigo el 8 de noviembre de 2021.

[192] Entrevista de testigo el 9 de diciembre de 2021.

[193] Entrevista de Testigo el 5 de enero de 2022.

[194] Entrevista de Testigo el 9 de noviembre de 2021.

[195] Entrevista de testigo el 9 de diciembre de 2021.

[196] Entrevista de testigo el 3 de diciembre de 2021.

[197] Entrevista de testigo el 9 de diciembre de 2021; Entrevista de testigo el 22 de diciembre de 2021.

[198] Entrevista de Testigo el 5 de enero de 2022; Entrevista de testigo el 9 de diciembre de 2021; Entrevista de testigo el 22 de diciembre de 2021; Entrevista de testigo el 7 de diciembre de 2021.

[199] Entrevista de testigo el 22 de diciembre de 2021; Entrevista de testigo el 3 de diciembre de 2021.

[200] Entrevista de testigo el 22 de diciembre de 2021; Entrevista de testigo el 3 de diciembre de 2021.

[201] Entrevista de testigo el 3 de diciembre de 2021.

[202] Entrevista de testigo el 22 de diciembre de 2021.

[203] Entrevista de testigo el 9 de diciembre de 2021.021.

[204] Números proporcionados por Testigo y vigentes al 9 de febrero de 2022.

[205] Números proporcionados por Testigo y vigentes al 9 de febrero de 2022.

[206] Entrevista de testigo el 15 de diciembre de 2021.

[207] *Id.*

[208] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de Testigo el 5 de enero de 2022.

[209] *Commvault Professional Foundations Dirigido por un Instructor,* Commvault, https://ea.commvault.com/CourseGroup/ Index/68/39; Commvault Professional Advanced Instructor-led, Commvault, https://ea.commvault.com/ CourseGroup/Index/70/39; Entrevista de testigo el 20 de diciembre de 2021.

[210] Entrevista de Testigo el 5 de enero de 2022; Entrevista de testigo el 22 de noviembre de 2021.

[211] Entrevista de Testigo el 5 de enero de 2022; Entrevista de testigo el 22 de noviembre de 2021.

[212] Entrevista de testigo el 15 de diciembre de 2021.

[213] Entrevista de testigo el 3 de diciembre de 2021.

[214] Informe inicial de la pérdida de datos de ITS, en 60.

[215] Entrevista de Testigo el 3 de diciembre de 2021.

[216] *Ver* Entrevista de testigo el 5 de enero de 2022; Entrevista de Testigo el 5 de enero de 2022; Entrevista de testigo el 22 de noviembre de 2021.

[217] Entrevista de testigo el 21 de diciembre de 2021; Entrevista de testigo el 8 de diciembre de 2021; Entrevista de testigo el 2 de diciembre de 2021.

[218] Entrevista de testigo el 2 de diciembre de 2021.

[219] *Detalles del incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021).

[220] Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 2 de diciembre de 2021.

[221] Entrevista de Testigo el 5 de enero de 2022.

[222] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de Testigo el 5 de enero de 2022.

[223] Entrevista de testigo el 9 de diciembre de 2021.

[224] Entrevista de testigo el 5 de noviembre de 2021.

[225] *Ciudad de Dallas - Evaluación de desarrollo de TI,* Forrester (14 de diciembre de 2020).

[226] Entrevista de testigo el 2 de diciembre de 2021.

[227] Entrevista de testigo el 2 de diciembre de 2021.

[228] *Id.*

[229] *Id.*

[230] Entrevista de testigo el 21 de diciembre de 2021.

[231] *Id.*

[232] Entrevista de testigo el 2 de diciembre de 2021.

[233] *Id.*; Entrevista de testigo el 21 de diciembre de 2021.

[234] Entrevista de testigo el 2 de diciembre de 2021.

[235] Entrevista de testigo el 21 de diciembre de 2021.

[236] *Id.*

[237] Entrevista de Testigo el 2 de diciembre de 2021.

[238] Entrevista de Testigo y Testigo el 25 de enero de 2022. Ver también Entrevista de Testigo el 2 de diciembre de 2021.

[239] Entrevista de testigo el 7 de diciembre de 2021.

[240] Entrevista de Testigo y Testigo el 25 de enero de 2022.

[241] Entrevista de Testigo el 25 de enero de 2022; Entrevista de testigo el 7 de diciembre de 2021. Ver Tex. Código Penal. Proc. Art. 39.14.

[242] Entrevista de testigo el 7 de diciembre de 2021; Entrevista de Testigo el 25 de enero de 2022.

[243] Entrevista de testigo el 7 de diciembre de 2021.

[244] *Nuestra Misión,* Abogado del Distrito Penal del Condado de Dallas, https://www.dallascounty.org/government/district-abogado/mission.php.

[245] Gráfico del registro de Azure que muestra el cambio en el volumen de 65.47 TB a 54.7 TB (10.77 TB menos) a partir del 1 de abril.

[246] Gráfico de registro de Azure que muestra el cambio en el volumen de 54.7 TB a 57.96 TB (3.26 TB recuperados entre el 1 y el 12 de abril).

[247] Gráfico de panel de Azure que muestra el cambio de 65,47 TB (el 1 de abril) a 57.96 TB (el 12 de abril).

[248] Actualización de la evaluación de la pérdida de datos – 8/27/2021.

[249] Entrevista de testigo el 9 de noviembre de 2021; Entrevista de Testigo el 5 de enero de 2022; Análisis EnCase de Stroz Friedberg.

[250] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de Testigo el 5 de enero de 2022; Entrevista de testigo el 22 de noviembre de 2021; Entrevista de testigo el 15 de diciembre de 2021.

[251] Entrevista de Testigo el 5 de enero de 2022.

[252] Entrevista de testigo el 5 de noviembre de 2021.

[253] Entrevista de testigo el 7 de diciembre de 2021.

[254] Entrevista de testigo el 9 de diciembre de 2021.

[255] Entrevista de testigo el 7 de diciembre de 2021; Entrevista de testigo el 9 de noviembre de 2021.

[256] *Ver* Entrevista de testigo el 9 de noviembre de 2021; Entrevista de testigo el 7 de diciembre de 2021; Entrevista de testigo el 9 de noviembre de 2021.

[257] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de Testigo el 5 de enero de 2022; Entrevista de testigo el 3 de diciembre de 2021.

[258] Cadena de correo electrónico ITS con fecha del 24 de enero de 2022.

[259] Entrevista de testigo el 5 de noviembre de 2021.

[260] Correos electrónicos entre la cadena de correo electrónico ITS con fecha del 23 de julio de 2020 al 28 de julio de 2020.

[261] Cadena de correo electrónico ITS con fecha del 20 de agosto de 2020 al 24 de agosto de 2020.

[262] *Detalle de Orden de Cambio:* 116670, ITS (inaugurado el 24 de agosto de 2020).

[263] Ciudad de Dallas - Evaluación de desarrollo de TI, Forrester (14 de diciembre de 2020).

[264] Cadena de correo electrónico ITS con fecha del 24 de enero de 2022.

[265] Ciudad de Dallas - Evaluación de desarrollo de TI, Forrester (14 de diciembre de 2020).

[266] Cadena de correo electrónico ITS con fecha del 11 de enero de 2021.

[267] Entrevista de testigo el 5 de noviembre de 2021.

[268] Entrevista de testigo el 5 de noviembre de 2021.

[269] Entrevista de testigo el 5 de noviembre de 2021.

[270] Cadena de correo electrónico ITS con fecha del 4 de marzo de 2021.

[271] *Informe de seguimiento de auditoría: eliminación permanente de cliente,* Commvault (generado el 26 de agosto de 2021); *Informe de seguimiento de auditoría: Eliminar política de almacenamiento,* Commvault (generado el 26 de agosto de 2021).

[272] Memorándum de Creuzot (11 de agosto de 2021); Cadena de correo electrónico de ITS y DPD con fecha del 9 de agosto de 2021.

[273] Informe inicial de la pérdida de datos de ITS, en 10; Entrevista de testigo el 9 de diciembre de 2021.

[274] *Detalles del incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021).

[275] Entrevista de testigo el 5 de noviembre de 2021.

[276] *Detalles del incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021).

[277] Informe inicial de la pérdida de datos de ITS, en 10.

[278] *Detalles del incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021).

[279] Informe de análisis de la pérdida de datos de ITS, en 11; Entrevista de testigo el 9 de diciembre de 2021.

[280] Informe de análisis de la pérdida de datos de ITS, en 11; Entrevista de testigo el 9 de diciembre de 2021.

[281] Informe de análisis de la pérdida de datos de ITS, en 11; Entrevista de testigo el 9 de diciembre de 2021.

[282] Informe de análisis de la pérdida de datos de ITS, en 11; Entrevista de testigo el 9 de diciembre de 2021.

[283] Entrevista de testigo el 2 de diciembre de 2021.

[284] *Id.*

[285] Cadena de correo electrónico ITS con fecha del 13 de abril de 2021.

[286] *Id.*

[287] *Detalles del incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021).

[288] *Actualización del Jefe: Documento 21-2015,* Departamento de Policía de Dallas (19 de abril de 2021).

[289] *Detalles del incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021).

[290] Cadena de correos electrónicos de ITS y DPD con fecha del 22 de abril de 2021.

[291] *Detalles del incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021).

[292] *Id.*

[293] *Informe de seguimiento de auditoría: eliminación permanente de cliente,* Commvault (generado el 26 de agosto de 2021).

[294] *Detalles del incidente: TR_210405_307,* Soporte de Commvault (creado el 5 de abril de 2021).

[295] *Id.*

[296] *Informe de seguimiento de auditoría:* eliminación permanente de cliente, Commvault (generado el 26 de agosto de 2021).

[297] *Id.*

[298] *Id.*

[299] *Id.*

[300] *Id.*

[301] *Id.*

[302] *Id.*

[303] *Id.*

[304] *Id.*

[305] Entrevista de testigo el 7 de diciembre de 2021; Entrevista de Testigo y Testigo el 25 de enero de 2022.

[306] Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 5 de noviembre de 2021.

[307] Cadena de correo electrónico de ITS y DPD con fecha del 9 de agosto de 2021.

[308] Cadena de correo electrónico de ITS y DPD con fecha del 4 de agosto de 2021.

[309] *Informe de seguimiento de auditoría: eliminación permanente de cliente,* Commvault (generado el 26 de agosto de 2021).

[310] Memorándum de Creuzot (11 de agosto de 2021).

[311] *Id.*; Cadena de correo electrónico ITS y DPD 9 de agosto de 2021.

[312] Memorándum de Creuzot (11 de agosto de 2021).

[313] Carta de Johnson (12 de agosto de 2021).

[314] Carta del representante legal a ITS de fecha 1 de noviembre de 2021.

[315] "Sospechoso de asesinato en Texas recibió fianza después de la pérdida de datos policiales, ABC News (13 de agosto de 2021), https://abcnews.go.com/US/wireStory/texas-murder-suspect-granted-bond-police-data-loss -79449121;

"Le otorgan a sospechoso de asesinato en Texas fianza luego de la pérdida de datos policiales," Fox News (14 de agosto de 2021),https://www.foxnews.com/us/texas-murder-suspect-bond-data-loss; Krista Torravla, " Sospechoso de asesinato en Dallas será liberado de la cárcel mientras la Ciudad determina si perdió pruebas," Dallas Morning News (13 de agosto de 2021),https://www.dallasnews.com/news/courts/2021/08/13/dallas-murder-suspect-to-be-released-from-jail-while- city-determines-if-it-lost-evidence/; Isabel Vincent, "Sospechoso de asesinato en Texas queda en libertad bajo palabra tras la pérdida de datos de la policía," New York Post (14 de agosto de 2021), https://nypost.com/2021/08/14/texas-murder-suspect-released-on-bond-after-police-data-loss/.

316 MinutActaas de la Reunión del Consejo de la Ciudad de Dallas (18 de agosto de 2021).

317 Entrevista de testigo el 22 de diciembre de 2021; Entrevista de testigo el 20 de diciembre de 2021.

318 Entrevista de testigo el 9 de noviembre de 2021.

319 Informe de análisis de la pérdida de datos de ITS, en 11; Entrevista de testigo el 9 de diciembre de 2021.

320 Entrevista de testigo el 3 de diciembre de 2021.

321 Cadena de correo electrónico de ITS y DPD con fecha del 26 de agosto de 2021.

322 Informe de análisis de la pérdida de datos de ITS, en 11.

323 *Notificación de audiencia previa al despido del técnico encargado de las copias de respaldo,* Ciudad de Dallas (30 de agosto de 2021).

324 Cadena de correos electrónicos de ITS, DPD y Oficina del Abogado del Distrito con fecha del 31 de agosto de 2021.

325 Entrevista de testigo el 22 de diciembre de 2021.

326 Acta de la Reunión del Comité Ad Hoc de Investigación General y Ética (10 de septiembre de 2021).

327 Acta de la Reunión del Comité Ad Hoc de Investigación General y Ética (14 de octubre de 2021).

328 *Notificación de Despido al técnico encargado de las copias de respaldo, Ciudad de Dallas (22 de octubre de 2021).*

329 Acta de la Reunión del Consejo de la Ciudad de Dallas (27 de octubre de 2021).

330 Contrato de Servicios Legales Profesionales entre la Ciudad de Dallas y Kirkland & Ellis, LLP (1 de noviembre de 2021); Solicitud de presentaciones, Ciudad de Dallas (17 de septiembre de 2021).

331 Informe de análisis de la pérdida de datos de ITS, en iii-iv.

332 Entrevista de testigo el 22 de diciembre de 2021.

333 Entrevista de testigo el 2 de diciembre de 2021.

334 Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 9 de noviembre de 2021; Entrevista de testigo el 22 de noviembre de 2021; Entrevista de testigo el 7 de diciembre de 2021; Entrevista de testigo el 7 de diciembre de 2021.

335 Entrevista de testigo el 9 de noviembre de 2021.

336 Entrevista de testigo el 5 de noviembre de 2021.

337 *Id.*

338 *Ver* Entrevista de testigo el 2 de diciembre de 2021; Entrevista de testigo el 8 de noviembre de 2021; Entrevista de testigo el 5 de noviembre de 2021.

339 Entrevista de testigo el 8 de noviembre de 2021.

340 Entrevista de testigo el 2 de diciembre de 2021.

341 Entrevista de testigo el 9 de noviembre de 2021.

342 *Ver* captura de pantalla del tutorial virtual de EnCase (9 de enero de 2022).

343 Entrevista de testigo el 5 de noviembre de 2021; Entrevista de testigo el 5 de noviembre de 2021.