INSTRUCTURE

CONTINUIDADE DOS NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

Engenharia, Segurança e Operações

Agosto 2024

Índice

INSTRUCTURE

INSTRUCTURE

Continuidade dos negócios

Cada organização está sujeita a uma variedade de riscos durante a condução dos negócios. Esses riscos podem assumir a forma de ameaças externas sérias, como terrorismo cibernético ou convulsão política para os riscos menos graves (mas ainda importantes) de reter pessoal-chave ou mesmo ter que enfrentar um panda furioso. Mas seja qual for o risco percebido, é fundamental que uma organização identifique, avalie e mantenha um Plano de Continuidade de Negócios (PCN) para prevenir e se recuperar de ameaças potenciais ou reais aos seus ativos mais valiosos. Na Instructure, nossos processos robustos de gestão de risco nos permitem identificar, avaliar e tratar esses riscos de forma contínua. Para ajudar a fortalecer nosso Plano de Continuidade de Negócios, nosso Comitê Gestor de Riscos Corporativos, composto por líderes-chave em toda a Instructure, se reúne regular e continuamente para identificar e mitigar riscos que podem impactar a Instructure, sua missão e seus ativos mais valiosos.

Naturalmente, no centro de cada programa de continuidade de negócios está um plano robusto de resposta a incidentes - um plano que ajuda a guiar com eficácia uma organização através de incidentes que podem surgir de tempos em tempos. Na Instructure, temos um plano detalhado, considerado e operacional de resposta a incidentes que inclui a preparação, detecção, avaliação, escalonamento, resposta, comunicação dos impactos e aprendizado com segurança, disponibilidade, privacidade, recursos humanos, finanças e outros incidentes imprevistos (leia-se: panda zangado). O plano de resposta a incidentes é o ponto de partida para todos os incidentes e pode facilmente escalar - dependendo do tipo e da gravidade do incidente - em uma variedade de outros planos existentes na Instructure, incluindo planos de recuperação de desastres, planos de continuidade de negócios, planos de gerenciamento de crises, planos de evacuação, planos de pandemia e outros planos estratégicos para ajudar na recuperação eficaz e eficiente de nossas operações comerciais.

Um dos riscos que afetam todas as organizações é a capacidade de manter as operações de negócios em andamento, identificando, avaliando e reduzindo as ameaças que podem impactar as operações de negócios. Isso ficou claramente evidente em 2020, um ano que nos testou como nenhum outro que tínhamos visto antes. A pandemia global COVID-19 mostrou-nos claramente - e a todos - quão crucial é um plano de continuidade de negócios em tempos incertos. A mudança e reviravolta que vimos em 2020 provavelmente ecoará por muitos anos, tanto em termos de tendências educacionais quanto nas mudanças na forma como vemos o trabalho e talvez de onde trabalhamos. O objetivo deste documento é estabelecer como abordamos a continuidade dos negócios aqui na Instructure como parte de nosso programa de gerenciamento de risco contínuo, enquanto continuamos nossa missão de ser a plataforma de gerenciamento de aprendizagem líder do setor.

Recuperação de Desastres

Também incluídos como parte de nosso plano de continuidade de negócios estão nossos planos e procedimentos de recuperação de desastres. Nenhuma empresa deseja um desastre, seja a perda catastrófica de um datacenter ou um panda louco correndo pelo escritório puxando cabos. Mas se ou quando chegar a hora, ter um plano de recuperação de desastre robusto em vigor nos permitirá restaurar nossos serviços o mais rápido possível e minimizar perdas ou interrupções para nossos clientes e nossas operações internas.

Incluído neste documento está uma visão geral do plano de recuperação de desastres e dos procedimentos que a Instructure estabeleceu para se recuperar de desastres que afetam suas operações de produção. Descrevemos como nossa oferta de Software como Serviço (SaaS) foi arquitetada para se recuperar de cenários de desastre, as etapas que tomaremos se um desastre for declarado, nossas políticas, estratégias de comunicação e procedimentos de notificação ao cliente e vários cenários de exemplo e avaliações de impacto.

Desenvolvendo Resiliência e Mantendo Planos de Recuperação Efetivos

A abordagem da Instructure à continuidade dos negócios está construindo resiliência em seus processos, tecnologia e pessoas. Este documento descreve as diferentes práticas que a Instructure usa para garantir a resiliência dos negócios por meio das principais funções de negócios, garantindo a sincronização entre o uso de tecnologia e aplicativos, provedores de serviços de infraestrutura de nuvem e pessoal. Essa abordagem é baseada nas melhores práticas do setor para SaaS para mitigar o tempo de inatividade causado por interrupção comum de vetores de serviço para empresas de SaaS, incluindo, mas não limitado a, ataques cibernéticos, violações de segurança física, dependências de fornecedores, fraudes e distúrbios civis, pandemias e desastres naturais ou causados pelo homem.

As práticas adotadas pela Instructure aumentam a capacidade de recuperar-se de uma interrupção no serviço e proteger os dados de seus clientes e de seu pessoal. Essas práticas envolvem processos para práticas preventivas e de recuperação que visam atingir os seguintes objetivos:

- Fornecer serviço contínuo aos clientes
- Reduzir o risco para operações de negócios principais
- Manter comunicação clara com clientes e funcionários

Processos

A Instructure projetou e opera os seguintes processos-chave para apoiar as operações comerciais contínuas (e efetivas de recuperação de incidentes que afetam) da Instructure:

- **Plano de resposta a incidentes -** A Instructure desenvolveu, mantém e opera planos abrangentes de resposta a incidentes. Esses planos incluem definições de preparação, detecção, avaliação da criticidade do incidente, escalonamento, ações de contenção a serem tomadas com base na criticidade do incidente, métodos de comunicação, testes e manuais - ou exemplos do que fazer diante de determinados incidentes e melhorias.

- **Planos de backup e recovery** - A Instructure desenvolveu, mantém e opera planos robustos de backup e recuperação de desastres. Esses planos incluem backups diários e replicação de dados quase em tempo real para um local separado e geograficamente isolado na região do cliente. Como a Instructure usa o líder mundial em infraestrutura como serviço (IaaS), Amazon Web Services (AWS) para hospedar dados na região geográfica do cliente, cada região tem vários locais isolados, conhecidos como zonas de disponibilidade, onde os dados do cliente são replicados para fins de recuperação de desastres . O uso de várias zonas de disponibilidade da AWS é para garantir que, se houver uma falha em um local físico, os dados estejam prontamente disponíveis em outro local geograficamente separado. Backups e objetos enviados pelo cliente são armazenados no Amazon S3, que apresenta 99,999999999% de tempo de atividade e confiabilidade em um determinado ano. Os backups são verificados quanto à integridade e testados pelo menos uma vez por mês.

- **Avaliações de fornecedores -** A Instructure opera um robusto programa de gerenciamento de riscos à segurança de terceiros. Essas práticas incluem o gerenciamento de um inventário preciso dos fornecedores, a realização de avaliações de risco e a revisão das práticas críticas de segurança e disponibilidade dos fornecedores. Essas análises incluem a garantia de que os fornecedores tenham práticas robustas para backup, recuperação de desastres e planos de continuidade de negócios. Além disso, a Instructure também garante que os Contratos de Nível de Serviço com fornecedores contenham uma descrição dos serviços prestados e informações sobre a disponibilidade de rede prometida.

- **Seguro cibernético -** A Instructure garante que protege seus negócios contra grandes despesas, perdas e multas e multas regulatórias, caso ocorra uma violação de dados por meio de cobertura de seguro cibernético.

- **Teste de recovery anual -** A Instructure testa seus planos de recovery pelo menos uma vez por ano usando dois métodos: cenários ao vivo e testes de mesa. Os cenários incluem eventos em que ocorrem interrupções de serviço e o pessoal incluído nos testes de mesa é responsável por determinar as ações usadas para recuperar os serviços.

- **Gerenciamento de risco -** A Instructure reconhece o gerenciamento de riscos como um componente crítico de suas operações que ajuda a verificar se os ativos do cliente estão adequadamente protegidos e incorpora o gerenciamento de riscos em todos os seus processos.

- **Planejamento estratégico -** A Instructure possui um plano estratégico geral que é apresentado ao conselho de administração. Esse plano é separado em planos de segmentos específicos projetados para operacionalizar o que é esperado dos segmentos, a fim de apoiar os objetivos gerais da Instructure.

- **Canais de Comunicação -** A Instructure possui processos para responder a incidentes e informar todo o seu pessoal em caso de uma interrupção ou evento do serviço que precise ser comunicado ao seu pessoal. Em geral, os clientes serão notificados principalmente por seu respectivo Customer Success Manager (CSM), que é o principal ponto de contato com todos os clientes. Os CSMs usarão os métodos preferidos de comunicação identificados pelo cliente. No caso de uma interrupção amplamente impactante, as notificações também serão fornecidas usando um site público mais amplamente disponível, com os detalhes mais recentes. Para comunicações internas, a Instructure identificou um meio primário e um meio secundário de comunicação durante um evento impactante, a fim de manter os esforços de recuperação eficazes durante um incidente.

- **Treinamento de crise -** A Instructure possui uma equipe de resposta a crises composta por equipes de Recursos Humanos, Comunicação, Jurídico e Segurança para responder a situações de crise nos escritórios da Instructure. Além disso, a Instructure se envolve em treinamentos e exercícios de crise, que incluem, por exemplo, respostas a atiradores ativos e exercícios de incêndio.

Propriedade

O Chief Information Security Officer (CISO) da Instructure é responsável por supervisionar a continuidade dos negócios em coordenação com o Vice-Presidente Sênior (SVP) de Engenharia. Também temos uma equipe definida de recuperação de desastres com escalação final para o vice-presidente sênior de engenharia. Do lado comercial, todos os desastres potenciais são encaminhados

imediatamente ao Diretor Financeiro, que é o responsável final por avaliar o evento e direcionar as notificações.

Local de Recuperação Alternativo

O pessoal da Instructure tem a capacidade de trabalhar em casa no caso de uma interrupção que afete a capacidade de trabalhar em um dos escritórios da Instructure. Para garantir que essa prática seja eficaz, a Instructure garante que haja políticas de teletrabalho em vigor e comunicadas a todo o pessoal, práticas de segurança para acessar redes corporativas e serviços de notificação de comunicação em massa em vigor. Vários provedores são usados para fornecer conectividade aos escritórios da Instructure - permitindo a rápida retomada da conectividade se um provedor for considerado incapaz de fornecer o nível de serviço necessário para manter a conectividade consistente e contínua. Como parte do teste anual de continuidade de negócios da Instructure, os casos de uso podem incluir eventos que afetam funcionários remotos, escritórios da Instructure e procedimentos de comunicação.

Treinamento

A Instructure possui uma equipe de resposta a crises composta por suas equipes de Recursos Humanos, Comunicação, Jurídico e Segurança para responder a situações de crise nos escritórios da Instructure. Além disso, a Instructure se envolve em treinamento e exercícios de crise, incluindo simulações de incêndio e evacuações de emergência.

Código-fonte aberto

O compromisso da Instructure com o código aberto comercial fornece outra camada de garantia aos clientes em termos de continuidade de negócios. O Canvas Learning Management System está disponível como código-fonte aberto, o que significa que o código do Canvas é gratuito, público e totalmente aberto em todos os momentos*. Qualquer pessoa pode usar o código Canvas LMS sem custo adicional. A Instructure atualiza o código do Canvas LMS regularmente, e o código é mantido no Github: https://github.com/instructure/canvas-lms/wiki.

No caso improvável de quaisquer alterações materiais nas operações normais de negócios da Instructure, nossos clientes têm acesso ao código-fonte aberto do Canvas LMS para permitir a continuidade dos negócios. Isso permitiria às instituições hospedar, operar e oferecer suporte ao código-fonte aberto do Canvas LMS em seus próprios servidores, caso a Instructure não pudesse mais fazê-lo. Além do nosso código-fonte aberto, o Canvas LMS também oferece exportação de conteúdo,

acesso aberto à API RESTful e dados do Canvas LMS. Isso significa que as instituições sempre terão acesso ao conteúdo e aos dados do curso.

*exclui alguns plugins e extensões que atualmente não são de código aberto

Recuperação de Desastres

Termos-chave e suposições

No espaço Software as a Service (SaaS), existem alguns termos-chave em relação à recuperação de desastres.

1) No contexto de um cenário de recuperação de desastre, dois termos são comumente usados para descrever como um processo de recuperação pode ser afetado: **Objetivo de tempo de recuperação (RTO)** e **Objetivo de Ponto de Recuperação (RPO)**. O RTO representa quanto tempo levará para restaurar o acesso aos dados e o RPO quantos dados estão em risco de serem perdidos. Por exemplo, se levar 8 horas para um serviço ser recuperado, o RTO é de 8 horas. Se as últimas 4 horas de dados forem potencialmente perdidas devido a um desastre, o RPO será de 4 horas.

2) Embora **"Recuperação de desastres"** e "**Alta disponibilidade"** sejam conceitos compartilhados em relação à continuidade dos negócios, eles impactam o planejamento de recuperação de desastres de forma diferente. A recuperação de desastres basicamente infere que haverá alguma forma de tempo de inatividade envolvido, medido em horas ou dias. Alta disponibilidade, no entanto, significa garantir a continuidade contínua das operações em um cenário de recuperação de desastre, especialmente por meio do projeto de redundâncias arquitetônicas, como failover automatizado de componentes.

Nossos serviços são projetados para alcançar RPO e RTO excepcionalmente baixos nos cenários mais comuns e alta disponibilidade para nossos clientes devido à natureza distribuída e resiliente de nossa infraestrutura. Para a grande maioria dos cenários de falha, a necessidade de failover para outra zona de disponibilidade (AZ) é evitada e os impactos em nossos serviços serão mínimos.

A suposição principal de nosso plano de recuperação de desastres é que ele trata apenas de eventos que afetariam um datacenter inteiro ou nossa arquitetura como um todo. As falhas de componentes individuais serão recuperadas por meio de redundâncias arquitetônicas robustas e mecanismos de failover.

Recuperação de desastres em um mundo SaaS

O software educacional da Instructure (e dados associados) é hospedado na nuvem pela Instructure e fornecido pela Internet por meio do provedor de nuvem pública mais confiável do mundo, Amazon Web Services (AWS). Este modelo de entrega de Software como Serviço (SaaS) significa que nossos

clientes não precisam se preocupar com a manutenção de hardware ou software de servidor, patches, service packs ou, no contexto deste documento, recuperação de desastres.

Não apenas mantemos nossos próprios planos e procedimentos robustos de recuperação de desastres, mas também nos beneficiamos do uso da AWS, uma infraestrutura como serviço (IaaS) líder mundial que cria redundância em seus serviços, fornecendo várias regiões, zonas de disponibilidade e data centers que nos permitem uma recuperação rápida no caso de um desastre imprevisto.

Dada a natureza do modelo de entrega SaaS, a Instructure é responsável por fornecer recuperação de desastres em relação ao nosso software e dados associados. Naturalmente, as melhores práticas também exigem que nossos clientes desenvolvam e mantenham seus próprios planos e procedimentos de recuperação de desastres.

Definição de Desastre

Um desastre é definido como qualquer evento perturbador que tenha efeitos adversos potencialmente de longo prazo no serviço Instructure. Em geral, os possíveis eventos de desastre serão abordados com a mais alta prioridade em todos os níveis no Instructure. Tais eventos podem ser intencionais ou não intencionais, como segue:

- **Desastres naturais:** tornado, terremoto, furacão, fogo, deslizamento de terra, inundação, tempestade elétrica e tsunami.
- **Sistemas de suprimento:** falhas de utilidades, como linhas de gás ou água cortadas, falhas na linha de comunicação, queda / queda de energia elétrica e escassez de energia.
- **Feito pelo homem / político:** Terrorismo, roubo, trabalhador descontente, incêndio criminoso, greve trabalhista, sabotagem, motins, vandalismo, vírus e ataques de hackers.

Procedimentos de recuperação de desastres

Fase de Monitoramento de Desastres

A Instructure monitora o desempenho de nossos serviços 24 horas por dia, usando ferramentas externas de monitoramento de desempenho e ferramentas internas de monitoramento de código aberto e fechado. Essas ferramentas são configuradas para enviar alertas em tempo real para o nosso pessoal quando certos eventos ocorrerem que justifiquem a investigação de um potencial cenário de desastre iminente.

Fase de Ativação

Todos os potenciais desastres são escalados imediatamente para a Equipe de Liderança Executiva e o Diretor Sênior de Engenharia de Produção (ou um oficial designado) que são responsáveis por avaliar o evento e confirmar o desastre. Uma vez confirmado, o Comandante do Incidente está autorizado a declarar um desastre e iniciar a ativação da Equipe de Recuperação de Desastres (DRT). Como os desastres podem variar em termos de gravidade e interrupção, e também podem ocorrer com ou sem aviso prévio, o DRT avaliará e analisará o impacto do desastre e agirá rapidamente para mitigar qualquer dano adicional.

Uma vez que um desastre tenha sido oficialmente declarado, o Comandante do Incidente é responsável por direcionar os esforços de recuperação do DRT e fazer notificações contínuas.

Fase de Execução

As operações de recuperação começam assim que o desastre é declarado, o plano de recuperação de desastre ativado, a equipe relevante notificada e a Equipe de Recuperação de Desastres (DRT) preparada para realizar as atividades de recuperação, conforme descrito em *Práticas de Backup e Recuperação, Executando a Recuperação.*

Recursos Organizacionais Chave
Incident Commander

Jon Fletcher, Diretor Sênior de Engenharia de Produção.

Equipe de Recuperação de Desastres

A equipe de recuperação de desastres (DRT) é formada por engenheiros e funcionários de operações. As responsabilidades do DRT incluem:

- Estabelecer comunicação entre os indivíduos necessários para executar a recuperação
- Determine as etapas necessárias para recuperar completamente do desastre
- Execute as etapas de recuperação
- Verifique se a recuperação está completa
- Informe o Comandante de incidente de conclusão

Communication Strategy
Notifying Internal Stakeholders

The Incident Commander is responsible for making sure the DRT and any other necessary staff are notified of an emergency or disaster and mobilized.

The DRT (and other key operational staff) have a scheduled on-call roster and are contactable 24x7 in an emergency or disaster. We use a paging platform that specializes in SaaS incident response which allows us to page key staff to commence activation at a moment's notice.

Notificando os clientes

- **Declaração de desastre:** Os clientes e parceiros de negócios afetados serão notificados imediatamente se um desastre for declarado. A notificação incluirá uma descrição do evento, o efeito no serviço e qualquer impacto potencial nos dados.

- **Atualizações durante a fase de execução:** Os clientes e parceiros de negócios afetados serão mantidos atualizados durante todo o processo de recuperação de desastres por telefone, mensagem e / ou e-mail. Também postaremos atualizações de status oficiais em status.instructure.com.

- **Conclusão da recuperação:** Assim que a recuperação for concluída e os serviços retomados, nossas notificações ao cliente incluirão informações gerais sobre as etapas executadas para a recuperação e quaisquer dados que possam ter sido afetados. Se a recuperação for parcial e o serviço ainda estiver em um estado degradado, as notificações incluirão uma estimativa de quanto tempo a degradação continuará.

Se o (s) contato (s) principal (is) para recuperação de desastre (indicado pelo cliente) não estiverem disponíveis, notificaremos o contato alternativo (também indicado pelo cliente). Se, por qualquer motivo, não formos capazes de entrar em contato com os contatos principais e alternativos do cliente, faremos o possível para entrar em contato com outros representantes da organização do cliente

Resiliência a Desastres
Infraestrutura Operacional

O software da Instructure é baseado em uma arquitetura baseada em nuvem de várias camadas. Cada componente é redundante com monitoramento ativo para detecção de falhas e failover. Os diferentes níveis são:

Balanceadores de carga

Todo o tráfego da Web é atendido por dois balanceadores de carga em uma configuração ativa / passiva. Os balanceadores de carga são responsáveis por direcionar o tráfego para o próximo nível.

Servidores de aplicativos

Os servidores de aplicaçãp processam solicitações de entrada de clientes dos balanceadores de carga. Os servidores de aplicaçãp implementam toda a lógica de negócios, mas não persistem dados importantes. As tarefas assíncronas também são executadas nos servidores de aplicativos. O número de servidores de aplicativos varia de acordo com a demanda, mas sempre haverá pelo menos dois em configurações ativas / ativas.

Cache

Para melhorar o desempenho do site, o software da Instructure armazena dados de forma agressiva em uma camada de armazenamento em cache. Os dados armazenados aqui são estritamente um cache de desempenho. Qualquer perda de dados resultante da perda de qualquer um desses servidores será limitada a um pequeno número de estatísticas de exibição de página que podem não ter sido liberadas para armazenamento persistente. O número de servidores de cache é variável e os dados de cache serão particionados entre todos os servidores.

Bancos de dados

A maioria dos dados estruturados - cursos, informações do usuário e tarefas, por exemplo - são armazenados em um banco de dados. Esses dados são agrupados entre instâncias com base na conta e na demanda. Cada shard possui um banco de dados primário e um secundário, localizados em sites geograficamente separados. Os dados de cada primário são replicados de forma assíncrona quase em tempo real para o secundário correspondente. Cada backup do primário também é feito completamente a cada 24 horas, e o backup é armazenado em um terceiro site geograficamente separado. A infraestrutura também inclui uma camada de proxy de banco de dados interno para os bancos de dados relacionais, que permite à equipe de Operações realizar manutenção nos servidores de banco de dados relacionais com tempo de inatividade mínimo.

Store de objetos de terceiros

O conteúdo, como documentos, PDFs, áudio e vídeo, é armazenado em um armazenamento de objetos escalável de terceiros.

Data Centers

Os data centers são construídos em clusters em várias regiões globais onde operamos. Todos os data centers estão online e atendendo continuamente nossos clientes; nenhum data center está em nossas dependências.

Em caso de falha, os processos automatizados movem o tráfego de dados do cliente para longe da área afetada. Nossos principais aplicativos são implantados em uma configuração N + 1, de forma que, em caso de falha do data center, haja capacidade suficiente para permitir o balanceamento de carga do tráfego para os demais sites. N, neste contexto, simplesmente se refere à quantidade de capacidade necessária para executar um serviço em plena carga. N + 1 indica que uma camada duplicada adicional foi adicionada para dar suporte à falha do serviço principal e, portanto, fornecer failover e redundância com capacidade equivalente.

Como líder mundial em infraestrutura como serviço (IaaS), Amazon Web Services (AWS) nos fornece a flexibilidade de colocar instâncias e armazenar dados em várias regiões geográficas, bem como em várias zonas de disponibilidade em cada região.

Cada zona de disponibilidade é projetada como uma zona de falha independente. Isso significa que as zonas de disponibilidade são fisicamente separadas dentro de uma região metropolitana típica e estão localizadas em planícies de inundação de baixo risco (a categorização específica da zona de inundação varia por região).

Além de utilizar fonte de alimentação ininterrupta (UPS) discreta e geradores de backup no local, cada um deles é alimentado por redes diferentes de utilitários independentes para reduzir ainda mais os pontos únicos de falha. As zonas de disponibilidade são todas redundantemente conectadas ao AWS Global Backbone, um backbone de classe de operadora construído de acordo com os padrões dos maiores ISPs do mundo (conhecidos como provedores de trânsito Tier 1).

Soberania de Dados

Arquitetamos nosso uso da AWS para aproveitar várias regiões e zonas de disponibilidade (AZ). A distribuição de aplicativos em várias zonas de disponibilidade fornece a capacidade de permanecer resiliente diante da maioria dos cenários de falha, incluindo desastres naturais ou falhas do sistema. Para privacidade dependente de localização e conformidade com requisitos de soberania de dados, como a Diretiva de Privacidade de Dados da UE, os dados não são replicados entre as regiões. No entanto, no caso improvável de um desastre que afete toda a região do cliente, nossos serviços podem ser realocados para várias regiões ativas dentro da infraestrutura da AWS que a Instructure usa.

Práticas de backup e recuperação

Os dados do cliente são copiados automaticamente em tempo real e em uma programação de 24 horas para várias localizações geográficas na região do cliente, garantindo a segurança e a confiabilidade dos dados em caso de desastre ou interrupção de qualquer escala. O backup do banco de dados é feito de um banco de dados ativo para outro, sem carga adicional em nossos sistemas. Os arquivos estáticos são armazenados em sistemas de armazenamento seguros e geograficamente redundantes. Os backups de recuperação são criptografados usando o algoritmo AES-GCM de 256 bits e armazenados em um local separado altamente seguro. A equipe de operações de TI é alertada quando os backups falham e quaisquer falhas são rastreadas até a resolução. Esses backups são retidos de acordo com um cronograma de retenção definido de acordo com o produto. Consulte *Retenção de backup*.

Como exemplo, nossos procedimentos de backup e recuperação do Canvas LMS estão descritos abaixo:

Dados do cliente de bancos de dados de produção

Executando Backup	**Os dados são replicados de forma assíncrona em tempo quase real para o site remoto (monitorado, etc.).** **Backups noturnos de cada banco de dados são armazenados em um local remoto.**
Executando Recuperação	Quando o banco de dados secundário está atualizado (caso comum): Promova o banco de dados secundário a primário, seguindo os documentos de replicação Provisione um novo banco de dados usando ferramentas de provisionamento Estabelecer novo banco de dados como novo secundário, seguindo os documentos de replicação Quando o secundário está> 24 horas atrasado (improvável):

	Copie o backup da última noite para o banco de dados secundário Carregar banco de dados secundário com backup noturno Provisione um novo banco de dados usando ferramentas de provisionamento Estabelecer novo banco de dados como novo secundário, seguindo os documentos de replicação

Ativos estáticos, como documentos e outros arquivos de conteúdo

Executando Backup	**Os arquivos são armazenados em um armazenamento escalonável, criptografado e geograficamente redundante (Amazon S3)**
Executando Recuperação	A recuperação em caso de falhas é integrada ao sistema de armazenamento escalonável

Web applications

Executando Backup	**O código-fonte do aplicativo da Web é armazenado no controle de origem com versão e com backup em vários locais** **Não há estado armazenado nos servidores de aplicativos que precisem de backup**
Executando Recuperação	Não aplicável

Retenção de Backup

Canvas

Canvas LMS

Além da replicação em tempo real para várias localizações geográficas na região do cliente, garantindo um RPO incrivelmente baixo, a Instructure mantém backups completos de banco de dados (também conhecidos como "snapshots") para clientes Canvas, totalizando 12 meses de dados de backup contínuo. Especificamente, retemos:

- 7 snapshots diários
- 4 snapshot semanais
- e, 12 x snapshot mensais.

Isso nos permite realizar a recuperação pontual (PITR - Point-In-Time-Recovery) para até 4 meses de dados antigos e realizar restaurações mensais para 5 a 12 meses de dados antigos.

Dados de objetos, como arquivos, documentos e mídia carregada, etc., são recuperáveis em caso de exclusão ou modificação por um período de 1 ano.

Student Pathways / Student ePortfolios

Os dados dos Student Pathways / Student ePortfolios são configurados para serem retidos por 35 dias.

Mastery

Mastery Connect

Os procedimentos de backup de dados foram configurados na AWS para executar um snapshot de backup completo diário dos bancos de dados Mastery Connect. Os backups do Mastery Connect são configurados para serem retidos da seguinte forma:

- Snapshots Point In Time (PITR) por 35 dias
- Snapshots diários por 35 dias

- Backups mensais por 1 ano
- Backup anual por 10 anos

Impact

Embora o Impact não armazene ou processe dados do cliente, os procedimentos de backup foram configurados na AWS para executar um snapshot de backup completo diário dos bancos de dados e configuração do sistema Impact. Os backups do Impact são configurados para serem retidos da seguinte forma:

- Snapshots diários por 7 dias

Elevate

Elevate K-12 Analytics

Os dados do cliente são ingeridos pelo Elevate K-12 Analytics para análise e, portanto, o Elevate K-12 Analytics não é considerado uma fonte de verdade para os dados do cliente. No entanto, usamos o AWS Backup para criar backups de instâncias do EC2 (configuração do usuário, painéis e configurações etc.) da seguinte forma:

- Backups diários da AWS por 15 dias
- Backups mensais da AWS por 1 ano

Elevate Data Quality

Os dados do cliente são ingeridos pelo Elevate Data Quality para análise e, portanto, o Elevate Data Quality não é considerado uma fonte de verdade para os dados do cliente. No entanto, usamos o AWS Backup para criar backups de instâncias do EC2 (configuração do usuário, painéis e configurações etc.) da seguinte forma:

- Backups mensais da AWS (atualmente não excluímos backups; retenção indefinida)

- Backups semanais de retenção de longo prazo por 6 meses
- Backups mensais de retenção de longo prazo por 1 ano
- Backups anuais de retenção de longo prazo; Mantém a Semana 52 por 3 anos

Teste de plano de recuperação de desastres

Um Plano de Recuperação de Desastres só é útil se for testado regularmente.

O Oficial de Incidentes é responsável por garantir que nosso Plano de Recuperação de Desastres seja revisado pelo menos anualmente e em parte sempre que os principais componentes de nossa arquitetura forem alterados. Realizamos exercícios de mesa anuais que discutem situações de emergência simuladas e permitem que a DRT discuta nossos processos e planos para gerenciar um incidente e as consequências de um desastre natural ou causado pelo homem. Normalmente, para nossos testes de mesa, focamos nos cenários mais extremos, como a perda de uma zona de disponibilidade e/ou região de hospedagem. Quaisquer alterações ou revisões de uma resposta de DR são capturadas e atualizadas em nosso plano formal de recuperação de desastres.

Nossos testes de DR de mesa são realizados anualmente e uma carta de atestado está disponível mediante solicitação.

Também testamos com frequência nossa capacidade de restaurar a partir do backup como parte de nosso ciclo de lançamento regular, pois os sites de não produção são preenchidos a partir de backups de produção. Por exemplo, as instâncias beta do Canvas são restauradas a cada semana a partir de dados de backup de produção, testando assim nossa capacidade de recuperar da perda de dados a cada semana (verificável na própria instância de um cliente).

Teste funcional

A Instructure tem uma equipe de resposta a crises que consiste nas equipes de Recursos Humanos, Comunicação, Jurídico e Segurança para responder a situações de crise e / ou cenários de desastre nos escritórios da Instructure. Em uma base contínua, nos envolvemos em treinamento e exercícios de crise, que incluem, por exemplo, respostas a atiradores ativos, simulações de incêndio e outros cenários de desastre.

Exemplos de Cenários de Desastres

Descrevemos abaixo vários cenários de desastres possíveis, os serviços afetados, as estratégias de recuperação e o Objetivo do Ponto de Recuperação (RPO)/Objetivo do Tempo de Recuperação (RTO), e visão geral da recuperação. Observe que eles se destinam apenas a transmitir a magnitude do impacto e os esforços de recuperação necessários em diferentes situações. A probabilidade é uma chance estimada do cenário ocorrer, mas não garante a ocorrência - sua presença não se destina a

transmitir probabilidade, mas apenas indicar chance e descrever a improbabilidade de alguns dos cenários mais extremos. Último Incidente refere-se à última vez que encontramos esse cenário de recuperação de desastres em um ambiente ativo.

Perda completa de um banco de dados primário

Serviços Afetados	A maioria das contas hospedadas no banco de dados afetado
Visão Geral da Recuperação	Quando o banco de dados secundário está atualizado (caso comum): O secundário é promovido para ser o novo primário de acordo com as etapas descritas acima Quando o banco de dados secundário é inconsistente: O secundário é preenchido com o último instantâneo noturno e colocado online como o novo primário.
RPO:	5 minutos (secundário consistente, caso comum), 24 horas (secundário inconsistente)
RTO:	1 hora (secundário consistente, caso comum), 6 horas (secundário inconsistente)
Probabilidade:	Improvável (uma vez a cada 5+ anos)
Último Incidente	Nunca

Perda completa simultânea de bancos de dados primários e secundários

Serviços Afetados	A maioria das contas hospedadas no banco de dados afetado.
Visão Geral da Recuperação	Novos bancos de dados primários e secundários são colocados online em locais separados O banco de dados primário é preenchido com dados do backup externo Servidores de aplicativos apontados para novo banco de dados primário Replicação restabelecida com o novo banco de dados secundário
RPO:	24 horas
RTO:	6 horas
Probabilidade:	Raramente (uma vez a cada 20 anos; os bancos de dados primário e secundário são hospedados em locais geograficamente separados, o que torna muito improvável a falha simultânea)
Último incidente	Nunca

Destruição de banco de dados por violação de segurança

Serviços Afetados	A maioria das contas hospedadas no banco de dados afetado.
Visão Geral da Recuperação	O banco de dados primário é restaurado a partir do backup completo mais recente A replicação é restabelecida com o banco de dados secundário
RPO:	24 horas
RTO	6 horas

Probabilidade:	Altamente improvável (uma vez a cada 10+ anos)
Último incidente	Nunca

Perda Completa da Instalação primária

Serviços Afetados	Plataforma para a maioria das contas
Visão Geral da Recuperação	Novos balanceadores de carga e servidores de aplicativos são apresentados no site secundário com o banco de dados secundário O banco de dados secundário antigo é promovido para o banco de dados primário. Um novo banco de dados secundário é criado em um terceiro site e a replicação é restabelecida O DNS é apontado para os novos balanceadores de carga no site de recuperação e os serviços são restaurados
RPO:	4 horas
RTO:	Comercialmente razoável
Probabilidade:	Extremamente improvável (uma vez a cada 100+ anos)
Último incidente	Nunca

Conclusão

Vivemos em um mundo imprevisível. Os desastres são inevitáveis de várias maneiras, e reconhecemos, apesar de arquitetar nossos produtos para alta disponibilidade e failover, que não seria sensato presumir que nosso negócio está imune a desastres. Como fornecedor líder de Software como Serviço (SaaS) educacional, reconhecemos que o seu bem não humano mais precioso que você nos confia são os dados. É por isso que tomamos um planejamento e preparação cuidadosos para criar um Plano de Recuperação de Desastre (DRP) robusto, conforme descrito neste documento, que esperamos infundir confiança e garantia de que, no evento inesperado de um desastre, estaremos preparados, capazes, e pronto para lançar esforços de recuperação para restaurar nossos serviços o mais rápido possível e minimizar a perda ou interrupção para nossos clientes.

Nossa abordagem para o planejamento de continuidade de negócios é que é uma parte viva da nossa organização que evolui à medida que mudamos e crescemos com nossos clientes. Aprendemos com a pandemia global do COVID-19 que a continuidade dos negócios não é ficção ou apenas um documento obrigatório para marcar no curso de negócios, mas, pelo contrário, é vital para sobreviver (e prosperar) em meio a desastres, ameaças e desafios. Durante os últimos dois anos da pandemia, nossos funcionários não apenas tiveram que se adaptar ao trabalho em casa e viver um novo normal por muitos meses de interrupção dos negócios como de costume, mas, ao mesmo tempo, foram obrigados a trabalhar em equipe unida. como nunca antes e fornecer esforços monumentais para manter nossos serviços funcionando normalmente quando milhares e milhares de alunos foram forçados a migrar para o aprendizado online. Graças ao nosso planejamento de continuidade de negócios, quando nossos clientes precisavam de nossos serviços mais do que nunca para fornecer alta disponibilidade e desempenho durante a pandemia global e tempos estressantes, nós entregamos.

Na Instructure, abordamos de forma proativa a continuidade dos negócios, criando resiliência em nossos processos-chave, uso de tecnologia e contratando e retendo pessoal-chave. Quando incidentes imprevistos impactarem ou interromperem nossos negócios, saiba que estamos prontos para agir, com planos robustos para recuperar rapidamente e garantir a continuidade de nossos negócios e dos seus durante e após qualquer incidente crítico que resulte em interrupção de nossa capacidade operacional normal.