INSTRUCTURE

DISASTER RECOVERY PLAN & PROCEDURES

Engineering, Security, y Operations

Junio 2022

Índice

INSTRUCTURE

Business Continuity

Cada organización está sujeta a una variedad de riesgos mientras realiza negocios. Estos riesgos pueden tomar forma en forma de amenazas externas graves, como el terrorismo cibernético o la agitación política, a los riesgos menos graves (pero aún importantes) de retener personal clave o incluso tener que enfrentarse a un panda enojado. Pero sea cual sea el riesgo percibido, es fundamental que una organización identifique, evalúe y mantenga un Plan de Continuidad del Negocio (PCN) para prevenir y recuperarse de amenazas potenciales o reales a sus activos más valiosos. En Instructure, nuestros sólidos procesos de gestión de riesgos nos permiten identificar, evaluar y tratar estos riesgos de forma continua. Para ayudar a fortalecer nuestro Plan de Continuidad del Negocio, nuestro Comité Directivo de Riesgos Empresariales, compuesto por líderes clave de Instructure, se reúne de manera regular y continua para identificar y mitigar los riesgos que podrían afectar a Instructure, su misión y sus activos más preciados.

Naturalmente, en el corazón de cada programa de continuidad del negocio se encuentra un plan sólido de respuesta a incidentes, un plan que ayuda a guiar eficazmente a una organización a través de los incidentes que pueden surgir de vez en cuando. En Instructure, tenemos un plan de respuesta a incidentes detallado, considerado y operativo que incluye preparar, detectar, evaluar, escalar, responder, comunicar los impactos y aprender de la seguridad, la disponibilidad, la privacidad, los recursos humanos, las finanzas y otros. incidentes imprevistos (léase: panda enojado). El plan de respuesta a incidentes es el punto de partida para todos los incidentes y puede escalar fácilmente, según el tipo y la gravedad del incidente, a una variedad de otros planes de Instructure, incluidos planes de recuperación ante desastres, planes de continuidad del negocio, planes de gestión de crisis, planes de evacuación, planes para pandemias y otros planes estratégicos para ayudar en la recuperación efectiva y eficiente de nuestras operaciones comerciales.

Uno de los riesgos que afecta a todas las organizaciones es la capacidad de mantener las operaciones comerciales en vuelo identificando, evaluando y mitigando las amenazas que podrían afectar las operaciones comerciales. Esto fue claramente evidente en 2020, un año que nos puso a prueba como ningún otro que habíamos visto antes. La pandemia mundial COVID-19 nos mostró claramente, y a todos, lo crucial que es un plan de continuidad comercial en tiempos de incertidumbre. El cambio y la agitación que vimos en 2020 probablemente se harán eco durante muchos años, tanto en términos de tendencias educativas como de cambios en la forma en que vemos el trabajo y quizás desde dónde trabajamos. El propósito de este documento es establecer cómo abordamos la continuidad del negocio aquí en Instructure como parte de nuestro programa continuo de gestión de riesgos a medida que continuamos con nuestra misión de ser la plataforma de gestión del aprendizaje líder en la industria.

Recuperación de desastres

También se incluyen como parte de nuestro plan de continuidad comercial nuestros planes y procedimientos de recuperación ante desastres. Ninguna empresa quiere un desastre, ya sea la pérdida catastrófica de un centro de datos o un panda loco corriendo por la oficina tirando de los cables. Pero si llega el momento, tener un plan sólido de recuperación ante desastres nos permite restaurar nuestros servicios lo más rápido posible y minimizar las pérdidas o interrupciones tanto para nuestros clientes como para nuestras operaciones internas.

En este documento se incluye una descripción general del plan y los procedimientos de recuperación de desastres que Instructure ha establecido para recuperarse de los desastres que afectan sus operaciones de producción. Describimos cómo nuestra oferta de software como servicio (SaaS) ha sido diseñada para recuperarse de escenarios de desastre, los pasos que tomaremos si se declara un desastre, nuestras políticas, estrategias de comunicación y procedimientos de notificación al cliente, y varios escenarios de ejemplo y evaluaciones de impacto.

Desarrollando Resiliencia y Manteniendo Planes de Recuperación Efectivos

El enfoque de Instructure para la continuidad del negocio está incorporando resiliencia en sus procesos, tecnología y personas. Este documento describe las diferentes prácticas que utiliza Instructure para garantizar la resiliencia empresarial a través de las funciones comerciales centrales al

garantizar la sincronización entre el uso de tecnología y aplicaciones, la infraestructura y los proveedores de servicios en la nube y el personal. Este enfoque se basa en las mejores prácticas de la industria para SaaS para mitigar el tiempo de inactividad causado por la interrupción común de los vectores de servicio para las compañías SaaS, incluidos, entre otros, ataques cibernéticos, violaciones de seguridad física, dependencias de proveedores, fraude y disturbios civiles, pandemias y desastres naturales o provocados por el hombre.

Las prácticas adoptadas por Instructure aumentan la capacidad de recuperarse de una interrupción en el servicio y proteger los datos de sus clientes, así como a su personal. Estas prácticas involucran procesos para prácticas preventivas y de recuperación que apuntan a cumplir los siguientes objetivos:

- Proporcionar un servicio continuo a los clientes
- Reducir el riesgo para las operaciones comerciales centrales
- Mantener una comunicación clara con clientes y empleados.

Procesos

Instructure ha diseñado y opera los siguientes procesos clave para respaldar las operaciones comerciales continuas (y eficaces de recuperación de incidentes que impactan) de Instructure:

- **Planes de respuesta a incidentes** - Instructure ha desarrollado, mantiene y opera planes integrales de respuesta a incidentes. Estos planes incluyen definiciones de preparación, detección, evaluación de la gravedad del incidente, escalada, acciones de contención que se tomarán en función de la gravedad del incidente, métodos de comunicación, pruebas y manuales, o ejemplos de qué hacer ante ciertos incidentes y mejoras.

- **Planes de backup y recovery:** Instructure ha desarrollado, mantiene y opera planes sólidos de respaldo y recuperación ante desastres. Estos planes incluyen tomar instantáneas diarias (copias de seguridad) y replicar datos casi en tiempo real en una ubicación separada y geográficamente aislada dentro de la región del cliente. Debido a que Instructure utiliza el líder mundial en infraestructura como servicio (IaaS), Amazon Web Services (AWS) para alojar datos en la región geográfica del cliente, cada región tiene múltiples ubicaciones aisladas conocidas como zonas de disponibilidad donde los datos del cliente se replican con fines de recuperación ante desastres. . El uso de varias zonas de disponibilidad de AWS es para garantizar que, si hay una falla en una ubicación física, los datos estén disponibles en otra ubicación geográficamente separada. Las copias de seguridad y los objetos cargados por el cliente se almacenan en Amazon S3, que cuenta con un 99,999999999% de tiempo de actividad y fiabilidad durante un año determinado. Las copias de seguridad se verifican para verificar su integridad y se prueban al menos una vez al mes.

- **Evaluaciones de proveedores -** Instructure opera un sólido programa de gestión de riesgos de seguridad de terceros. Estas prácticas incluyen la administración de un inventario preciso de proveedores, la realización de evaluaciones de riesgos de proveedores y la revisión de las

prácticas críticas de seguridad y disponibilidad de los proveedores. Estas revisiones incluyen garantizar que los proveedores tengan prácticas sólidas para los planes de respaldo, recuperación ante dEnesastres y continuidad del negocio. Además, Instructure también garantiza que los acuerdos de nivel de servicio con los proveedores contengan una descripción de los servicios prestados y contengan información sobre la disponibilidad de red prometida.

- **Ciberseguro -** Instructure asegura que protege a su negocio de gastos mayores, pérdidas comerciales y multas y sanciones regulatorias en caso de que se produzca una violación de datos al tener cobertura de seguro cibernético.

- **Prueba anual de recuperación -** Instructure prueba los planes de recuperación al menos una vez al año utilizando tanto pruebas de escenarios en vivo como pruebas de mesa. Los escenarios incluyen eventos donde ocurren interrupciones del servicio y el personal incluido en las pruebas de mesa es responsable de determinar las acciones utilizadas para recuperar los servicios.

- **Gestión de Riesgos -** Instructure reconoce la gestión de riesgos como un componente crítico de sus operaciones que ayuda a verificar que los activos de los clientes estén debidamente protegidos e incorpora la gestión de riesgos en todos sus procesos.

- **Planificación estratégica -** Instructure tiene un plan estratégico general que se presenta a la junta directiva. Este plan se divide en planes de segmento específicos diseñados para poner en funcionamiento lo que se espera de los segmentos para apoyar los objetivos generales de Instructure.

- **Canales de comunicación -** Instructure cuenta con procesos para responder a incidentes e informar a todo su personal en caso de una interrupción del servicio o evento que deba comunicarse a su personal. En general, los clientes serán notificados principalmente por su respectivo Customer Success Manager (CSM), que es el principal punto de contacto con todos los clientes. Los CSM utilizarán los métodos preferidos de comunicación identificados por el cliente. En el caso de una interrupción que afecte ampliamente, las notificaciones también se proporcionarán utilizando un sitio web público más ampliamente disponible con los últimos detalles. Para las comunicaciones internas, Instructure ha identificado medios de comunicación primarios y secundarios durante un evento impactante para mantener los esfuerzos de recuperación efectivos durante un incidente.

- **Entrenamiento de crisis -** Instructure cuenta con un equipo de respuesta a crisis que consta de sus equipos de Recursos Humanos, Comunicación, Legal y Seguridad para responder a situaciones de crisis en las oficinas de Instructure. Además, Instructure participa en entrenamiento y ejercicios de crisis, que incluyen, por ejemplo, respuestas a tiradores activos y simulacros de incendio.

Propiedad

El director de seguridad de la información (Chief Information Security Officer - CISO) de Instructure es responsable de supervisar la continuidad del negocio en coordinación con el vicepresidente sénior

(SVP) de Ingeniería. También contamos con un equipo de recuperación ante desastres definido con escalamiento final al vicepresidente sénior de ingeniería. En el aspecto comercial, todos los posibles desastres se escalan de inmediato al director financiero, quien es el responsable final de evaluar el evento y dirigir las notificaciones.

Sitio de Recuperación Alternativo

El personal de Instructure tiene la capacidad de trabajar desde casa en caso de una interrupción que afecte la capacidad de trabajar desde una de las ubicaciones de la oficina de Instructure. Para asegurar que esta práctica sea efectiva, Instructure asegura que existen políticas de teletrabajo implementadas y comunicadas a todo el personal, que existen prácticas de seguridad para acceder a las redes corporativas y que se implementan servicios de notificación de comunicación masiva. Se utilizan varios proveedores para proporcionar conectividad a las oficinas de Instructure, lo que permite reanudar rápidamente la conectividad si un proveedor no puede proporcionar el nivel de servicio requerido para mantener una conectividad constante y continua. Como parte de las pruebas de mesa de continuidad del negocio anual de Instructure, los casos de uso pueden incluir eventos que afecten a los empleados remotos, las oficinas de Instructure y los procedimientos de comunicación.

Capacitación

Instructure tiene un equipo de respuesta a crisis que consiste en sus equipos de Recursos Humanos, Comunicación, Legal y Seguridad para responder a situaciones de crisis en las oficinas de Instructure. Además, Instructure participa en entrenamientos y ejercicios de crisis que incluyen simulacros de incendio y evacuaciones de emergencia.

Código fuente abierto

El compromiso de Instructure con el código abierto comercial proporciona otra capa de tranquilidad a los clientes en términos de continuidad comercial. Canvas Learning Management System está disponible como código abierto, lo que significa que el código Canvas LMS es gratuito, público y completamente abierto en todo momento*. Cualquiera puede usar el código Canvas LMS sin costo adicional. Instructure actualiza el código de Canvas LMS de forma regular y el código se mantiene en Github: https://github.com/instructure/canvas-lms/wiki.

En el improbable caso de que se produzcan cambios sustanciales en las operaciones comerciales normales de Instructure, nuestros clientes tienen acceso al código de fuente abierta de Canvas LMS para permitir la continuidad del negocio. Esto permitiría a las instituciones alojar, operar y admitir el código de fuente abierta de Canvas LMS en sus propios servidores en caso de que Instructure ya no pudiera hacerlo. Además de nuestro código fuente abierto, Canvas LMS también proporciona exportación de contenido, acceso abierto a la API RESTful y datos de Canvas LMS. Esto significa que las instituciones siempre tendrán acceso al contenido y a los datos del curso.

*excluye algunos complementos y extensiones que actualmente no son de código abierto

Recuperación de Desastres

Términos clave y suposiciones

En el espacio Software como servicio (SaaS), hay algunos términos clave en relación con la recuperación ante desastres.

1) En el contexto de un escenario de recuperación ante desastres, se suelen utilizar dos términos para describir cómo puede verse afectado un proceso de recuperación: **Objetivo de tiempo de recuperación (RTO)** y **Objetivo de punto de recuperación (RPO)**. El RTO representa cuánto tiempo se necesitará para restaurar el acceso a los datos y el RPO la cantidad de datos que corren el riesgo de perderse. Por ejemplo, si se necesitan 8 horas para recuperar un servicio, el RTO es de 8 horas. Si las últimas 4 horas de datos se perderán potencialmente debido a un desastre, el RPO es de 4 horas.

2) Si bien **"Recuperación ante desastres"** y **"Alta disponibilidad"** son conceptos compartidos en relación con la continuidad del negocio, tienen un impacto diferente en la planificación de la recuperación ante desastres. La recuperación ante desastres básicamente infiere que habrá algún tipo de tiempo de inactividad involucrado, medido en horas o días. Sin embargo, la alta disponibilidad se trata de garantizar la continuidad continua de las operaciones en un escenario de recuperación ante desastres, especialmente mediante el diseño de redundancias arquitectónicas, como la conmutación por error automatizada de componentes.

Nuestros servicios están diseñados para lograr RPO y RTO excepcionalmente bajos en los escenarios más comunes y alta disponibilidad para nuestros clientes debido a la naturaleza distribuida y resistente de nuestra infraestructura. Para la gran mayoría de los escenarios de falla, se obvia la necesidad de conmutar por error a otra zona de disponibilidad (AZ) y los impactos en nuestros servicios serán mínimos.

La suposición principal de nuestro plan de recuperación ante desastres es que solo aborda los eventos que afectarían a todo un centro de datos a nuestra arquitectura en su conjunto. Las fallas de los componentes individuales se recuperarán mediante robustas redundancias arquitectónicas y mecanismos de conmutación por error.

Recuperación ante desastres en un mundo SaaS

El software educativo de Instructure (y los datos asociados) está alojado en la nube por Instructure y se entrega a través de Internet a través del proveedor de nube pública más confiable del mundo, Amazon Web Services (AWS). Este modelo de entrega de software como servicio (SaaS) significa que nuestros clientes no tienen que preocuparse por el mantenimiento del hardware o software del servidor, parches, paquetes de servicios o, en el contexto de este documento, la recuperación ante desastres.

No solo mantenemos nuestros propios planes y procedimientos sólidos de recuperación ante desastres, sino que también nos beneficiamos del uso de AWS, un líder mundial en infraestructura como servicio (IaaS) que integra la redundancia en sus servicios al proporcionar numerosas regiones,

zonas de disponibilidad y centros de datos. que nos permiten recuperarnos rápidamente en caso de un desastre imprevisto.

Dada la naturaleza del modelo de entrega de SaaS, Instructure es responsable de proporcionar recuperación ante desastres en relación con nuestro software y los datos asociados. Naturalmente, las mejores prácticas también dictan que nuestros clientes desarrollen y mantengan sus propios planes y procedimientos de recuperación de desastres.

Definición de Desastre

Un desastre se define como cualquier evento perturbador que tenga efectos adversos potencialmente a largo plazo en el servicio de instrucción. En general, los eventos de desastre potenciales se abordarán con la más alta prioridad en todos los niveles en Instructure. Tales eventos pueden ser intencionales o no intencionales, de la siguiente manera:

- **Desastres naturales:** tornados, terremotos, huracanes, incendios, deslizamientos de tierra, inundaciones, tormentas eléctricas y tsunamis.

- **Sistemas de suministro:** fallas en los servicios públicos, como líneas de gas o agua cortadas, fallas en las líneas de comunicación, cortes / aumentos de energía eléctrica y escasez de energía.

- **Hecho por el hombre / político:** terrorismo, robo, trabajador descontento, incendio provocado, huelga laboral, sabotaje, disturbios, vandalismo, virus y ataques de piratas informáticos.

Procedimientos de recuperación ante desastres

Fase de Monitoreo de Desastres

Instructure monitorea el desempeño de nuestros servicios las 24 horas del día utilizando herramientas externas de monitoreo de desempeño y herramientas de monitoreo internas, abiertas y cerradas. Estas herramientas están configuradas para enviar alertas en tiempo real a nuestro personal cuando ocurren ciertos eventos que justificarían la investigación de un posible escenario de desastre inminente.

Fase de Activación

Todos los posibles desastres se escalan inmediatamente tanto al Equipo de Liderazgo Ejecutivo como al Director Sénior de Ingeniería de Producción (o un oficial designado) que son responsables de evaluar el evento y confirmar el desastre. Una vez confirmado, el Comandante de Incidentes está autorizado a declarar un desastre y comenzar la activación del Equipo de Recuperación de Desastres (DRT). Debido a que los desastres pueden variar en términos de gravedad e interrupción, y también pueden ocurrir con o sin previo aviso, el DRT evaluará y analizará el impacto del desastre y actuará rápidamente para mitigar cualquier daño adicional.

Una vez que se ha declarado oficialmente un desastre, el Comandante de Incidentes es responsable de dirigir los esfuerzos de recuperación de DRT y las notificaciones en curso.

Fase de Ejecución

Las operaciones de recuperación comienzan una vez que se ha declarado el desastre, se ha activado el plan de recuperación de desastres, se ha notificado al personal correspondiente y el Equipo de recuperación de desastres (DRT) está preparado para realizar las actividades de recuperación como se describe en *Prácticas de respaldo y recuperación, Realización de la recuperación*.

Recursos Organizativos Clave

Jon Fletcher, Director Senior de Ingeniería de Producción

Equipo de Recuperación de Desastres

El Equipo de recuperación de desastres (DRT) está formado por ingenieros clave y empleados de operaciones. Las responsabilidades de la DRT incluyen:

- Establecer comunicación entre los individuos necesarios para ejecutar la recuperación.
- Determine los pasos necesarios para recuperarse completamente del desastre.
- Ejecutar los pasos de recuperación
- Verifique que la recuperación esté completa
- Informar al Comandante de incidentes de la finalización

Estrategia de Comunicación

Notificación a las partes interesadas internas

El Comandante de Incidentes es responsable de asegurarse de que el DRT y cualquier otro personal necesario sean notificados de una emergencia o desastre y movilizados.

El DRT (y otro personal operativo clave) tienen una lista de guardia programada y están disponibles las 24 horas del día, los 7 días de la semana en caso de emergencia o desastre. Utilizamos una plataforma de localización que se especializa en la respuesta a incidentes de SaaS que nos permite localizar al personal clave para comenzar la activación en cualquier momento.

Notificando a los clientes

- **Declaración de desastre:** los clientes y socios comerciales afectados serán notificados de inmediato si se declara un desastre. La notificación incluirá una descripción del evento, el efecto en el servicio y cualquier impacto potencial en los datos.

- **Actualizaciones durante la fase de ejecución:** los clientes y socios comerciales afectados se mantendrán actualizados durante todo el proceso de recuperación ante desastres por teléfono, mensajería y / o correo electrónico. También publicaremos actualizaciones de estado oficiales en status.instructure.com.

- **Finalización de la recuperación:** una vez que se complete la recuperación y se reanuden los servicios, las notificaciones de nuestros clientes incluirán información general sobre los pasos tomados para la recuperación y cualquier dato que pueda haber sido afectado. Si la recuperación es parcial y el servicio aún se encuentra en un estado degradado, las notificaciones incluirán una estimación de cuánto tiempo continuará la degradación.

Si el contacto principal para la recuperación de desastres (designado por el cliente) no está disponible, notificaremos al contacto alternativo (también designado por el cliente). Si, por cualquier motivo, no podemos comunicarnos con los contactos principales y alternativos del cliente, nos esforzaremos por ponernos en contacto con otros representantes de la organización del cliente.

Resiliencia ante desastres

Infraestructura operativa

El software de Instructure se basa en una arquitectura de múltiples niveles basada en la nube. Cada componente es redundante con supervisión activa para la detección de fallas y failover. Los diferentes niveles son:

Balanceadores de carga

Todo el tráfico web es atendido por dos balanceadores de carga en una configuración activa / pasiva. Los balanceadores de carga son responsables de dirigir el tráfico al siguiente nivel.

Servidores de aplicaciones

Los servidores de aplicaciones procesan las solicitudes entrantes de los clientes desde los balanceadores de carga. Los servidores de aplicaciones implementan toda la lógica empresarial, pero no persisten datos importantes. Los trabajos asíncronos también se ejecutan en los servidores de aplicaciones. El número de servidores de aplicaciones varía según la demanda, pero siempre habrá al menos dos en configuraciones activas / activas.

Almacenamiento en caché

Para mejorar el rendimiento del sitio web, el software de Instructure almacena de forma agresiva los datos en una capa de almacenamiento en caché. Los datos almacenados aquí son estrictamente un caché de rendimiento. Cualquier pérdida de datos que resulte de la pérdida de cualquiera de estos servidores se limitaría a una pequeña cantidad de estadísticas de visualización de páginas que pueden no haberse vaciado al almacenamiento persistente. El número de servidores de caché es variable y los datos del caché se dividirán entre todos los servidores.

Bases de datos

La mayoría de los datos estructurados (cursos, información del usuario y tareas, por ejemplo) se almacenan en una base de datos. Estos datos se reparten entre instancias según la cuenta y la demanda. Cada fragmento tiene una base de datos primaria y una secundaria, ubicadas en sitios geográficamente separados. Los datos de cada primario se replican de forma asíncrona en tiempo casi real a su correspondiente secundario. Cada primario también se respalda por completo cada 24 horas, y el respaldo se almacena en un tercer sitio geográficamente separado. La infraestructura también incluye una capa interna de proxy de base de datos para las bases de datos relacionales que permite al equipo de Operaciones realizar el mantenimiento en los servidores de bases de datos relacionales con un tiempo de inactividad mínimo.

Store de objetos de terceros

El contenido, como documentos, archivos PDF, audio y video, se almacena en un almacén de objetos escalable de terceros.

Data Centers

Los centros de datos están integrados en clústeres en varias regiones del mundo donde operamos. Todos los centros de datos están en línea y continuamente prestan servicios a nuestros clientes; no hay ningún centro de datos en nuestras instalaciones.

En caso de falla, los procesos automatizados alejan el tráfico de datos de los clientes del área afectada. Nuestras aplicaciones principales se implementan en una configuración N + 1, de modo que, en caso de falla del centro de datos, haya capacidad suficiente para permitir que el tráfico se equilibre en la carga de los sitios restantes. N en este contexto simplemente se refiere a la cantidad de capacidad necesaria para ejecutar un servicio a plena carga. N + 1 indica que se ha agregado una capa duplicada adicional para admitir fallas del servicio primario y, por lo tanto, proporcionar conmutación por error y redundancia a una capacidad equivalente.

Como líder mundial en infraestructura como servicio (IaaS), Amazon Web Services (AWS) nos brinda la flexibilidad de colocar instancias y almacenar datos en múltiples regiones geográficas, así como en múltiples zonas de disponibilidad dentro de cada región.

Cada zona de disponibilidad está diseñada como una zona de falla independiente. Esto significa que las zonas de disponibilidad están físicamente separadas dentro de una región metropolitana típica y están ubicadas en llanuras de inundación de menor riesgo (la categorización específica de la zona de inundación varía según la región).

Además de utilizar una fuente de alimentación ininterrumpida (UPS) discreta y generadores de respaldo en el sitio, cada uno de ellos se alimenta a través de diferentes redes de servicios públicos independientes para reducir aún más los puntos únicos de falla. Las zonas de disponibilidad están todas conectadas de forma redundante a AWS Global Backbone, una red troncal de clase de operador construida según los estándares de los ISP más grandes del mundo (conocidos como proveedores de tránsito de nivel 1).

Soberanía de Datos

Diseñamos nuestro uso de AWS para aprovechar múltiples regiones y zonas de disponibilidad. La distribución de aplicaciones en múltiples zonas de disponibilidad brinda la capacidad de permanecer resistente frente a la mayoría de los escenarios de falla, incluidos desastres naturales o fallas del sistema. Para la privacidad dependiente de la ubicación y el cumplimiento de los requisitos de soberanía de datos, como la Directiva de privacidad de datos de la UE, los datos no se replican entre regiones. Sin embargo, en el improbable caso de un desastre que afecte a toda la región de un cliente, todos los servicios y datos se pueden reubicar en numerosas regiones activas dentro de la infraestructura de AWS que utiliza Instructure.

Prácticas de backup y recuperación

Los datos del cliente se respaldan automáticamente tanto en tiempo real como en un horario de 24 horas en múltiples ubicaciones geográficas en la región del cliente, lo que garantiza la seguridad y confiabilidad de los datos en caso de un desastre o interrupción de cualquier escala. La base de datos se respalda de una base de datos en vivo a otra, sin carga adicional en nuestros sistemas. Los archivos estáticos se almacenan en sistemas de almacenamiento seguros y geográficamente redundantes. Las copias de seguridad de recuperación se cifran con el algoritmo AES-GCM de 256 bits y se almacenan en una ubicación separada altamente segura. El equipo de operaciones de TI recibe una alerta cuando fallan las copias de seguridad y se realiza un seguimiento de las fallas hasta su resolución. Estas copias de seguridad se conservan de acuerdo con un programa de retención definido según el producto. Consulte *Retención de copia de seguridad*.

A modo de ejemplo, nuestros procedimientos de copia de seguridad y recuperación de Canvas LMS se describen a continuación:

Realización de copia de seguridad	**Los datos se replican de forma asincrónica casi en tiempo real en un sitio remoto (supervisado, etc.).** **Las copias de seguridad nocturnas de cada base de datos se almacenan en un sitio remoto.**
Realización de recuperación	Cuando la base de datos secundaria está actualizada (caso común): Promocionar la base de datos secundaria a primaria, siguiendo los documentos de replicación Aprovisionar nueva base de datos utilizando herramientas de aprovisionamiento Establecer una nueva base de datos como nueva secundaria, siguiendo los documentos de replicación

	Cuando la secundaria tiene un retraso de> 24 horas (poco probable): Copie la copia de seguridad de anoche en la base de datos secundaria Cargue la base de datos secundaria con respaldo nocturno Aprovisionar nueva base de datos utilizando herramientas de aprovisionamiento Establecer una nueva base de datos como nueva secundaria, siguiendo los documentos de replicación

Activos estáticos como documentos y otros archivos de contenido

Realización de cópia de seguridad	**Los archivos se almacenan en un almacenamiento escalable, cifrado y geográficamente redundante (Amazon S3)**
Realización de recuperación	La recuperación en caso de fallas está integrada en el sistema de almacenamiento escalable

Web applications

Realización de cópia de seguridad	**El código fuente de la aplicación web se almacena en el control de fuente versionado y se realiza una copia de seguridad en varias ubicaciones** **No hay ningún estado almacenado en los servidores de aplicaciones que deban respaldarse**
Realización de recuperación	No aplica

Retención de copia de seguridad

Canvas

Canvas LMS

Además de la replicación en tiempo real en múltiples ubicaciones geográficas en la región del cliente, lo que garantiza un RPO increíblemente bajo, Instructure conserva copias de seguridad completas de la base de datos (también conocidas como "instantáneas") para los clientes de Canvas, por un total de 12 meses de datos de copia de seguridad continua. En concreto, conservamos:

- 7 instantáneas diarias
- 4 instantáneas semanales
- y 12 instantáneas mensuales.

Esto nos permite realizar una recuperación puntual (PITR) de hasta 4 meses de datos antiguos y realizar restauraciones mensuales de 5 a 12 meses de datos antiguos.

Los datos de objetos, como archivos, documentos y medios cargados, etc., son recuperables en caso de eliminación o modificación por un período de 1 año.

Student Pathways / Student ePortfolios

Student Pathways / Student ePortfolios están configurados para conservarse durante 35 días.

Mastery

Mastery Connect

Los procedimientos de copia de seguridad de datos se han configurado en AWS para ejecutar una instantánea de copia de seguridad completa diaria de las bases de datos de Mastery Connect. Las copias de seguridad de Mastery Connect están configuradas para conservarse de la siguiente manera:

- Instantáneas Point in Time (PITR) durante 35 días
- Instantáneas diarias durante 35 días
- Copias de seguridad mensuales de durante 1 año
- Copia de seguridad anuales durante 10 años

Impact

Si bien Impact no almacena ni procesa datos de clientes, los procedimientos de copia de seguridad se han configurado dentro de AWS para ejecutar una instantánea de copia de seguridad completa diaria de las bases de datos y la configuración del sistema Impact. Las copias de seguridad de impacto están configuradas para conservarse de la siguiente manera:

- Instantáneas diarias durante 7 días

Elevate

Elevate K-12 Analytics

Los datos de los clientes son ingeridos por Elevate K-12 Analytics para su análisis y, por lo tanto, Elevate K-12 Analytics no se considera una fuente de verdad para los datos de los clientes. Sin embargo, usamos AWS Backup para crear copias de seguridad de instancias EC2 (configuración de usuario, paneles y configuraciones, etc.) de la siguiente manera:

- Copias de seguridad diarias de AWS durante 15 días
- Copias de seguridad mensuales de AWS durante 1 año

Elevate Data Quality

Los datos del cliente son ingeridos por Elevate Data Quality para su análisis y, por lo tanto, Elevate Data Quality no se considera una fuente de verdad para los datos del cliente. Sin embargo, usamos AWS Backup para crear copias de seguridad de instancias EC2 (configuración de usuario, paneles y configuraciones, etc.) de la siguiente manera:

- Copias de seguridad mensuales de AWS (actualmente no eliminamos copias de seguridad; retención indefinida)

Elevate Data Hub

- Copias de seguridad semanales de retención a largo plazo durante 6 meses
- Copias de seguridad mensuales de retención a largo plazo durante 1 año
- Copias de seguridad anuales de retención a largo plazo; Conservar la semana 52 durante 3 años

Prueba del plan de recuperación ante desastres

Un plan de recuperación ante desastres solo es útil en la medida en que se prueba con regularidad.

El Oficial de Incidentes es responsable de garantizar que nuestro Plan de Recuperación de Desastres se revise al menos una vez al año y en parte cada vez que se cambien los componentes principales de nuestra arquitectura. Realizamos ejercicios de simulación anuales que analizan situaciones de emergencia simuladas y permiten que el DRT analice nuestros procesos y planes para gestionar tanto un incidente como las consecuencias de un desastre natural o provocado por el hombre. Por lo general, para nuestras pruebas de escritorio, nos enfocamos en los escenarios más extremos, como la pérdida de una zona de disponibilidad o una región de alojamiento. Cualquier cambio o revisión de una respuesta de DR se captura y actualiza en nuestro Plan de Recuperación de Desastres formal.

Nuestra última prueba DR de sobremesa se realizó en diciembre de 2021 y la próxima está programada para diciembre de 2022.

También probamos con frecuencia nuestra capacidad para restaurar desde una copia de seguridad como parte de nuestro ciclo de lanzamiento regular, ya que los sitios que no son de producción se llenan con copias de seguridad de producción. Por ejemplo, las instancias beta de Canvas se restauran cada semana a partir de los datos de respaldo de producción, lo que prueba nuestra capacidad de recuperación de la pérdida de datos cada semana (verificable en la propia instancia del cliente).Con frecuencia probamos nuestra capacidad para restaurar desde una copia de seguridad como parte de nuestro ciclo de lanzamiento regular, ya que los sitios que no son de producción se completan a partir de copias de seguridad de producción. Por ejemplo, las instancias beta de Canvas se restauran cada semana a partir de los datos de respaldo de producción, lo que prueba nuestra capacidad para recuperarnos de la pérdida de datos todas las semanas (verificable en la propia instancia del cliente).

Pruebas funcionales

Instructure tiene un equipo de respuesta a crisis que consta de sus equipos de Recursos Humanos, Comunicación, Legal y Seguridad para responder a situaciones de crisis y / o escenarios de desastre en las oficinas de Instructure. De forma continua, participamos en entrenamientos y ejercicios de crisis, que incluyen, por ejemplo, respuestas a tiradores activos, simulacros de incendio y otros escenarios de desastre.

Ejemplos de escenarios de desastre

A continuación, describimos varios posibles escenarios de desastre, los servicios afectados, las estrategias de recuperación y el objetivo de punto de recuperación (RPO)/objetivo de tiempo de recuperación (RTO), los servicios afectados y la descripción general de la recuperación. Tenga en cuenta que estos solo pretenden transmitir la magnitud del impacto y los esfuerzos de recuperación necesarios en diferentes situaciones. La probabilidad es una probabilidad estimada de que ocurra el escenario, pero no garantiza que ocurra; su presencia no pretende transmitir probabilidad, sino simplemente indicar probabilidad y describir la improbabilidad de algunos de los escenarios más

extremos. Último incidente se refiere a la última vez que nos encontramos con este escenario de recuperación ante desastres en un entorno real.

Pérdida completa de una base de datos primaria

Servicios afectados	**La mayoría de las cuentas alojadas en la base de datos afectada**
Visión general de la recuperación	Cuando la base de datos secundaria está actualizada (caso común): se promueve la secundaria para que sea la nueva primaria de acuerdo con los pasos descritos anteriormente Cuando la base de datos secundaria es inconsistente: la secundaria se rellena con la última instantánea nocturna y se pone en línea como la nueva primaria.
RPO:	5 minutos (secundaria consistente, caso común), 24 horas (secundaria inconsistente)
RTO:	1 hora (secundaria consistente, caso común), 6 horas (secundaria inconsistente)
Probabilidad:	Improbable (una vez cada 5 años o más)
Ultimo incidente	Nunca

Pérdida completa simultánea de bases de datos primarias y secundarias

Servicios afectados	**La mayoría de las cuentas alojadas en la base de datos afectada**
Visión general de la recuperación	Las nuevas bases de datos primarias y secundarias se ponen en línea en ubicaciones separadas La base de datos primaria se llena con datos de la copia de seguridad externa Los servidores de aplicaciones apuntaron a una nueva base de datos primaria Replicación restablecida con la nueva base de datos secundaria
RPO:	24 horas

RTO:	6 horas
Probabilidad	Raro (una vez cada 20 años; las bases de datos primaria y secundaria se alojan en ubicaciones geográficamente separadas, lo que hace que la falla simultánea sea muy improbable)
Ultimo incidente	Nunca

Destrucción de la base de datos por violación de la seguridad

Servicios afectados	La mayoría de las cuentas alojadas en la base de datos afectada.
Visión general de la recuperación	La base de datos primaria se restaura a partir de la copia de seguridad completa más reciente. La replicación se restablece con la base de datos secundaria
RPO:	24 horas
RTO:	6 horas
Probabilidad:	Muy improbable (una vez cada 10 años o más)
Ultimo incidente	Nunca

Pérdida completa de instalaciones de alojamiento primario

Servicios afectados	Plataforma para la mayoría de las cuentas
Visión general de la recuperación	Los nuevos load balancers y servidores de aplicaciones se muestran en el sitio secundario con la base de datos secundaria La base de datos secundaria anterior se promueve a base de datos primaria. Se presenta una nueva base de datos secundaria en un tercer sitio y se restablece la replicación DNS apunta a los nuevos load balancers en el sitio de recuperación y se restauran los servicios
RPO:	4 horas
RTO:	Comercialmente razonable
Probabilidad:	Extremadamente improbable (una vez cada 100 años o más)

Ultimo incidente	Nunca

Conclusión

Vivimos en un mundo impredecible. Los desastres son, en muchos sentidos, inevitables, y reconocemos, a pesar de diseñar nuestros productos para una alta disponibilidad y conmutación por error, que no sería prudente asumir que nuestro negocio es inmune a los desastres. Como proveedor líder de software educativo como servicio (SaaS), reconocemos que el activo no humano más preciado que nos confía son los datos. Es por eso que hemos realizado una cuidadosa planificación y preparación para crear un Plan de Recuperación ante Desastres (DRP) sólido como se describe en este documento, que esperamos infunda confianza y seguridad de que, en el evento inesperado que encontremos un desastre, estamos preparados, capaces, y listo para lanzar esfuerzos de recuperación para restaurar nuestros servicios lo más rápido posible y minimizar las pérdidas o interrupciones para nuestros clientes.

Nuestro enfoque de la planificación de la continuidad del negocio es que es una parte viva y respirable de nuestra organización que evoluciona a medida que cambiamos y crecemos con nuestros clientes. Hemos aprendido de la pandemia global de COVID-19 que la continuidad del negocio no es una ficción o simplemente un documento requerido para marcar una casilla en el curso de la actividad comercial, sino que, por el contrario, es vital para sobrevivir (y prosperar) a través de desastres, amenazas y desafíos Durante los últimos dos años de la pandemia, nuestros empleados no solo tuvieron que adaptarse a trabajar desde casa y vivir una nueva normalidad durante muchos meses de interrupción del negocio como de costumbre, sino que, al mismo tiempo, tuvieron que trabajar como un equipo unido. como nunca antes y proporcionar esfuerzos monumentales para mantener nuestros servicios funcionando con normalidad cuando miles y miles de estudiantes se vieron obligados a migrar al aprendizaje en línea. Gracias a nuestra planificación de continuidad comercial, cuando nuestros clientes necesitaban nuestros servicios más que nunca para brindar alta disponibilidad y rendimiento durante la pandemia global y los tiempos estresantes, cumplimos.

En Instructure, nos acercamos de manera proactiva a la continuidad del negocio mediante la creación de resiliencia en nuestros procesos clave, el uso de la tecnología y la contratación y retención de personal clave. Cuando incidentes imprevistos impactan o interrumpen nuestro negocio, sepa que estamos listos para actuar, con planes sólidos para recuperarnos rápidamente y garantizar la continuación de nuestro negocio y el suyo durante y después de cualquier incidente crítico que provoque la interrupción de nuestra capacidad operativa normal.