Kaseya

datto

EBOOK

Simplifica la venta de BCDR:

Estrategias y Guiones para Profesionales de TI

Tabla de contenido

Introducción 3

Calculando el costo del tiempo de inactividad 4

Presentación del RPO 9

Presentación de reputación de la marca 10

Desarrollando experiencia en ventas 11

Presentando BCDR a tus clientes 12

Introducción

Muchas MSPs luchan para comunicar con claridad el valor de una verdadera solución de continuidad de negocio y recuperación ante desastres (BCDR) a clientes de pequeñas empresas. El reporte "State of the MSP 2026" de Kaseya reveló que el 71% de los MSPs considera que conseguir nuevos clientes es su mayor desafío.

Entonces, ¿qué está pasando?

Para empezar, muchos dueños de negocios no comprenden en qué se diferencia una solución de BCDR de un respaldo tradicional. Cuanto más conscientes son de los costos, más les cuesta justificar un mayor gasto en protección de datos en comparación con años anteriores, especialmente si nunca han sufrido una pérdida de datos grave ni interrupciones del servicio.

Luego están aquellos que no tienen idea de lo que significan la ciberseguridad o el ransomware (ni por qué deberían preocuparse).

Dicho esto, para convencer con éxito en la propuesta de BCDR, los MSPs deben tomarse el tiempo de educar a sus clientes y prospectos a traves de contenido informativo.

En este eBook aprenderás a cómo explicar los beneficios de una solución de BCDR totalmente gestionada frente a los productos de respaldo tradicionales, de la mano de MSPs exitosas que ya dominan este tema a la perfección.

También conocerás ejemplos reales de cómo las soluciones de BCDR pueden reducir el impacto financiero de una interrupción (es decir, el tiempo de inactividad del negocio) y tendrás acceso a un guion de ventas para presentar tu propuesta con eficacia.

"BCDR es un hueso duro de roer para muchas organizaciones. Muchas organizaciones pagan por soluciones de BCDR, pensando que están protegidas, pero no lo están. Antes de introducir cambios en el entorno de un cliente, necesitamos entender sobre qué estamos construyendo. BCDR es la base sobre la que construimos nuestra práctica. Si hay grietas en la base, tenemos una gran solución (Datto SIRIS 5) para llenar esos vacíos."

Robert Thurston,
Director de Operaciones, Vicinity

Herramienta adicional GRATIS

Descubre rápidamente la madurez del BCDR de tu MSP

Comienza ahora

Calcula el costo del tiempo de inactividad

Incluso unas pocas horas de inactividad pueden ser devastadoras para un negocio. Cuando un negocio está inactivo, los clientes no pueden realizar compras ni acceder a la información de sus cuentas. Los empleados no pueden trabajar y la perdida de acceso a cuentas se acumula rápidamente. Hubo un tiempo en que tardar días o semanas en recuperarse no tenía el impacto duradero que tiene ahora. Las copias de seguridad en cinta que requerían transporte físico eran lo suficientemente fiables para la época. Pero en 2026, las empresas no pueden esperar semanas o incluso días para volver a operar. En el mundo actual, la inactividad ya no es aceptable. La buena noticia: las soluciones BCDR eliminan la inactividad. Las empresas que no priorizan la implementación de BCDR simplemente se están exponiendo a problemas.

Desde fallas de servidores y cortes de energía hasta ciberamenazas, la inactividad puede ser causada por diversos factores. Según investigaciones de Oxford Economics, la inactividad le cuesta a las empresas aproximadamente **$9,000 por minuto**, o $540,000 por hora. Cuanto más tarde la recuperación, más severo es el impacto financiero y el daño a la reputación.

Estas son cifras que ninguna empresa puede permitirse tener. Piensa en el número de empleados afectados por un desastre, sus salarios, los costos generales asociados y las ganancias perdidas debido al desastre y súmalos todos por cada hora de inactividad. Añade a eso el impacto negativo de un incidente de inactividad en la reputación de una empresa (es decir, pérdida de confianza y/o negocios), y tendrás un golpe significativo a los resultados financieros en tus manos.

Las copias de seguridad manuales y las herramientas obsoletas ya no son suficientes. Las soluciones creadas hace 40 años resolvían problemas diferentes. Las herramientas de respaldo que añaden más trabajo a los empleados no son óptimas. Las personas cometen errores. El panorama de amenazas moderno ha evolucionado drásticamente.

Los clientes que se aferran a procesos de respaldo obsoletos o manuales pueden alcanzar el objetivo de respaldar sus datos, pero no pueden garantizar su disponibilidad cuando sea necesario, ni pueden asegurarse de que el proceso realmente esté funcionando. La continuidad del negocio no puede garantizarse con respaldos que dependen de que los empleados recuerden copiar los datos al final de la semana. Eso significa que se requiere de automatización. En particular, un respaldo en la nube híbrida promueve la continuidad.

“Una copia de seguridad es como un seguro. No lo necesitas hasta que lo necesitas. Y a veces, cuando te das cuenta de que lo necesitas, ya es un poco tarde.”

Keith Burton,
CEO, DataSHUR Corporation

La solución más rentable para las empresas que buscan respaldar cargas de trabajo críticas es basada en la nube. En 2026, la resistencia a la nube debido a preocupaciones sobre la fiabilidad ya no tiene sentido; solo está retrasando a las organizaciones. Las soluciones de respaldo híbrido en la nube ofrecen a las empresas acceso a una copia de seguridad local almacenada en el sitio y una copia adicional de toda su red almacenada en la nube. La copia de seguridad local permite un acceso rápido a los datos cuando es necesario. Mientras tanto, la nube mantiene otra copia disponible para conmutar en caso de un problema a gran escala, ayudando a las empresas a evitar tiempos de inactividad prolongados. El respaldo híbrido en la nube brinda a las organizaciones la seguridad que necesitan para responder rápidamente tanto ante desastres de datos pequeños como grandes.

Ninguna empresa es inmune a un desastre de datos. Las ganancias perdidas por tiempos de inactividad prolongados son demasiado sustanciales para arriesgarse. La tecnología obsoleta no es la solución.

Tambien puede interesarte:

Lista para elegir la solución de respaldo correcta de Microsoft 365 para tus clientes

Descárgalo ahora

Las empresas que desean seguridad frente a la creciente lista de amenazas necesitan considerar lo que pueden perder, así como las soluciones diseñadas para minimizar por completo el tiempo de inactividad.

El argumento de RTO/RPO es una excelente manera de justificar rápidamente el mayor costo de una solución integral de continuidad del negocio y recuperación ante desastres (BCDR) en comparación con una solución de respaldo tradicional. El objetivo es resaltar el valor de la continuidad del negocio frente al respaldo. Aquí hay una manera rápida y fácil de hacerlo utilizando la **Calculadora de Tiempo de Recuperación** gratuita de Datto. Vea cómo funciona.

Paso 1 – Determinar la cantidad de tiempo de inactividad que enfrenta la empresa

Al reunirte con clientes potenciales, comienza evaluando la cantidad de tiempo que se tarda en recuperar datos, ya sea localmente o desde la nube, en caso de pérdida de datos o interrupción. Necesitarás las siguientes métricas durante dicha evaluación:

Datos críticos del sistema: X GB
Los datos críticos del sistema son la cantidad de datos perdidos en un escenario que resulta en tiempo de inactividad para los empleados.

Intervalo entre copias de seguridad: X DÍAS X HORAS X MINUTOS
El intervalo en el que se realizan las copias de seguridad. Esto se utiliza para verificar el objetivo del punto de recuperación.

Inicio del proceso de recuperación: X DÍAS X HORAS X MINUTOS
El tiempo requerido para iniciar la recuperación de archivos o del sistema, incluyendo la notificación a un proveedor de servicios gestionados y la configuración del punto de recuperación.

Tiempo estimado de inactividad: X DÍAS X HORAS X MINUTOS
La cantidad de tiempo de inactividad se determina sumando el TIEMPO DE INICIO DEL PROCESO DE RECUPERACIÓN a la cantidad de tiempo que se tarda en recuperar completamente los datos perdidos (TIEMPO DE RECUPERACIÓN LOCAL).

La velocidad a la que se recuperan los datos perdidos depende de si se restauran localmente o desde la nube.
Velocidad local: La velocidad de restauración local predeterminada se basa en una conexión gigabit típica.

Nube: La velocidad de restauración en la nube predeterminada se basa en la velocidad promedio de conexión a Internet de las empresas en EE. UU.

Ejemplo:

- HORA DE INICIO DEL PROCESO DE RECUPERACIÓN: 1 Hora
- TIEMPO DE RECUPERACIÓN LOCAL: 1170 segundos
- HORA DE INICIO DEL PROCESO DE RECUPERACIÓN + TIEMPO DE RECUPERACIÓN LOCAL = TIEMPO DE INACTIVIDAD
- 1HR + (100 GB / VELOCIDAD LOCAL) = TIEMPO DE INACTIVIDAD
- 1HR + (819200 MB / 700 Megabits por Segundo (MBPs)*) = TIEMPO DE INACTIVIDAD
- 1HR + 1170 segundos = TIEMPO DE INACTIVIDAD
- TIEMPO DE INACTIVIDAD = 1HR 20MI

*Toma en consideración el tráfico de la red

Nota: Dado que la recuperación local es más rápida que la recuperación en la nube, resulta en menos tiempo de inactividad

Descubre por qué Xtona confía en Datto para la continuidad del negocio de sus clientes

Ver video

Paso 2 – Determinar el costo del tiempo de inactividad

Una vez que hayas estimado la cantidad de tiempo de inactividad que enfrenta la empresa en un escenario de pérdida de datos o interrupción, use la calculadora para encontrar el costo por hora del tiempo de inactividad.

El costo del tiempo de inactividad se determina primero por el costo total del tiempo de cada empleado. Esto incluye los salarios de los empleados, los costos generales (costos de suscripción, beneficios, etc.) y los ingresos perdidos como resultado de que los empleados no trabajan (pérdida de oportunidades de venta).

También podría incluir un sitio de e-comercio que se haya caído y que ya no genere ventas debido a una interrupción del sistema.

Valores de ejemplo:

- Empleados afectados: 10
- Salario promedio: $25/HORA
- Costos generales: $100/HORA
- Ingresos perdidos: $250/HORA
- Costo total del tiempo de inactividad: $600/HORAR

Introdúzcalo:

- (EMPLEADOS * SALARIO) + (COSTOS GENERALES + INGRESOS PERDIDOS) = COSTO DEL TIEMPO DE INACTIVIDAD
- (10 * $25/HORA) + ($100/HORA + $250/HORA) = COSTO DEL TIEMPO DE INACTIVIDAD
- ($250/HORA) + ($350/HORA) = COSTO DEL TIEMPO DE INACTIVIDAD
- COSTO DEL TIEMPO DE INACTIVIDAD = $600/HORA

Entonces, esto es lo que se dice: "RTO, que significa tiempo objetivo de recuperación, es el tiempo que toma restaurar las operaciones comerciales después de una interrupción."

También te puede interesar:

eBook: la última guia del BCDR

Descárgalo ahora

Luego, explícales por qué deberían preocuparse por esta métrica. "Claro, tienes copias de seguridad, pero ¿y si se va la luz? ¿Has considerado el tiempo que tomaría restaurar las copias de seguridad en caso de un corte de energía? Con la solución que estás utilizando actualmente, podría tomar días. Para algunas empresas, esto no es un gran problema: pueden funcionar sin conexión perfectamente. Para tu negocio, ¿cuánto tiempo de inactividad podrías permitirte?" ¿Viste lo que hice allí?

Muchas personas asumen que una copia de seguridad es simplemente una copia de seguridad. Y en cierto modo, eso es cierto: todos los productos de copia de seguridad crean una copia de los datos. Pero no todas las copias de seguridad se crean de la misma manera cuando se trata de restaurar datos y aplicaciones. Tienes que hablarles sobre el tiempo de recuperación.

Según el **Informe sobre el Estado de BCDR 2025**, solo el 40% de las empresas se sienten seguras de que sus sistemas de respaldo pueden proteger datos críticos en caso de una crisis.

El informe también revela una desconexión significativa entre las capacidades de recuperación percibidas y el rendimiento real. Mientras que más del 60% de los encuestados creían que podían recuperarse en menos de un día, solo el 35% pudo hacerlo durante eventos reales de interrupción.

Muchas empresas todavía dependen de procesos manuales frágiles. Por ejemplo, uno de los clientes de STCNtech respaldaba múltiples hosts Hyper-V en unidades USB. Técnicamente, los datos estaban almacenados en otro lugar, pero en la práctica, restaurarlos habría tomado días.

Como dice **Bruce Sarte**, Director de Operaciones de STCNtech: "Es genial que estés haciendo copias de seguridad. Pero si algo sale mal, restaurarlas llevará una eternidad. Podrías estar inactivo durante días."

Al hablar con clientes potenciales sobre BCDR, aclara los próximos pasos alentándolos a revisar sus métodos de respaldo actuales. Pídeles que identifiquen riesgos potenciales y discutan qué tan rápido podría recuperarse su negocio de una falla.

> "Me gusta la capacidad de decirles a los clientes: 'No importa lo que pase, podemos volver a ponerlo en línea.' Incluso si un coche choca contra su edificio, un avión aterriza en su oficina, hay una inundación o alguien roba su servidor, estamos cubiertos."
>
> **Keith Burton,**
> **CEO, DataSHUR Corporation**

El guión de venta del RPO (Objetivo de punto de recuperación)

Escenario: Supongamos que un cliente potencial o actual está utilizando el software de copia de seguridad XYZ para respaldar 500 GB de datos diariamente. Sabes por experiencia que restaurar 500 GB de datos utilizando el producto XYZ tomará un mínimo de 3 horas, suponiendo que no sea necesario adquirir ningún hardware nuevo.

Primero, pregunte: Si los sistemas de su empresa estuvieran caídos durante 3 horas, ¿cuánto le costaría ese tiempo de inactividad en ingresos perdidos? ¿Qué tal un día entero?

A continuación, explícale al cliente: Necesita pensar en el objetivo de punto de recuperación, o RPO, de su negocio. Su RPO se refiere a la cantidad de datos que su empresa corre el riesgo de perder entre copias de seguridad. Entonces, digamos que creó 10 GB de datos nuevos en un día, y una tubería se rompió, inundando un servidor a las 4 p.m. Si su copia de seguridad anterior ocurrió a las 6 p.m. de la noche anterior, esos 10 GB de datos se han perdido, para siempre. Por eso es una práctica estándar para las empresas actuales realizar copias de seguridad de datos periódicamente a lo largo del día.

Para resumir: Entonces, sabiendo esta información, también es importante que sepas que es casi imposible programar copias de seguridad periódicas a lo largo del día utilizando el software de respaldo XYZ.

Con tu solución actual, te enfrentas a la pérdida de un día de trabajo (o más). Estoy seguro de que te das cuenta de que esto se traduce al 100 % en pérdida de ingresos.

Cuando un propietario de negocio puede poner un valor en dólares a lo que podría perder, es mucho más fácil explicar el valor de una solución BCDR. En otras palabras, la pérdida de ganancias es más probable que resuene con un empresario que la pérdida de datos.

Las pruebas de recuperación ante desastres (DR) son esenciales para cumplir con los RTO y RPO, sin embargo, muchas organizaciones no prueban con suficiente frecuencia. Según el Informe sobre el Estado de BCDR 2025, el 21% realiza pruebas trimestralmente y el 13% anualmente, dejando a un número significativo sin preparación para tiempos de inactividad inesperados.

También puede interesarte:

10 consejos profesionales para vender BCDR de manera más efectiva

Descargue ahora

El guión de venta de la reputación de marca

Como se señaló anteriormente, muchos dueños de pequeñas empresas no entienden que no todas las soluciones de respaldo se crean por igual cuando se trata del tiempo de recuperación.

Dependiendo de los productos que elija, la recuperación de los sistemas críticos para el negocio puede llevar mucho tiempo, y el impacto financiero de la inactividad empresarial puede ir más allá de la simple pérdida de ingresos.

La inactividad puede tener un impacto serio en la reputación de una empresa. Este es un concepto importante para comunicar también a los prospectos.

Una manera de ilustrar esto a los clientes potenciales es pedirles que imaginen cómo reaccionarían sus propios clientes si ellos no pudieran atenderlos durante un período de tiempo prolongado, digamos, un día entero. Considera la naturaleza del negocio y adapta el mensaje de acuerdo a eso. Por ejemplo, un día de inactividad en TI no va a afectar la reputación de un restaurante local de la misma manera en que afectaría a un pequeño bufete de abogados. Busca ejemplos en tu propio negocio. Si tienes un cliente que dejó a otro proveedor de servicios de TI porque no pudo recuperar las operaciones de TI rápidamente, podrías incluir su historia en tu presentación.

Las brechas de seguridad pueden afectar negativamente la reputación de un negocio, especialmente en industrias que manejan datos sensibles de los clientes. Aunque una solución BCDR no es exactamente una herramienta de seguridad, sí permite a los usuarios recuperarse rápidamente de una brecha de seguridad.

> “Hay mucho valor en trabajar con Datto. Son excelentes con el programa de fondos para desarrollo de marketing (MDF), que aprovechamos mucho para promover eventos únicos a los clientes, mostrándoles el verdadero valor de cómo las soluciones de Datto pueden ayudar a salvar sus negocios.”
>
> **Nicolas Côté,**
> **Gerente de Práctica de Ciberseguridad**

También puede interesarte

Demasiadas copias de seguridad, no suficiente beneficio: Una manera más inteligente de avanzar

Mira el Webinar ahora

Desarrolla experiencia en ventas

Tienes la información que necesitas para educar a los clientes potenciales sobre el valor de BCDR. Eso es un buen comienzo, pero la tecnología no se vende sola. Por lo tanto, todavía necesitas dedicar tiempo y recursos a las ventas.

Como se señaló al inico de este eBook, hay dos formas de desarrollar experiencia en ventas: contratar a alguien con experiencia en ventas o capacitar a alguien que ya esté en el personal. Si realmente te importa el crecimiento, contratar vendedores capacitados puede marcar una gran diferencia. Sin embargo, esto podría no estar dentro del presupuesto para algunos negocios. Muchos negocios no tienen la capacidad para enfocarse en ventas y desarrollo empresarial. Ya tienen las manos ocupadas haciendo lo que mejor hacen: monitorear, mejorar o reparar las infraestructuras de TI de los clientes.

Entonces, ¿cómo hacer para dedicarte a las ventas y marketing, incluso si es solo a tiempo parcial? Supongamos que eres el propietario de un MSP con cinco empleados a tiempo completo (incluyéndote a ti). ¿Qué te impide entrenar a tu empleado más senior para que asuma algunas de tus responsabilidades técnicas? O si no tienes inclinación por las ventas, quizás uno de tus empleados sea adecuado para asumir un papel en ventas.

Una vez que tengas a alguien dedicado a ventas, es esencial enfocar tus esfuerzos en encontrar clientes que sean adecuados para tu negocio. Esto surge una y otra vez en conversaciones con MSP exitosos: no todos los clientes son buenos clientes.

Esto puede ser una píldora muy difícil de aceptar cuando recién estás comenzando en el negocio de servicios de TI. Cuando no tienes muchos clientes, es difícil rechazar a cualquiera. Pero necesitas dejar de perseguir cada oportunidad y concentrarte en las correctas. Debes saber cuándo decir no.

Identificar buenos clientes comienza con la investigación. ¿De qué es la empresa? ¿Está sujeta a regulaciones de cumplimiento? Identifica esos detalles, verifica si están sujetos a ciertas regulaciones y preséntate con ese argumento.

Muchas pequeñas empresas están tan concentradas en los costos iniciales de la tecnología que pasan por alto un punto obvio. El costo de la inactividad puede ser mucho mayor para su negocio. Cuando los prospectos no entienden este concepto, no deberías molestarte en perseguirlos.

Presentando BCDR a tus clientes

Por qué necesitas una solución BCDR

Cada organización necesita un plan sólido de continuidad del negocio y recuperación ante desastres. Sin embargo, la protección de datos a menudo se pasa por alto, a pesar de los graves riesgos de ignorarla. Entonces, ¿por qué deberías preocuparte?

El tiempo de inactividad es costoso

Si sus empleados o clientes no tienen acceso a aplicaciones y datos esenciales, la productividad y los ingresos se verán directamente afectados. Aunque esto suena obvio, muchas organizaciones no consideran los costos reales del tiempo de inactividad. Para entender mejor el costo del tiempo de inactividad, considere el siguiente ejemplo. Supongamos que su empresa tiene 100 empleados, el ingreso promedio por hora es de $1,500 y el conjunto de datos de respaldo es de 2 TB. Con estos parámetros, una restauración completa desde una copia de seguridad local usando software de respaldo tradicional tomaría más de 8 horas. El tiempo de inactividad asociado costaría $34,000 en ingresos perdidos. Algunos productos modernos de protección de datos permiten que las aplicaciones se ejecuten desde el dispositivo de respaldo o en la nube.
Esto permite a los usuarios continuar con las operaciones mientras se restauran los servidores de aplicaciones principales. Elegir una solución BCDR diseñada para reducir el tiempo de inactividad tiene sentido desde el punto de vista empresarial.

La copia de seguridad por sí sola no es suficiente

Sería difícil encontrar hoy en día un negocio que no realice algún tipo de copia de seguridad de datos. Pero, ¿qué sucede si una inundación destruye sus servidores principales y de respaldo? Enviar una copia de los datos fuera del sitio para la recuperación ante desastres también debe considerarse esencial. Históricamente, esto significaba enviar cintas a una ubicación secundaria, como una bóveda de cintas. Como se señaló anteriormente, los productos modernos de BCDR pueden ejecutar aplicaciones desde instancias de respaldo de servidores virtuales, y algunos pueden extender esta capacidad a la nube.

Este enfoque se llama con frecuencia DR en la nube o Recuperación ante Desastres como Servicio (DRaaS). La capacidad de ejecutar aplicaciones en la nube mientras se restaura la infraestructura en el sitio se considera ampliamente un cambio fundamental para la recuperación ante desastres.

No todos los desastres son desastres naturales generalizados. De hecho, la mayor parte del tiempo de inactividad de TI es causada por eliminación accidental (o intencional) de datos, daños en el hardware y malas prácticas de seguridad. Por ejemplo, un reciente estudio de Panda Security encontró que **casi el 25 % de los estadounidenses omiten protecciones básicas**, como VPN o software antivirus, al conectarse a Wi-Fi público. Como resultado, casi el 40 % reporta haber experimentado incidentes de seguridad después de usar estas redes. Un ataque de criptolocker o un virus puede detener las operaciones con tanta facilidad como una tubería rota o un aumento de tensión eléctrica. Estos desastres ocurren regularmente, y los costos de tiempo de inactividad asociados se acumulan con el tiempo. Contar con tecnología que permita a su negocio continuar operando después de estos pequeños desastres es igualmente, si no más, importante que protegerse contra un huracán que puede o no ocurrir.

La continuidad del negocio es una preocupación de todos

Los datos son esenciales para todo tipo de organizaciones hoy en día, por lo que garantizar el acceso a las aplicaciones y a los datos después de un desastre es fundamental. Pero es solo una pieza del rompecabezas de la protección de datos. Evaluar la capacidad de su negocio para restaurar las operaciones de TI puede ser un buen punto de partida para los esfuerzos de continuidad del negocio a nivel de toda la empresa. Una buena **planificación de la continuidad del negocio** debe considerar el negocio en su conjunto, con el objetivo de desarrollar la resiliencia empresarial. De hecho, muchos esfuerzos de planificación de continuidad del negocio comienzan con un análisis de impacto empresarial o una evaluación de riesgos: estos estudios pueden revelar debilidades en la capacidad de su negocio para continuar las operaciones que se extienden mucho más allá de TI.

Ayuda a los clientes a entender el valor de BCDR

Justificar el costo más alto de las soluciones BCDR a pequeñas empresas conscientes de los costos es definitivamente un desafío. Sin embargo, si enfocas tus esfuerzos en encontrar las empresas correctas y comunicar el mensaje adecuado, se puede superar fácilmente.

Como se señaló anteriormente, la educación del cliente es una pieza esencial. En la página siguiente, encontrarás un folleto que explica los beneficios de BCDR sobre otras soluciones de protección de datos. Comunica el valor de BCDR a los dueños de negocios y tomadores de decisiones en términos claros y fáciles de entender.

Mientras tanto, mira a Datto en acción y descubre cómo nuestra solución BCDR, todo en uno, protege los datos críticos para el negocio de tus clientes sin importar dónde se encuentren.

Agenda una Demo