Acronis

INFORME

Seis amenazas para los datos de G Suite que pueden salir muy caras y cómo corregirlas

UN INCIDENTE DE PÉRDIDA DE DATOS EN CUALQUIER MOMENTO

Si su empresa depende de G Suite, disfrutará de acceso fiable a sus aplicaciones con un tiempo de actividad muy elevado. Sin embargo, muchos profesionales de TI trabajan con una idea equivocada, ya que creen que Google proporciona protección total de los datos, así como conservación de los datos a largo plazo para G Suite.

La realidad es que los mensajes de correo electrónico, los eventos de calendario, los contactos y los archivos almacenados en G Suite no están protegidos frente a los riesgos de pérdida de datos más importantes y habituales, que van desde la simple eliminación accidental hasta los sofisticados ataques de malware.

Por este motivo, para muchas empresas, G Suite deja una importante brecha en la seguridad de los datos, abriendo la puerta a una sorpresa desagradable que puede ocurrir en cualquier momento. Es posible que sea demasiado tarde cuando averigüen que Google solo ofrece funciones limitadas para restaurar los datos de G Suite perdidos, destruidos o dañados, que no se parecen ni de lejos a las funcionalidades o la solidez de la copia de seguridad con la que la mayoría de las empresas protegen las demás aplicaciones críticas.

> Este documento describe varias limitaciones de las funciones de protección de datos de Google, que pueden pasar desapercibidas, y examina cómo suplir estas carencias para garantizar una rápida recuperación si se produce alguno de los numerosos problemas de pérdida de datos a los que G Suite es vulnerable.

6 PRINCIPALES AMENAZAS PARA LA SEGURIDAD DE LOS DATOS A LAS QUE SU EMPRESA PUEDE ENFRENTARSE AL UTILIZAR G SUITE

Google ha invertido mucho en hardware, software, redes, seguridad y operaciones de sus centros de datos para garantizar un alto rendimiento, un fácil acceso y un tiempo de actividad óptimo para G Suite. Sus objetivos principales son la resiliencia de la infraestructura básica, la capacidad de recuperarse cuando se producen grandes desastres naturales (por ejemplo, inundaciones, terremotos o huracanes) y la recuperación de datos de G Suite perdidos o dañados en algunos casos limitados y a corto plazo.

Por eso puede detectar y recuperarse rápidamente cuando se producen muchos de sus propios errores de funcionamiento del centro de datos en la nube, interrupciones de servicio, fallos de hardware y problemas de la red, lo que le permite cumplir sus acuerdos de nivel de servicio, que se centran en el tiempo de actividad de la aplicación. Pero estas medidas no protegen a su empresa frente a muchos de los problemas habituales de pérdida de datos de G Suite, incluida la eliminación accidental o maliciosa de datos por parte de los empleados, y las amenazas externas para la integridad de los datos, como el ransomware y otros ataques de malware. Además, es muy fácil y bastante habitual que los administradores de TI establezcan períodos de retención de los mensajes de correo electrónico de Gmail extremadamente agresivos, es decir, demasiado cortos, lo que lleva a la rápida eliminación de mensajes que se podrían necesitar más adelante, cuando Google ya no puede restaurarlos.

> Google es capaz de restaurar la mayoría de los recursos de datos de G Suite durante un breve período de tiempo después de que hayan sido eliminados por un usuario o un administrador (de forma predeterminada, 25 días para los mensajes de Gmail y archivos de Drive, 20 días para los perfiles de usuarios). Es posible que necesite un proyecto que lleva inactivo mucho tiempo o mensajes o archivos de un empleado que ha dejado la empresa, sin embargo, tras una larga búsqueda, puede que descubra que Google no ha conservado una copia que pueda recuperar.

LOS ADMINISTRADORES DE G SUITE DEBEN AFRONTAR LAS AMENAZAS CONTRA LOS DATOS EN SEIS ÁREAS

1. Problemas de eliminación accidental

RIESGO PARA LOS DATOS: a lo largo de una jornada de trabajo, los administradores y los empleados eliminan de forma rutinaria perfiles de usuario de G Suite, mensajes y adjuntos de Gmail, eventos de Calendar, contactos y archivos de Google Drive. Ya sean accidentales o intencionadas, es posible que el usuario se arrepienta más tarde de estas eliminaciones; la mayoría de nosotros hemos necesitado alguna vez consultar un mensaje que habíamos eliminado solo un día antes.

PUNTO DÉBIL DE GOOGLE: este tipo de eliminaciones cotidianas de recursos se repiten de forma rutinaria por toda la red. Lógicamente cuanto más antiguos sean los datos, más definitiva será la eliminación y más difícil será recuperarlos. Las eliminaciones más recientes de recursos no tan antiguos son ligeramente menos problemáticas, ya que los archivos y mensajes no eliminados permanentemente pueden recuperarse durante un breve período de la papelera de reciclaje o la carpeta de elementos recuperables.

2. Personal interno malintencionado

RIESGO PARA LOS DATOS: Los recursos de G Suite no solo deben protegerse frente a las eliminaciones rutinarias, no maliciosas, sino también frente a los casos de alteración o destrucción intencionada de datos por parte de empleados disgustados o malintencionados, o contratistas o partners descontentos.

PUNTO DÉBIL DE GOOGLE: con la excepción de las eliminaciones relativamente recientes de recursos, Google no protege contra la destrucción o alteración de datos de G Suite por parte de personal interno malintencionado. Después de todo, no tiene forma de saber qué constituye o no una amenaza.

3. Ciberamenazas

RIESGO PARA LOS DATOS: los datos de G Suite pueden ser destruidos o alterados por distintas amenazas de malware, particularmente el ransomware, que cifra los datos de los usuarios y los retiene hasta que se paga un rescate para recuperarlos. Estos ataques pueden ser obra de hackers, ciberdelincuentes o actores de Estados hostiles.

PUNTO DÉBIL DE GOOGLE: Google ofrece una protección muy limitada frente a los ataques de malware, como el ransomware, y tiene una capacidad reducida para restaurar los archivos cifrados o alterados por el malware y recuperar su estado previo al ataque.

4. Exempleados

RIESGO PARA LOS DATOS: las empresas cometen con frecuencia el error de cancelar las cuentas de G Suite de los empleados que abandonan la empresa o que son despedidos sin guardar sus datos.

PUNTO DÉBIL DE GOOGLE: con la excepción de las cancelaciones recientes de cuentas de G Suite (las realizadas en los últimos 20 días), Google no puede restaurar los datos de G Suite de los usuarios eliminados.

5. Lagunas en las directivas de retención

RIESGO PARA LOS DATOS: si las prioridades han cambiado o no son correctas en G Suite, se pueden eliminar datos de forma permanente cuando todavía son útiles. Esto solo se puede mitigar parcialmente mediante la revisión y actualización periódica de las directivas de conservación de información.

PUNTO DÉBIL DE GOOGLE: los clientes de G Suite son responsables de gestionar las directivas de conservación, pero, si por algún motivo, se produce una eliminación permanente debido a que la directiva actual sea obsoleta, Google no puede recuperar el recurso eliminado.

6. Problemas legales y de cumplimiento de normativas

RIESGO PARA LOS DATOS: los requisitos de cumplimiento de normativas (por ejemplo, el almacenamiento de documentos fiscales durante un período establecido) y los problemas legales pueden disparar los costes de pérdidas de datos no protegidos en la empresa, como se ha descrito anteriormente. La pérdida irrecuperable de datos de G Suite puede exponer a la empresa a sanciones de la Administración o del sector específico, a multas legales (por ejemplo, por daños o demandas judiciales por pérdidas derivadas del incumplimiento de los requisitos probatorios o de descubrimiento electrónico), a pérdidas de ingresos o valor bursátil, a la pérdida de la confianza del cliente y a daños en la imagen de marca de la empresa.

PUNTO DÉBIL DE GOOGLE: ante estas situaciones, Google no puede hacer mucho para proteger a las empresas que utilizan G Suite contra una variedad de riesgos legales y de incumplimiento. Por ejemplo, tras un ataque de ransomware, es posible que una empresa que almacene los datos personales de sus clientes europeos en G Suite no pueda satisfacer las solicitudes de una copia de los datos, lo que infringiría los requisitos del RGPD.

EN RESUMEN

Una vez que conoce los puntos flacos de Google en cuanto a protección de los datos de G Suite, puede empezar a buscar soluciones de protección de datos que suplan estas carencias. Todos sabemos que hay mucho en juego: la falta de prevención de pérdida de datos en G Suite puede tener efectos devastadores para la empresa.

ACRONIS BACKUP PROPORCIONA COPIA DE SEGURIDAD FÁCIL, EFICAZ Y SEGURA PARA G SUITE

COPIA DE SEGURIDAD DE NUBE A NUBE FÁCIL DE UTILIZAR PARA G SUITE

Acronis Backup protege sus datos de G Suite con una copia de seguridad directa, sin agente, desde la mayoría de los centros de datos de Google en la red global de centros de datos de Acronis. El agente de Acronis Backup se ejecuta en la nube segura Acronis Cloud, en lugar de en sus instalaciones, lo que simplifica y agiliza el proceso de configuración y mantenimiento.

RECUPERACIÓN MUY ESPECÍFICA PARA G SUITE

Acronis Backup ofrece una serie de funciones de recuperación mejoradas que facilitan la recuperación rápida de distintos elementos de G Suite. Estas funciones de recuperación muy específicas permiten descargar un archivo directamente desde la copia de seguridad, descargar varias versiones de documentos (no solo la más reciente) o restaurar cualquier elemento de datos en su ubicación original o en un nuevo destino.

FUNCIONES DE BÚSQUEDA AVANZADAS

Una funcionalidad de búsqueda práctica y sencilla permite encontrar rápidamente lo que necesita, como un mensaje de un empleado que se ha ido o un documento antiguo que necesita para resolver problemas legales. En el caso de Gmail, los clientes pueden recurrir a la búsqueda de metadatos para los buzones de correo, y realizar búsquedas por asunto, destinatario, remitente, nombre y fecha del archivo adjunto, o utilizar la búsqueda de texto completo para encontrar contenido en el cuerpo de los mensajes de correo electrónico. En Drive, Contactos y Calendar, los clientes pueden buscar por metadatos, como nombres de archivo.

CERTIFICACIÓN EXCLUSIVA BASADA EN BLOCKCHAIN PARA LOS DATOS DE GOOGLE DRIVE

Las empresas que hacen copias de seguridad de sus instancias de Google Drive a través de Acronis Backup pueden aprovechar el servicio integrado Acronis Notary, que utiliza la tecnología blockchain para comprobar que las copias de seguridad de Google Drive no han sido manipuladas. Esta capacidad para acreditar la integridad de sus copias de seguridad de Google Drive es particularmente útil en el caso de los documentos legales, contratos, archivos multimedia, grabaciones de cámaras de vigilancia, historias médicas, contratos de alquiler o leasing, y contratos de préstamos.

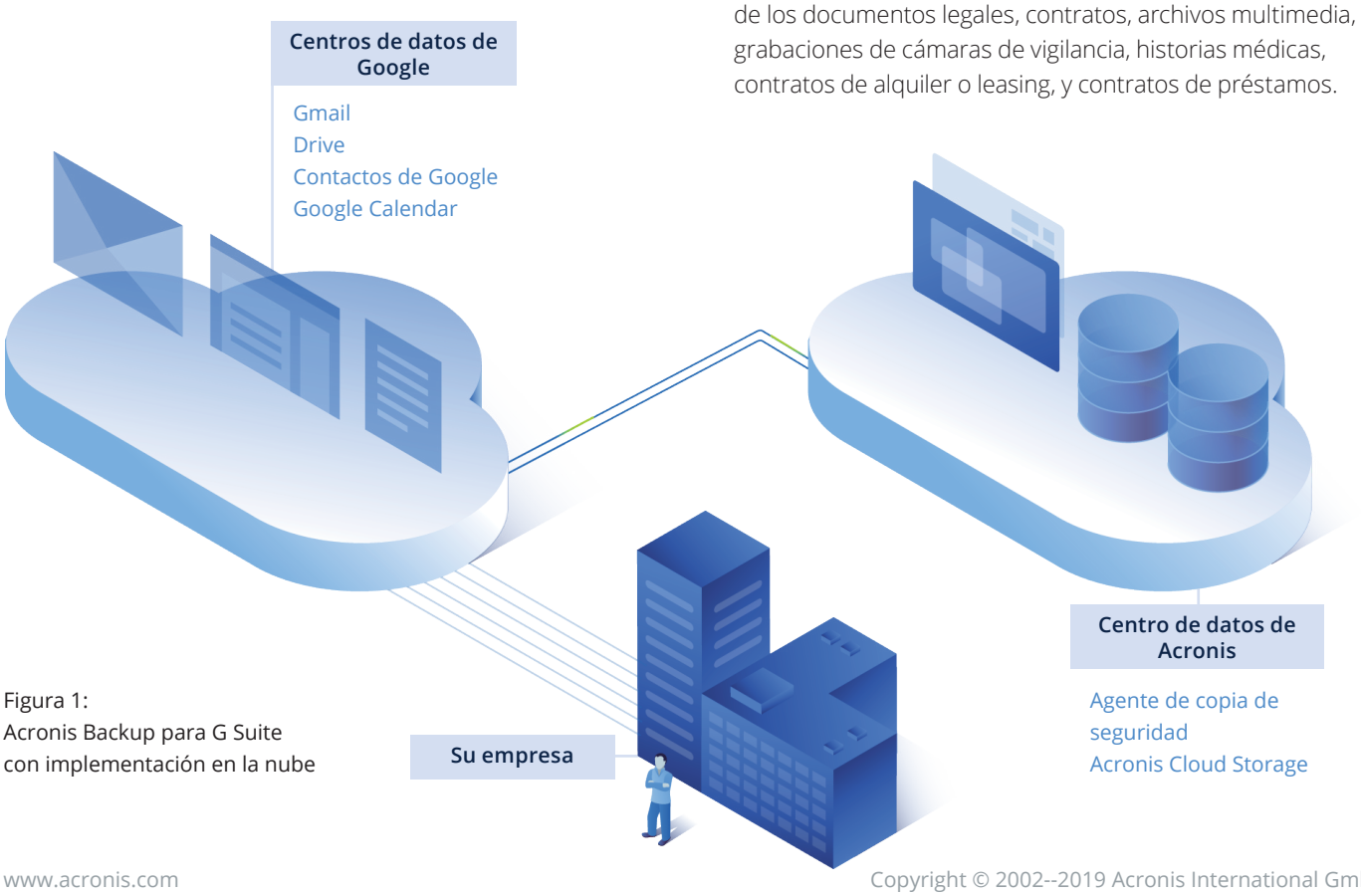

Figura 1:
Acronis Backup para G Suite con implementación en la nube

PRIVACIDAD DE DATOS MEJORADA

Acronis Backup protege los datos frente a la mirada de curiosos con cifrado de copias de seguridad multinivel reforzado por transferencias de datos por la red con cifrado TLS, almacenamiento en centros de datos con cifrado a nivel de disco de alta categoría y cifrado por archivo mediante AES-256.

RECUPERACIÓN AUTOMÁTICA DE NUEVOS USUARIOS DE G SUITE Y TEAM DRIVES

Una vez que se ha configurado y activado para G Suite un plan inicial de copia de seguridad de grupo, el personal de TI no tiene que preocuparse por modificarlo cada vez que se añade un nuevo usuario o Team Drive. Acronis Backup detecta automáticamente estas incorporaciones y actualiza el plan de copia de seguridad para incluirlas.

COMPATIBILIDAD CON LA AUTENTICACIÓN MULTIFACTOR DE GOOGLE

Acronis admite la autenticación multifactor (MFA) de Google para poder emplear otras medidas de autenticación, como los dispositivos de confianza o huellas dactilares. Sin MFA, solo se necesita una contraseña para la verificación.

HERRAMIENTAS POTENTES DE GENERACIÓN DE INFORMES Y SUPERVISIÓN DE ESTADO

Acronis ofrece funciones avanzadas de generación de informes y supervisión de estado, para ayudar al personal de TI a mejorar la eficiencia y la capacidad de reacción. El portal de administración de Acronis contiene widgets compactos y sencillos que incluyen todas las estadísticas de copia de seguridad y restauración, así como informes, notificaciones y alertas para incidentes críticos.

NUBE DE ACRONIS EXTREMADAMENTE SEGURA

Acronis guarda los datos de G Suite en la nube Acronis Cloud, una red global de centros de datos protegidos a través de un programa integral de seguridad de la información y cumplimiento que incluye controles administrativos, físicos y técnicos basados en la evaluación continua de riesgos.

Nuestros procesos y directivas de seguridad de la información se basan en normas de seguridad internacional aceptadas en todo el mundo, como ISO 27001 y NIST (National Institute of Standards and Technology), y tienen en cuenta los requisitos de los marcos de regulación locales, como el Reglamento general de protección de datos (RGPD) de la Unión Europea y la ley Health Insurance Portability and Accountability Act (HIPAA) de Estados Unidos. Las funciones de seguridad de Acronis Cloud incluyen:

- **Control de acceso en toda la empresa**, basado en ID de usuario exclusivos y contraseñas fuertes, protocolos de autenticación seguros (LDAP, Kerberos y certificados SSH), autenticación de dos factores y el uso de firewalls para aplicaciones web.
- **Seguridad multinivel basada en la zona,** reforzada con cifrado de datos en tiempo real, en tránsito y en espera, transferencias de datos seguras a través de HTTPS (TLS), cifrado AES-256 de categoría empresarial para los datos de los clientes, y la tecnología Acronis Cloud RAID para una máxima disponibilidad de los datos.
- **Seguridad física rigurosa,** con acceso controlado por exploración biométrica de la mano y tarjetas de clave de proximidad, videovigilancia respaldada por el archivado de 90 días y con personal de seguridad disponible 24x7x365.
- **Infraestructura de centros de datos de alta disponibilidad y redundante,** protegida por sistemas de alimentación ininterrumpida (UPS) y grupos electrógenos diésel de respaldo, HVAC redundantes, sistemas UPS y de red, muestreo de aire VESDA y sistemas de extinción de preacción en dos zonas (tubería seca), además de la monitorización de la temperatura.

ACRONIS PROTEGE SU ENTORNO COMPLETO DE G SUITE (Y TODO LO DEMÁS TAMBIÉN)

Acronis Backup es una **única solución de protección de datos para su entorno completo de G Suite**, ya tenga sus cargas de trabajo in situ o alojadas en nubes públicas o privadas.

Eso incluye una **amplia gama de plataformas** y aplicaciones, como entornos físicos, virtuales y en la nube, además de servidores que ejecutan alguno de los principales sistemas operativos e hipervisores, una amplia variedad de aplicaciones y base de datos, así como sistemas operativos para equipos de sobremesa, como macOS, y para móviles, como iOS y Android.

Una sola plataforma de protección de datos para su entorno de TI completo elimina la incompatibilidad mutua entre las distintas soluciones de copia de seguridad que solo se usan in situ o bien en la nube. Asimismo, reduce el coste de las licencias, la formación y la integración. La figura 2 muestra las más de 20 plataformas protegidas por **Acronis Backup.**

Además, la interfaz de usuario de Acronis Backup es lo suficientemente sencilla para que la utilicen incluso los generalistas de TI, lo que facilita la ampliación rápida de la plantilla de protección de datos, y ahorra costes diarios de implementación, mantenimiento y operaciones.

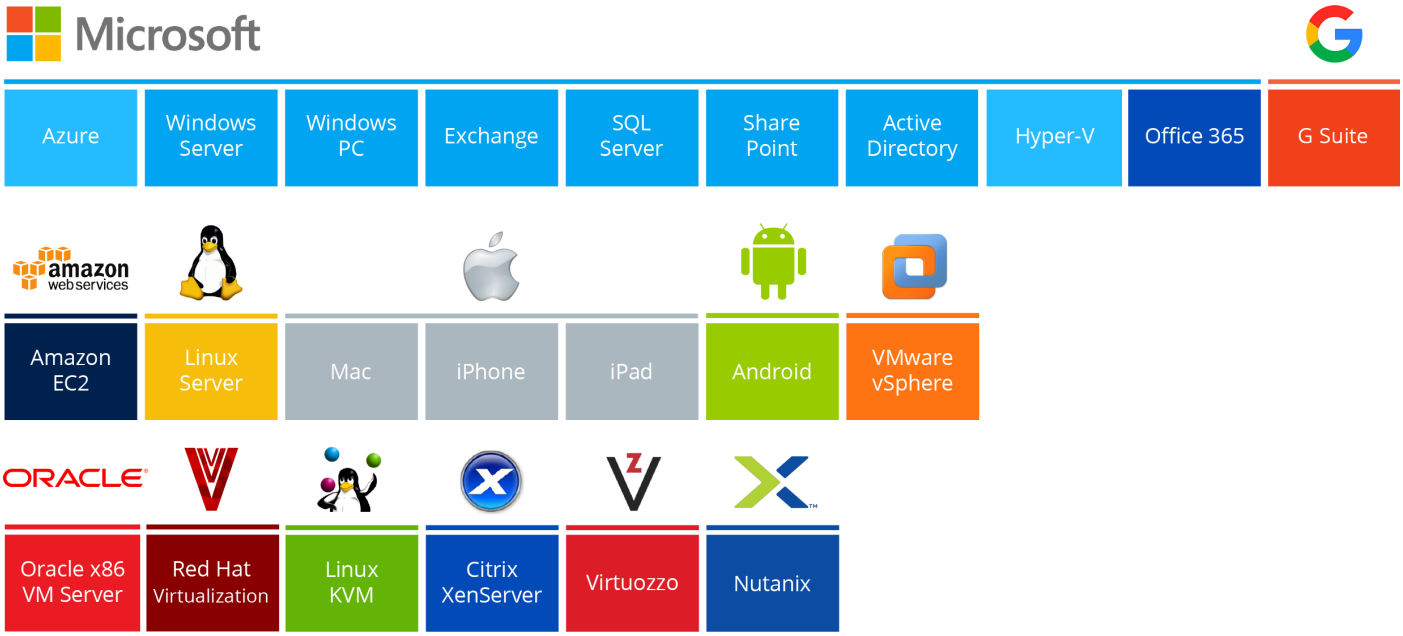

Figura 2. Plataformas protegidas por Acronis Backup

CONCLUSIÓN

Si su empresa depende de G Suite, necesita complementar la rudimentaria protección de datos que ofrece Google con Acronis Backup, la solución de copia de seguridad más fiable y fácil de utilizar para empresas de todos los tamaños.

Para obtener más información sobre las enormes ventajas en cuanto a **mejora, simplificación y reducción del coste de protección de datos de** G Suite que ofrece Acronis Backup, consiga una prueba gratuita de 30 días aquí o localice un distribuidor de Acronis aquí.