opentext™

Informe

# Seguridad de la información integrada OpenText

Existen sinergias entre la visibilidad que ofrece OpenText para plataformas de datos no estructuradas en sus diversos formatos de contenido y la protección ofrecida para garantizar su naturaleza crítica, independientemente de la ubicación, el dispositivo y los medios por los que se accede. En este informe realizado en 2020 por analistas de TAG Cyber, se describe el ecosistema del que disfrutan ahora los clientes, empleados y socios de OpenText para la gestión segura de experiencias digitales.

opentext™

## Contents

La seguridad, **después de redefinir el entorno de trabajo y la pandemia**, reaparece revitalizado como una iniciativa estratégica y esencial para apoyar los procesos de transformación digital, ya sea para proteger los dispositivos y aplicaciones que acceden, transforman y comparten datos estructurados o no. Los datos estructurados significan información que puede almacenarse en estructuras de bases de datos tradicionales, mientras que su opuesto, está representada por datos que no tienen características predefinidas en el formato de los campos, como imágenes, archivos PDF, textos, videos etc.

Independientemente de su formato, estructurado o no, es esencial comprender que, en la era posterior a la automatización de procesos y ERP, la información y su uso son actualmente responsables de la longevidad y la diferenciación competitiva de su empresa. La información estática y aislada en un entorno local o en la nube es un activo altamente perecedero, con colaboración y compartiendo el valor intrínseco de su contenido.

Tomemos a los bancos como ejemplo: de forma rutinaria durante sus procesos de digitalización de documentos para abrir cuentas, contratos de cambio de divisas, compensación de cheques, etc. organizan la documentación de sus clientes dentro de sus estructuras computacionales y supuestamente seguras, pero todos continúan invirtiendo fuertemente en tecnología de prevención de fraude porque en un mundo sin fronteras e interconectado, el costo de oportunidad y la probabilidad de quedar atrapado en el fraude en línea es infinitamente mayor que el de los delitos físicos. Por lo tanto, la seguridad debe integrarse y auditarse continuamente en el nivel crítico de información, su significado, contexto y formato del contenido o archivo donde reside, de lo contrario, siempre será después del hecho, incidente, dejando entender lo que sucedió para tratar de prevenir un ataque futuro.

Segundo, y quizás más importante, las tareas de ciberseguridad empresarial, como la investigación de fraudes o la respuesta ante incidentes, requieren cada vez más acceso a repositorios de datos de gran valor. Esto implica que las herramientas de seguridad requieren visibilidad de estos datos compartidos y deben poder determinar el contexto y usar inteligencia para identificar anomalías de seguridad o mitigar los efectos de la explotación de datos, de lo contrario, las organizaciones siempre serán rehenes por la escasez de profesionales altamente especializados con años de experiencia. Las contramedidas no pueden esperar la intervención humana, deben actuar rápidamente, replicando los estándares esperados y las mejores prácticas para contener violaciones de secretos o ataques.

El enfoque tradicional de la gestión de seguridad basado en eventos o incidentes ya no cumple con la 'nueva normalidad', ya que tomar medidas después de lo ocurrido, la violación de la confidencialidad o el fraude ya no previene el daño, la exposición de la marca y la pérdida financiera. La "nueva normalidad" requiere una postura de seguridad ***proactiva***, identificando qué información es crítica, dónde se encuentra y cómo y quién la maneja ***antes*** de perderla, comprometerla o compartirla por error.

El compromiso de OpenText con la seguridad comenzó con la inclusión de extensiones en sus plataformas de gestión de contenido - OpenText Content Manager y OpenText Documentun - agregando funciones de archivado de datos masivo y desmantelamiento de aplicaciones que garantizan la resistencia del acceso a los datos y los sistemas con costos operativos más efectivo. Más tarde evolucionando con la adquisición de Guidance Software, fabricante de EnCase™, la emblemática suite de software de investigación digital. La línea de productos de EnCase™ ahora es compatible con análisis forense digital, detección y respuesta de incidentes de seguridad en terminales, investigación forense remota de terminales, eDiscovery y análisis de seguridad, son los componentes clave de la solución de resiliencia cibernética de OpenText, sobre todo en el contexto de programas de seguridad empresarial.

Luego, OpenText dio otro paso significativo para lograr una experiencia de seguridad integrada mediante la adquisición de Carbonite, a fin de sumar copias de seguridad y recuperación a esta oferta. Las copias de seguridad y la recuperación de datos de gran valor en la nube son requisitos evidentes para lograr una verdadera resiliencia cibernética. Por lo tanto, la integración de Carbonite agregó un ingrediente clave a la plataforma de resiliencia cibernética de OpenText. Los analistas coinciden: "Haber sumado Carbonite proporciona una funcionalidad esencial y crítica de copia de seguridad para la gestión empresarial de OpenText", señaló Katie Teitler, analista de la industria cibernética de TAG Cyber.


Ecosistema en la nube y/o on-premise de gestión segura de contenido de OpenText

La incorporación de estas funciones de seguridad, como copias de seguridad y recuperación, soporte de investigación, herramientas analíticas de seguridad y seguridad de dispositivos o Endpoints, supone una nueva capa protectora central para el modelo de ecosistema de gestión de contenido de información de OpenText. Este conjunto de protecciones permite que los clientes de OpenText aprovechen las ventajas de la seguridad diseñada desde adentro, en lugar de tener que seleccionar, integrar y operar sistemas de seguridad que se agregan al proceso de gestión de información más adelante.

La plataforma de resiliencia cibernética de OpenText proporciona a las organizaciones seguridad y continuidad que permiten localizar datos dondequiera que se encuentren, sin importar el usuario, la ubicación, la red, la aplicación o la terminal. Las empresas no tienen de qué preocuparse, ya que los procesos y datos de gran valor están protegidos en cualquier circunstancia.

La protección **integrada** de OpenText se centra en un modelo de repositorio de datos compartidos. Es decir, así como las tareas de la plataforma de gestión de contenido deben acceder a los datos para el soporte de servicios de contenido, las tareas de seguridad empresarial acceden a los mismos datos para la protección cibernética. Este acceso compartido a los datos de gran valor crea oportunidades de sinergia, lo que explica cómo OpenText integró herramientas como EnCase™ al ecosistema de OpenText Content Manager y OpenText Documentum.

Este modelo de gestión de contenido seguro e integrado de OpenText se basa en las siguientes características del repositorio de datos compartidos:

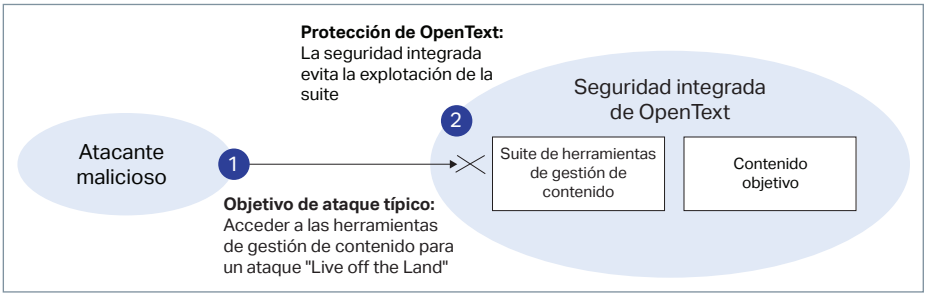
- **Datos críticos:** los equipos recopilan y usan datos para impulsar funciones empresariales. Los ejemplos van desde equipos legales que organizan un juicio en torno a los documentos que se usan para defender a un cliente, hasta gerentes ejecutivos que usan un repositorio de datos compartidos como base para la colaboración entre los grupos de su organización. En todos los casos, el valor de los datos es alto porque está directamente relacionado con el éxito de la misión.
- **Uso dinámico:** en un modelo de repositorio compartido, los atributos importantes de los datos almacenados son de carácter dinámico. Es decir, los datos estructurados y no estructurados de un repositorio cambiarán con rapidez, al igual que los valores, como propiedad, controles de acceso, normas y registros de auditoría. Por lo tanto, los repositorios requieren protección y seguridad continuas para adaptarse al ritmo de este cambio constante y dinámico.
- **Integración de procesos:** el uso de repositorios de datos compartidos deberá integrarse con otros flujos de trabajo de procesos en una organización. Estos flujos de trabajo pueden ser desde autorizaciones para el acceso hasta procesos más complejos, como el acceso legal por parte de las fuerzas de seguridad si se presenta una circunstancia inusual. OpenText tiene una vasta experiencia en dichos casos.
- **Alcance ilimitado:** la combinación de la funcionalidad de protección de la información y el soporte para múltiples dispositivos y sistemas operativos aseguran que la información relevante y crítica se encuentre donde sea que se encuentre y se monitoree de manera proactiva para que, en caso de amenazas o uso no autorizado, las contramedidas sean tomado de forma automática e inmediata.

La incorporación de la seguridad al modelo de repositorio compartido lleva el soporte de OpenText para el sistema de gestión de contenido a un nuevo nivel de protección de datos. "La empresa ahora puede ofrecer a sus clientes un modelo de seguridad exclusivo para sus datos mediante la integración de las características que OpenText siempre proporcionó para la gestión de datos en repositorios compartidos con herramientas de protección e investigación avanzadas como EnCase™", señaló Edward Amoroso, analista industrial de TAG Cyber.

La **gestión de contenido** es un componente importante de cualquier ecosistema digital a gran escala debido a la prominencia de los casos de uso de repositorios compartidos para equipos empresariales. Como es de esperarse, el riesgo de seguridad asociado con la gestión de contenido es considerable, y esto se debe, en parte, a las consecuencias graves de un ciberataque exitoso a un sistema de gestión (por lo general, con el objetivo de robar propiedades intelectuales o datos confidenciales importantes).

Sin embargo, el riesgo de seguridad más significativo asociado con la gestión de contenido deriva de la facilidad con la que un hacker puede aprovechar las herramientas y los programas avanzados de un entorno digital típico. Esto se puede ilustrar mediante la conocida amenaza *"Living off the Land"*, mediante la cual el intruso irrumpe en un sistema y se encuentra con que las herramientas existentes le serán útiles para el ataque.

El equipo de OpenText comprende el desafío de seguridad que implica que los hackers irrumpan en un sistema de gestión de contenido con la esperanza de encontrar herramientas avanzadas para organizar, buscar, ordenar, agregar y filtrar la información almacenada. Al integrar seguridad en sus productos de gestión de contenido, el equipo de OpenText aborda este escenario del ataque *"Living off the Land"* en la gestión de contenido a través de controles nativos.

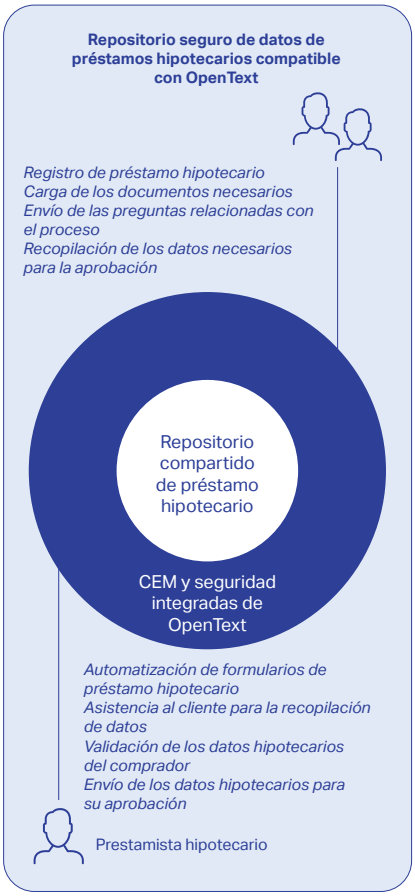



Ataque "Living off the Land" (y protección integrada) para la gestión de contenido

Se recomienda que los equipos que se basan en sistemas de Gestión de Contenido Empresarial (ECS) se aseguren de que su soporte de gestión de contenido incluya alguna medida de reducción de riesgos. Algunos proveedores de soluciones recomiendan agregar un proveedor de seguridad de terceros, y esto podría ser suficiente. Sin embargo, la solución de protección de seguridad integrada de OpenText proporciona seguridad y resiliencia superiores con un mínimo de tiempo y esfuerzo de integración adicional.

Brindar una gestión de experiencias digitales de primer nivel comienza por la visibilidad de los datos. Es decir, las organizaciones modernas siempre logran las mejores interacciones digitales con los clientes mediante la organización explícita y el uso compartido de contenido e información de gran valor. OpenText admite esta experiencia de ECS integrada mediante una suite de soluciones de plataformas comerciales que abordan las siguientes tareas esenciales de servicios de contenido:

- Gestión de contenido de website: el soporte relacionado con CEM (Customer Experience Management) es necesario para administrar y organizar de forma adecuada el texto y el contenido multimedia del website de un cliente.
- Gestión de comunicaciones con el cliente: gestionar y analizar las comunicaciones ayuda a las organizaciones a conocer el estado de las relaciones con los clientes.
- Automatización de formularios inteligentes: las empresas modernas saben que los formularios deben automatizarse para mantener un alto nivel de participación y satisfacción del cliente con los procesos.
- Optimización de marketing: los programas de marketing de primer nivel ahora están completamente impulsados por datos, lo que supone la necesidad de admisión de procesamiento de plataformas y automatización.
- Optimización de la fuerza laboral: las organizaciones modernas optimizan el valor y las contribuciones de su fuerza laboral mediante el análisis de tendencias y datos.
- Gestión de activos digitales: todos los activos digitales requieren coordinación y gestión mediante una plataforma compatible con el análisis y la creación de informes de forma automatizada.
- Análisis e inteligencia empresarial: el uso de analíticas de datos para fundamentar las decisiones empresariales ya está firmemente establecido en casi todos los contextos empresariales exitosos.




**Caso de estudio:** Seguridad integrada de OpenText con soporte de experiencias digitales y ECS para un proceso de préstamo hipotecario

El caso de estudio del préstamo hipotecario es muy útil porque ilustra la necesidad de integrar el ECS y la seguridad en un proceso que ya está creando una nueva experiencia para los clientes. Durante muchos años, los compradores llenaron formularios en papel para adquirir una hipoteca, por lo que el cambio a una experiencia en línea más automatizada puede generar incomodidad. Por lo tanto, evitar los roces adicionales de la seguridad y la administración de procesos son diferenciadores empresariales importantes.


Ecosistema de OpenText Digital Experience Management

La plataforma de OpenText se diseñó a fin de alinearse con las diversas tareas necesarias para lograr una visibilidad adecuada de los datos en ecosistemas de experiencias digitales. Estas tareas relacionadas con los servicios de contenido, que incluyen optimización, entrega, producción, análisis, organización y contacto, son compatibles con la plataforma comercial de OpenText. Estas tareas son necesarias para garantizar que las empresas modernas maximicen los datos de gran valor compartidos con sus clientes.

## Sobre OpenText

OpenText, The Information Company, permite a las organizaciones adquirir conocimientos a través de soluciones de gestión de información de primer nivel, en las instalaciones o en la nube. Para obtener más información sobre OpenText (NASDAQ: OTEX, TSX: OTEX), visite: opentext.com.

## Contáctenos:

- Blog de Mark Barrenechea, CEO de OpenText
- Twitter | LinkedIn

**opentext.com/contact**