



PANORAMA DE LA SEGURIDAD

Ingeniería, Seguridad y
Operaciones

Agosto 2024

Índice

| | |
|--|----------|
| Introducción | 4 |
| Overview | 4 |
| Programa de Seguridad de Instructure | 5 |
| Seguridad en Capas..... | 6 |
| Seguridad física..... | 6 |
| Seguridad Personal..... | 8 |
| Verificación de antecedentes..... | 8 |
| Seguridad 3PP..... | 8 |
| Seguridad AWS | 9 |
| Seguridad de Red y de Sistema | 12 |
| Acceso y autenticación del Sistema..... | 13 |
| Ataques de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS)..... | 14 |
| Seguridad de la Aplicación | 16 |
| Seguridad de Datos | 20 |
| Escaneo de virus y antimalware | 22 |
| Seguridad de Contraseña | 22 |
| Seguridad del correo electrónico | 24 |
| Ransomware | 24 |
| Gestión de vulnerabilidades y auditorías de seguridad | 26 |

| | |
|--|----|
| Cumplimiento de SOC 2..... | 29 |
| Cumplimiento de la norma ISO 27001..... | 29 |
| Respuesta de Instructure a las alertas de seguridad | 29 |
| Normas de seguridad de datos de la industria de tarjetas de pago ("PCI") ("DSS").. | 34 |
| General Data Protection Regulation (GDPR)..... | 34 |
| Conclusión..... | 36 |

Introducción

Overview

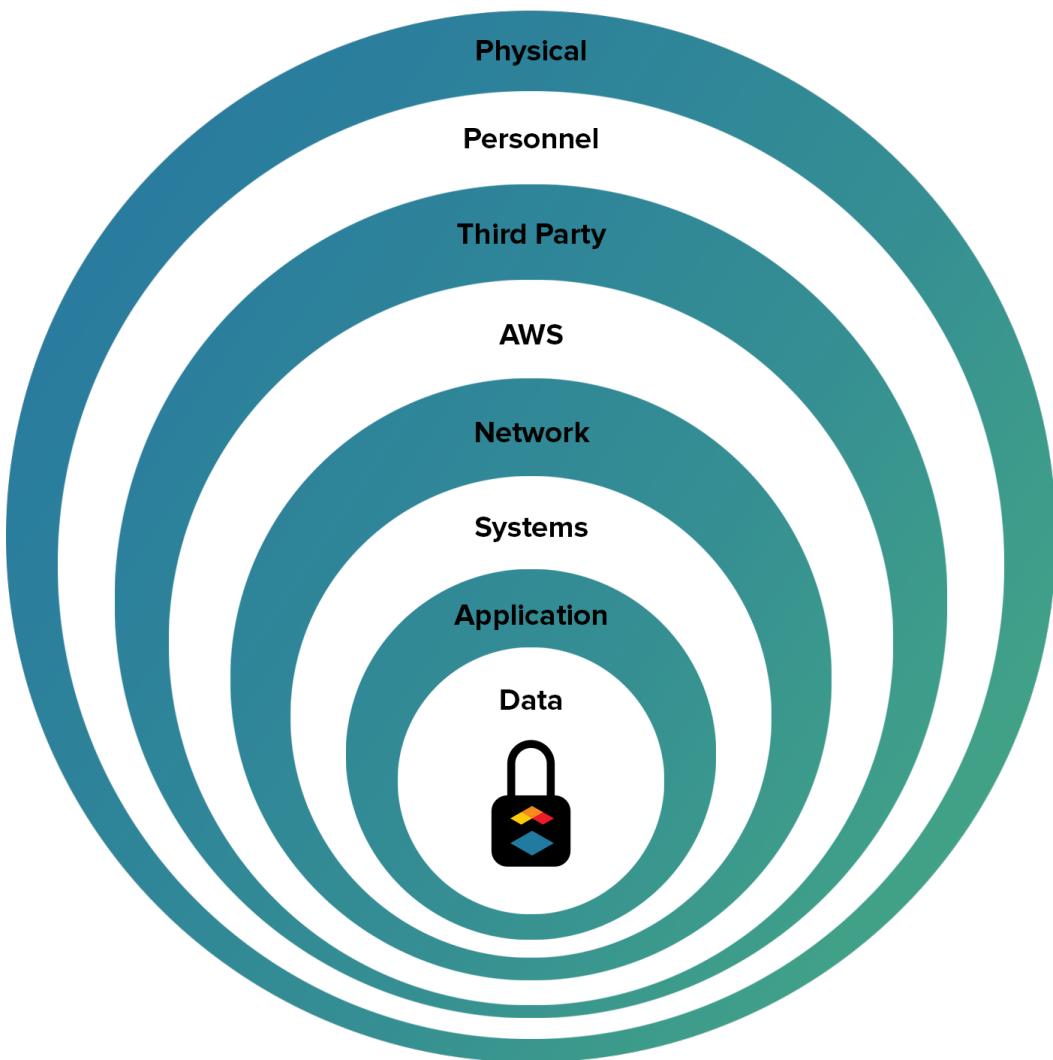
No debería ser un secreto para nadie en el mundo actual que la seguridad es fundamental. En un mundo cada vez más en línea, nos damos cuenta de que las amenazas para nuestra gente, nuestro negocio y sus datos están siempre presentes, y el esfuerzo y las medidas que tomamos para protegerlos son interminables. De hecho, a medida que crecen tanto nuestro negocio como el suyo, reconocemos que las amenazas también pueden aumentar en gravedad. El año pasado, el mundo ha visto el aumento de ransomware cada vez más insidioso y exploits generalizados como Apache Log4j, donde hasta un 50% de todos los negocios en línea informaron intentos de ataques a sus activos a través de la vulnerabilidad Log4Shell.

Es por eso que nuestro programa de seguridad se basa en estándares reconocidos internacionalmente, como ISO 27001, Marco de seguridad cibernética de NIST, Principios y criterios de servicios de confianza de AICPA y Controles de seguridad crítica CIS de SANS. Y, hablando de estándares, también nos aseguramos de desarrollar nuestras aplicaciones de acuerdo con el Top 10 de OWASP. En Instructure, implementamos mecanismos preventivos y de detección, así como procesos, controles y herramientas en capas, lo que ayuda a mitigar los riesgos que pueden afectar los datos. , personas, sistemas, operaciones, productos y nuestra misión como empresa. El propósito de este documento es describir estas capas y los tipos de controles que aplicamos para proteger a nuestros clientes de la maldad.



Programa de Seguridad de Instructure

El programa de seguridad de Instructure está dirigido por el director de seguridad de la información (CISO) de Instructure y cuenta con un equipo de profesionales de seguridad de la información talentosos, capacitados y experimentados. El equipo de seguridad de la información de Instructure es responsable de establecer sólidas prácticas de seguridad en todo Instructure a través de la gobernanza, la gestión de riesgos, las políticas, la educación, la ingeniería de seguridad, el cumplimiento de la seguridad, las operaciones de seguridad y la seguridad de las aplicaciones.



Seguridad en Capas

Seguridad física

Instructure aloja todas las aplicaciones web de cara al cliente y la infraestructura de soporte en AWS. La infraestructura de AWS es altamente estable, tolerante a fallas y segura. AWS publica un detallado documento técnico de seguridad que describe cómo AWS implementó mecanismos de seguridad física y protección ambiental para proteger los centros de datos de AWS en todo el mundo. Instructure se basa en la capacidad de AWS para diseñar y operar estos mecanismos y controles críticos para proteger el acceso físico a los datos y la disponibilidad de los servicios de Instructure.

Los centros de datos de AWS utilizan sistemas de control de acceso multifactor y vigilancia electrónica de última generación. Los centros de datos están atendidos las 24 horas del día, los 7 días de la semana, por guardias de seguridad capacitados y el acceso está autorizado estrictamente sobre la base de los privilegios mínimos. Los sistemas ambientales están diseñados para minimizar el impacto de las interrupciones en las operaciones. Las zonas de disponibilidad múltiples brindan resistencia frente a la mayoría de los modos de falla, incluidos desastres naturales o fallas del sistema. Los sistemas de energía eléctrica del centro de datos de AWS están diseñados para ser completamente redundantes y fáciles de mantener sin afectar las operaciones, las 24 horas del día y los siete días de la semana.

Las unidades de suministro de energía ininterrumpida (UPS) brindan energía de respaldo en caso de una falla eléctrica para cargas críticas y esenciales en la instalación. Los generadores proporcionan energía de respaldo para los centros de datos de toda la instalación.

Además, los controles de seguridad de AWS han sido auditados por una organización de evaluación de terceros de renombre y han producido las siguientes (y muchas otras) atestaciones y certificaciones:

- Informe SOC 2 Tipo II utilizando el marco de control de la organización de servicios presentado por el Instituto Americano de Contadores Públicos Certificados (AICPA)
- Certificación ISO / IEC 27001: 2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos
- Certificación TX-RAMP Nivel 2



- Proveedor de servicios de nivel 1 según el Estándar de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI)

Seguridad Personal

Como parte de nuestro compromiso con la seguridad, Instructure se dedica a mantener a nuestros empleados actualizados e informados sobre los últimos desarrollos y prácticas de la industria. Instructure brinda a los empleados capacitación sobre seguridad en el momento de la contratación y anualmente a partir de entonces. Como parte de la capacitación de concientización sobre seguridad de Instructure, se incluyen valiosos conocimientos y orientación relacionados con mantener seguros los datos de los clientes y los activos de Instructure de la variedad de amenazas comunes contra estos activos. Esto también incluye el requisito de que todos los empleados lean, entiendan y firmen los formularios de cumplimiento de la Ley de privacidad y derechos educativos de la familia (FERPA) y la Ley de protección de la privacidad en línea de los niños (COPPA).

Verificación de antecedentes

Instructure realiza verificaciones de antecedentes de todos los empleados y contratistas durante el proceso de contratación, y el empleo depende de los resultados de la verificación de antecedentes. Se realizan verificaciones de antecedentes adicionales, como verificaciones financieras/crediticias, verificaciones de calificaciones, antecedentes penales, etc., en empleados y/o funciones clave, por ejemplo, empleados que manejarán datos confidenciales o desempeñarán funciones financieras.

Seguridad 3PP

Instructure utiliza varias organizaciones de terceros para alojar sus productos para los clientes. Como parte de ayudar a garantizar que las organizaciones de terceros brinden servicios de manera segura a Instructure, el equipo de seguridad de Instructure realiza una investigación exhaustiva antes y periódicamente a lo largo de la relación con los proveedores externos.

Instructure utiliza varios terceros para brindar soporte a los productos de Instructure. Para ayudar a proporcionar una garantía de seguridad razonable de las prácticas y los mecanismos de seguridad en estos terceros, Instructure solicita y revisa copias de los informes de garantía de terceros proporcionados por estas organizaciones de manera continua para confirmar que estos controles



están operando de manera efectiva. Los contratos legales con estos terceros también incluyen disposiciones de seguridad para ayudar a garantizar la implementación y operación de controles de seguridad efectivos en las organizaciones de terceros.

Seguridad AWS

Los productos de Instructure se alojan en la infraestructura de nube de última generación proporcionada por Amazon Web Services (AWS). La infraestructura de AWS es altamente estable, tolerante a fallas y segura. Para obtener información adicional sobre el programa de seguridad de AWS, las certificaciones y el cumplimiento de los estándares, consulte <http://aws.amazon.com/security> y <http://aws.amazon.com/compliance/>.

Seguridad de la red AWS

Al utilizar las amplias protecciones y salvaguardas de la infraestructura en la nube de AWS, Canvas proporciona un monitoreo de seguridad y red sólido y considerable para proteger el entorno de producción, los datos y a nuestros clientes. Estas salvaguardas protegen e incluyen:

- **Ataques de Man in the Middle (MITM)**: todas las API de AWS están disponibles a través de puntos finales protegidos por SSL que proporcionan autenticación de servidor mediante certificados SSL firmados.
- **IP Spoofing**: las instancias de Amazon EC2 no pueden enviar tráfico de red falsificado. La infraestructura de firewall basada en host y controlada por AWS no permitirá que una instancia envíe tráfico con una dirección IP o MAC de origen distinta a la suya propia.
- **Escaneo de puertos**: cuando se detecta un escaneo de puertos, se registra e investiga.
- **Virtual Private Cloud**: Instructure utiliza VPC para segmentar, proteger y aislar aún más el tráfico de red.
- **Prevención de intrusiones**: Instructure utiliza Lacework y AWS GuardDuty para alertar e informar sobre incidentes de seguridad que ocurren contra los servicios de Instructure alojados en AWS.



- **Detección de intrusiones:** Instructure aprovecha la detección de intrusiones basada en host (HIDS) de Lacework en todos los productos y envía alertas al equipo de seguridad de Instructure. Todos los resultados se envían al sistema de gestión de registro centralizado de Instructure para su posterior análisis y generación de alertas.
- **Web Application Firewall:** utilizamos un Web Application Firewall (WAF) para todas las instancias de Canvas. Canvas también se fortaleció significativamente de una manera que ya es resistente a lo que bloquearía un firewall de aplicaciones web (WAF).
- **AWS Shield/ELB:** utilizamos AWS Shield y AWS Elastic Load Balancers para defendernos de los ataques de denegación de servicio distribuido administrado (DDoS).

Servicios AWS

Los servicios de AWS utilizados para alojar productos de Instructure incluyen Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Auto Scaling Groups (ASG), Simple Storage Service (S3), Elastic Block Store (EBS), Virtual Private Cloud (VPC) , Servicio de correo electrónico simple (SES), Gestión de acceso e identidad (IAM) y varios otros. Los productos de Instructure están diseñados para aprovechar al máximo las capacidades de capacidad y redundancia en tiempo real que ofrece AWS, ejecutándose en múltiples zonas de disponibilidad en regiones de todo el mundo. El almacenamiento principal lo proporciona Amazon S3, que está diseñado para una durabilidad superior al 99,99999999 %.

Regiones y Datacenters AWS

Amazon Web Services tiene múltiples ubicaciones (llamadas "regiones") en todo el mundo. Cada región es un área geográfica separada, y cada región tiene múltiples ubicaciones aisladas conocidas como Zonas de disponibilidad. Instructure utiliza las siguientes regiones de Amazon Web Services (AWS):

- Región Este de los Estados Unidos (Virginia del Norte)
- Región Oeste de EE. UU. (Oregón)
- Región central de Canadá (Montreal)
- Región Oeste de la UE (Irlanda)
- Región Central de la UE (Alemania)
- Región Asia Pacífico (Sydney)
- Región Asia Pacífico (Singapur)
- Región de Asia Pacífico (Bombay) (solo para Impact)



Seguridad de datos AWS

Instructure ha establecido varios controles para garantizar que los datos estén protegidos contra la divulgación, modificación o destrucción no autorizada, que incluyen:

- Todos los datos en reposo, incluidas las copias de seguridad de recuperación fuera del sitio, se cifran mediante el algoritmo AES-GCM de 256 bits.
- Todo el tráfico de datos que entra y sale de Canvas se cifra mediante TLS (v.12), cifrados que cumplen con la confidencialidad directa siempre que sea posible (p. ej., ECDHE-ECDSA-AES128-GCM-SHA256). La lista de cifrado aceptable se mantiene constantemente para garantizar que no haya vulnerabilidades presentes (por ejemplo, DELITO, BESTIA).
- Las copias de seguridad de recuperación fuera del sitio se cifran mediante el algoritmo AES-GCM de 256 bits y se almacenan en una ubicación altamente segura.

Además, los datos se almacenan de forma redundante en múltiples zonas de disponibilidad a través de Amazon S3. Los productos de Instructure replican datos casi en tiempo real en bases de datos de respaldo y secundarias, y los datos se respaldan diariamente. Instructure crea copias de seguridad diarias de la base de datos de datos y contenido en Amazon S3. La replicación de datos y las copias de seguridad garantizan que, en caso de que sea necesaria una restauración del sistema, el potencial de pérdida de datos sea limitado.

Seguridad de Red y de Sistema

Los productos Instructure se han diseñado para lograr un alto nivel de seguridad al proporcionar un enfoque sencillo y utilizable para la autenticación de usuarios, el acceso al sistema y los permisos jerárquicos basados en roles. Estos productos están diseñados para respaldar las propias políticas de seguridad interna de la institución y para brindar una protección rigurosa contra intrusiones internas o externas. Estos productos refuerzan la seguridad del sistema al presentar un modelo de seguridad simple a los usuarios finales.



Acceso y autenticación del Sistema

Instructure utiliza un sistema de aprobación múltiple para otorgar acceso a los empleados. El gerente del empleado que solicita acceso debe completar un boleto solicitando el nivel detallado de acceso al sistema y especificando qué partes, funciones y características deben ser accesibles para el empleado. Se debe proporcionar una justificación comercial clara, válida y necesaria para el usuario en cuestión. Se incluyen otras aprobaciones según sea necesario y en función del acceso que se solicita. Si todas las partes aprueban el acceso del empleado, el equipo de tecnología respectivo otorga el acceso según lo solicitado en el ticket. De acuerdo con la política de salida de empleados, las cuentas de usuario se eliminan tras la terminación del empleo.

Todos los empleados de Instructure a bordo deben leer, comprender y firmar los formularios de cumplimiento de la Ley de Privacidad y Derechos Educativos de la Familia (FERPA) y la Ley de Protección de la Privacidad Infantil en Línea (COPPA).

Los equipos de tecnología de Instructure facilitan la instalación de claves para todos los empleados con acceso a los servidores. Un sistema de configuración automatizado instala las claves públicas de los empleados por servidor según las necesidades. Este mismo proceso de configuración revoca automáticamente las claves globalmente cuando es necesario. Los empleados deben utilizar el cifrado de disco completo y la protección con contraseña en sus máquinas de trabajo para proteger sus claves privadas y otros datos confidenciales. Las claves privadas utilizadas para HTTPS se almacenan cifradas y descifradas por operaciones cuando se implementan en los servidores de aplicaciones.

El monitoreo y las alertas están en su lugar para detectar y advertir de cualquier cambio en las claves, los usuarios del sistema, los intentos de inicio de sesión y sudo, y otros eventos de interés.



Ataques de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS)

Instructure sigue estrictamente las mejores prácticas de la industria para mitigar los ataques de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS) sin afectar la disponibilidad del servicio para los usuarios finales. Naturalmente, la infraestructura de AWS es resistente a DDoS por diseño y cuenta con el respaldo de sistemas de mitigación de DDoS que pueden detectar y filtrar automáticamente el exceso de tráfico. Por ejemplo, empleamos AWS Shield como un servicio de protección de denegación de servicio distribuido (DDoS) administrado que protege nuestras aplicaciones. AWS Shield proporciona detección siempre activa y mitigaciones automáticas en línea, y ha mitigado algunos de los ataques DDoS más grandes jamás registrados, deteniendo un ataque de 2,3 Tbps a mediados de febrero de 2020. Esto brinda a nuestros clientes protección y defensa automáticas contra la red y los ataques más comunes. Ataques DDoS en la capa de transporte. Pero, como es el caso con nuestra filosofía actual de proporcionar productos de software como servicio de primer nivel, vamos mucho más allá que simplemente ofrecer protección DDoS estándar.

Para nuestras aplicaciones web, los balanceadores de carga (AWS Elastic Load Balancing) solo escuchan un único protocolo en dos puertos. HTTP (TCP) en el puerto 80, que se redirige a HTTPS en el puerto 443, que sirve todos los datos a través de TLS. Al distribuir automáticamente el tráfico de aplicaciones entrantes entre múltiples objetivos y controlar y absorber el tráfico de red, los balanceadores de carga crean una aplicación de alta disponibilidad para los usuarios y una sólida estrategia de mitigación de DoS/DDoS, que desvía fácilmente las solicitudes maliciosas o no deseadas. Reducir la superficie de ataque de esta manera significa que bloqueamos el tráfico de muchos vectores de ataque DDoS comunes que no se comunican en el mismo puerto o protocolo que nuestra aplicación.

Al utilizar Elastic Load Balancing (ELB), reducimos en gran medida el riesgo de sobrecargar la aplicación mediante la distribución del tráfico entre muchas instancias de back-end y creamos una línea de defensa entre Internet y nuestra red Virtual Private Cloud (VPC) que aloja nuestros servicios.



ELB se escala automáticamente, lo que nos permite administrar mayores volúmenes de tráfico no anticipado, como multitudes repentinas o ataques DDoS. Los balanceadores de carga solo aceptan conexiones TCP bien formadas, lo que significa que muchos ataques DDoS comunes, como inundaciones SYN o ataques de reflexión UDP, no se aceptarán ni pasarán a la aplicación. Cuando nuestros balanceadores de carga detectan este tipo de ataques, escalan automáticamente para absorber el tráfico adicional, lo que garantiza que no haya cambios en la disponibilidad del servicio para los usuarios finales.

Debido a que todo el ecosistema de Instructure Learning Platform se ejecuta en servidores virtualizados como parte de las nubes privadas virtuales (VPC) de Amazon Web Services (AWS), tenemos una arquitectura resistente a DDoS que minimiza los puntos de entrada públicos mediante grupos de seguridad y listas de control de acceso a la red (ACL). Esto significa que no solo se minimizan las superficies de ataque de las aplicaciones, sino que los ataques DDoS comunes se detectan y mitigan rápidamente mediante los grupos de seguridad de AWS. Configuramos los grupos de seguridad de AWS para permitir el tráfico de red (denegar todo, permitir por excepción aprobada) solo a los puertos autorizados, por lo tanto, denegar automáticamente el acceso a cualquier otro puerto o protocolo y, a su vez, proteger los componentes backend de nuestras aplicaciones de un ataque directo

Además de las mejores prácticas anteriores, el registro y la supervisión constantes del servicio de Instructure Learning Platform nos permite identificar rápidamente cualquier ataque DoS/DDoS legítimo y participar en una respuesta inmediata al incidente.



Seguridad de la Aplicación

Codificación segura y prácticas de Desarrollo

Mantener y mejorar la seguridad es un proceso disciplinado, continuo y continuo. La codificación segura y las pruebas de seguridad son, por lo tanto, componentes integrales de la metodología de ingeniería y desarrollo de Instructure. Todo el código de la aplicación debe pasar por un proceso de revisión por pares de desarrolladores antes de fusionarse con el repositorio de base de código. La revisión del código incluye auditoría de seguridad basada en los documentos de revisión de código y codificación segura del Proyecto de seguridad de aplicaciones web abiertas (OWASP) y otras fuentes de la comunidad sobre las mejores prácticas de seguridad.

Todos los desarrolladores están capacitados para identificar y analizar problemas de seguridad al escribir y revisar código. Los miembros de los equipos de tecnología de Instructure se suscriben a listas, blogs y otros recursos centrados en la seguridad para mantener, ampliar y compartir el cuerpo colectivo de conocimientos. Instructure mantiene una wiki interna para discutir y compartir las mejores prácticas para la mitigación y prevención de problemas de seguridad y vulnerabilidades. Los equipos de seguridad e ingeniería se mantienen actualizados sobre las prácticas generales de seguridad, sobre los vectores de ataque recientes y sobre cualquier problema de seguridad específicamente relacionado con los lenguajes, aplicaciones web, marcos y entornos que Instructure emplea para desarrollar, alojar y mantener los productos de Instructure.

Las revisiones por pares de todos los cambios en el código fuente son obligatorias. Se realizan múltiples revisiones por pares para cada cambio en la base del código para detectar y corregir cualquier error, falla de seguridad y cualquier otro defecto del código. Los cambios en el código deben ser validados por revisión por pares antes de que el código sea aprobado y enviado al repositorio base de código.

Pruebas y control de calidad

Una vez que el nuevo código ha pasado la revisión por pares, el código se incorpora a la base del código y se somete a pruebas y garantía de calidad. El nuevo código se implementa en un servidor de integración continua donde se prueba de inmediato. El equipo de pruebas de Instructure ejecuta lo siguiente:

- Pruebas unitarias (código de prueba con código)
- Pruebas de integración (prueba de código con integraciones con otro código)
- Pruebas de Selenium (prueba de cómo funciona el código en el navegador) en todos los diferentes entornos y en diferentes bases de datos.

Después de pasar estas pruebas, el código se incorpora en la rama principal del código para garantizar la calidad (QA) formal. El equipo de control de calidad prueba el nuevo código en todas las plataformas y navegadores compatibles.

Identidad del cliente y gestión de acceso

Los productos de Instructure admiten la gestión de identidad centralizada y la autenticación delegada a través de la integración con el Servicio de autenticación central (CAS) y SAML 2.0. Si la autenticación falla, la aplicación busca las credenciales utilizando su servicio de autenticación interno. Si la autenticación falla nuevamente, la aplicación negará el inicio de sesión del usuario.

Protocolo y seguridad de sesión

Los productos de Instructure utilizan HTTPS (HTTP sobre TLS) para todas las comunicaciones. Todo el tráfico entrante y saliente se cifra mediante TLS 1.2, lo que garantiza que toda la información de identificación personal, el intercambio de credenciales, las solicitudes de página y los datos de sesión sean seguros. Estos productos cifran los datos en reposo en la capa de la base de datos. Esto incluye toda la información del usuario, el rendimiento, la información del curso y las pruebas en cursos creados de forma nativa.

Las sesiones se mantienen y se pueden invalidar. Una cookie de sesión cifrada, firmada con un código de autenticación de mensaje hash (HMAC), solo se utiliza para identificar una sesión actual. El HMAC y el contenido de las cookies están encriptados con Advanced Encryption Standard (AES) -256 en modo de retroalimentación de cifrado (CFB). El contenido de la cookie no puede secuestrarse durante la transmisión a través de la red, el usuario no puede verlo ni manipularlo, y no se puede acceder a él a través de JavaScript. Los ID de sesión se comparan y validan con los valores almacenados en el servidor. Una sesión invalidada requerirá que el usuario inicie sesión nuevamente.

Las sesiones se restablecen en cada inicio de sesión exitoso para evitar el acceso a los ID de sesión en inicios de sesión posteriores. Para evitar vulnerabilidades de falsificación de solicitudes entre sitios (CSRF), todas las acciones del usuario que modifican datos requieren una clave secreta de sesión para publicar datos. Todas las solicitudes que modifican datos se realizan con solicitudes HTTPS POST o PUT, nunca GET.

Cómo evitar ataques de scripts entre sitios (XSS)

Instructure emplea una variedad de estrategias para prevenir ataques de secuencias de comandos entre sitios (XSS). Por ejemplo, cuando la aplicación crea un formulario para la entrada del usuario, se incrusta un token de uso único en el formulario HTML para que la aplicación pueda identificar el formulario y verificar que no originó otro sitio en un posible intento de ataque.

Las aplicaciones desinfectan el contenido para protegerlo contra vulnerabilidades intencionales o no intencionales. Cuando el contenido se coloca en un formulario, como el contenido que ingresa un usuario con el Editor de contenido enriquecido, la aplicación limpia (tanto del lado del cliente como del lado del servidor) el contenido y elimina cualquier contenido malicioso. La desinfección del contenido evita el secuestro de sesiones, los ataques de formularios y otros accesos y / o modificaciones de datos no autorizados.

Todo el contenido introducido por el usuario se desinfecta antes de guardarse en la base de datos. La desinfección se realiza mediante una lista de permisos explícitos, no una lista de bloques, lo que evita la adición de JavaScript a los datos HTML y también evita la adición de etiquetas HTML no seguras.

Seguridad de carga y descarga de archivos

Los archivos cargados por el usuario se almacenan en la infraestructura de Amazon S3 con nombres y carpetas únicos. Para evitar la toma lateral de los archivos cargados por el usuario y preservar la integridad del sistema, Canvas coloca los archivos cargados en el repositorio de Archivos bajo un subdominio diferente para establecer un dominio de seguridad separado con el fin de aprovechar las medidas de seguridad del mismo origen del navegador. El navegador aplicará la seguridad entre los archivos cargados y la sesión del usuario y evitará el secuestro de la sesión. Si un archivo cargado ejecuta código usando JavaScript, Java u otras tecnologías, ese código no podrá acceder a la sesión del usuario ni podrá realizar solicitudes a Canvas en nombre del usuario. Todas las descargas de archivos requieren claves de autorización únicas y de corta duración.



Seguridad de Datos

Instructure tiene una Política de clasificación, manejo y cifrado de datos establecida, documentada, aprobada y difundida. Esta política describe los procesos para clasificar y manejar datos durante su vigencia. Como parte de esta política, los datos se clasifican en uno de los siguientes:

- Confidencial
- Interno
- Público

Confidencial

Los datos confidenciales son elementos de datos sensibles que legal y contractualmente requieren mecanismos de protección de seguridad y privacidad. Los ejemplos de datos confidenciales incluyen datos de clientes, información de autenticación, información de identificación personal (PII), información de pago y cualquier cosa sujeta al privilegio abogado-cliente. Los datos confidenciales deben estar cifrados en todo momento, tanto en tránsito como en reposo, compartidos solo con el personal apropiado y autorizado, y se destruyen de forma segura.

Interno

Los datos internos son datos para uso interno de Instructure solamente. Estos elementos de datos se consideran "información privilegiada" y están protegidos del público. Algunos ejemplos de datos internos son la correspondencia por correo electrónico, los materiales marcados como "Instructure internal" y otra información de Instructure no publicada o disponible públicamente. Estos elementos de datos residen en los sistemas de Instructure y solo se comparten con entidades externas en virtud de un acuerdo de confidencialidad (NDA) totalmente ejecutado.

Público

Los datos públicos son datos de fuentes de acceso público. Los ejemplos de datos públicos incluyen datos de artículos de noticias, comunicados de prensa y contenido de búsqueda en Internet. En Instructure, los datos clasificados como públicos no requieren ningún requisito especial de manejo de datos.

Escaneo de virus y antimalware

Instructure realiza análisis antivirus y antimalware de todos los archivos cargados y almacenados en Canvas que tengan un tamaño de archivo de 64 MB o menos. La mayoría de los programas maliciosos que se encuentran normalmente en los archivos suelen tener menos de un megabyte (MB) de tamaño y, por lo general, los virus y el malware no se activan a menos que se abran explícitamente en Canvas. Al igual que con los archivos de cualquier otra fuente, recomendamos que las instituciones académicas sigan buenas prácticas de seguridad, como ejecutar software antivirus/malware y tener la debida precaución al ejecutar archivos desconocidos de otras computadoras.

En todos los dispositivos de Instructure, utilizamos software mejorado de detección y respuesta de puntos finales (EDR) en todos los dispositivos, más allá del antivirus estándar con activación de alertas.

Seguridad de Contraseña

Las contraseñas de los usuarios están encriptadas. Las credenciales utilizadas para acceder al sistema nunca se almacenan en la infraestructura de la aplicación. Más bien, las contraseñas se cifran unidireccionalmente mediante una combinación de un valor salt aleatorio específico del usuario y SHA512, el algoritmo criptográfico de hash unidireccional. Las credenciales entrantes pasan por el mismo procedimiento y se comparan con el valor almacenado cifrado y salt. De esta manera, Instructure no tiene conocimiento ni forma de recuperar las credenciales de usuario. Si un cliente se integra con un proveedor de identidad externo (p. ej., LDAP, AD, CAS, SAML, etc.), se utilizará la configuración de seguridad, como las políticas de contraseñas, definidas en el proveedor de autenticación externo.

Como una capa adicional de seguridad de contraseña, Canvas proporciona una funcionalidad de autenticación multifactor (MFA) integrada que se puede habilitar con una de tres opciones: requerida para los administradores, requerida para todos los usuarios u opcional para todos los usuarios. La autenticación multifactor de Canvas requiere un dispositivo móvil para configurar MFA con una cuenta

de usuario. El dispositivo debe poder enviar mensajes de texto (SMS), o si sus usuarios tienen un teléfono inteligente, pueden descargar su aplicación MFA preferida, como Google Authenticator o Authy, etc.

Seguridad del correo electrónico

Las notificaciones por correo electrónico dentro de nuestros productos usan SPF, que es un sistema de validación de correo electrónico diseñado para evitar el correo no deseado y el phishing al detectar y prevenir la suplantación de correo electrónico. SPF permite a los administradores especificar qué hosts (direcciones IP, computadoras) pueden enviar correo desde un dominio determinado mediante la creación de registros SPF específicos en el DNS. Los intercambiadores de correo luego usan el DNS para verificar que el correo de un dominio determinado esté siendo enviado por un host sancionado.

También usamos DomainKeys Identified Mail (DKIM) para firmar el correo. DKIM asocia nuestro nombre de dominio a un mensaje de correo electrónico, lo que permite, por ejemplo, que Canvas se responsabilice del mensaje (firmar el mensaje). La firma digital es validada por el destinatario. La responsabilidad la reclama un firmante (instructure.com), independientemente de los autores o destinatarios reales del mensaje, agregando un campo DKIM-Signature: al encabezado del mensaje. El verificador recupera la clave pública del firmante mediante el DNS y luego verifica que la firma coincida con el contenido real del mensaje.

Ransomware

El sólido programa de seguridad de la información de Instructure se ejecuta en un ciclo continuo de mejora de PDCA. Para mitigar el malware y el ransomware, utilizamos una serie de prácticas de seguridad recomendadas por la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA).

Estas prácticas incluyen (pero no se limitan a):

- **Mantener los sistemas actualizados;** Eliminación de bibliotecas y sistemas operativos al final de su vida útil y mantenimiento de sistemas y aplicaciones actualizados con parches de seguridad.

- **Gestión de usuarios;** Aprovisionamiento de usuarios con privilegios mínimos y control de acceso basado en roles. Realizar revisiones regulares de acceso de usuarios en todos los sistemas y directorios, prohibiendo específicamente las cuentas compartidas.
- **Seguridad de punto final de usuario;** Utilizando el software mejorado de detección y respuesta de puntos finales (EDR) en todos los dispositivos de los usuarios, más allá del antivirus estándar.
- **Autenticación multifactor;** Habilitación de la autenticación multifactor frente a todas las VPN, bastiones y aplicaciones para evitar la reutilización de las credenciales perdidas. Registro y alertas sobre direcciones IP y ubicaciones nuevas e inusuales utilizadas por un usuario para autenticarse en los servicios.
- **Recuperación de desastres;** Un plan integral de recuperación ante desastres que identifica los componentes críticos de cada servicio y cómo se respalda y recupera cada componente crítico en respuesta a un evento significativo. La recuperación de cada componente crítico se prueba periódicamente.
- **Mapeo de datos;** Auditoría del almacenamiento de datos confidenciales. Reducir elementos de datos almacenados a solo lo necesario para operar un servicio. Revisiones y monitoreo continuos en sistemas con almacenamiento de datos confidenciales.
- **Desarrollo y operaciones;** Todo el código pasa por una revisión por pares del desarrollador antes de fusionarse con el repositorio de base de código y se escanea en busca de vulnerabilidades de seguridad (incluidas las dependencias) antes de lanzarlo a producción.
- **Identificación de vulnerabilidades;** Los puntos finales públicos y los entornos internos se escanean en busca de vulnerabilidades de forma regular. Se contrata a terceros competentes para realizar pruebas de penetración dirigidas a fin de descubrir problemas de seguridad. Se fomentan y recompensan las pruebas de seguridad colaborativas.
- **Simplificar y optimizar;** Implementamos un conjunto común de controles de seguridad en todos los equipos y servicios. Esto incluye un método coherente de autenticación de usuarios en servidores, entornos de nube y servicios de producción.

- **Equipo de seguridad;** Un equipo de seguridad dedicado con la responsabilidad general de la seguridad que reside dentro de la organización. El equipo de seguridad es responsable de que todos los aspectos de la seguridad se tengan en cuenta en la comunicación con la gerencia, el análisis de riesgos y la planificación trimestral y anual para incorporar el trabajo de seguridad para todos los equipos.
- **Capacitación;** Capacitación continua y regular sobre seguridad del personal que incluye, entre otros, pruebas de phishing automatizadas de todo el personal y remediación del personal propenso a phishing.

Gestión de vulnerabilidades y auditorías de seguridad

Revisiones de Seguridad Interna y Gestión de Vulnerabilidad

El equipo de seguridad de Instructure lleva a cabo exploraciones periódicas de vulnerabilidades tanto de nuestros activos no públicos como de nuestros entornos de producción, utilizando una serie de herramientas internas y externas, scripts personalizados y agentes de supervisión para buscar bibliotecas de código abierto y vulnerabilidades de dependencia.

Los tipos de análisis de vulnerabilidades que realizamos incluyen (pero no se limitan a):

- Análisis de composición de software (vulnerabilidades de código abierto)
- Escaneos dinámicos de seguridad de aplicaciones
- Configuraciones de la nube
- Exposiciones de secretos
- Vulnerabilidades del sistema operativo

Los miembros del equipo de seguridad de Instructure tienen muchos años de experiencia en auditorías de seguridad realizadas por grandes corporaciones y agencias gubernamentales. Las políticas y procedimientos de auditoría se revisan periódicamente y se actualizan según sea necesario por el equipo de seguridad. El equipo de seguridad de Instructure realiza auditorías de seguridad internas exhaustivas, exhaustivas y prescriptivas. En estas auditorías, el equipo de seguridad:

- Escanea la aplicación externamente, utilizando herramientas tanto internas como personalizadas.
- Documenta las posibles vulnerabilidades, recomienda correcciones e implementa la solución más ventajosa. Las correcciones se vuelven a probar, tanto por el descubridor (es) original (s) como por otros miembros nuevos del equipo para el problema.
- Las correcciones realizadas en bibliotecas externas a las actividades de desarrollo ascendentes se aplican e incluyen inmediatamente en los paquetes oficiales en lugar de esperar a la próxima versión programada de la actualización de Canvas.

Revisiones de seguridad externa

Además del escaneo regular y las auditorías de seguridad internas periódicas realizadas a lo largo del año, Instructure realiza revisiones de seguridad abiertas de terceros. La auditoría de seguridad externa y abierta es una forma en que Instructure puede demostrar no solo el estado de la seguridad de la aplicación, sino también nuestra capacidad de respuesta ante cualquier vulnerabilidad. Utilizando BugCrowd, un especialista en seguridad de terceros, los especialistas en seguridad externos realizan pruebas de penetración de recompensas por errores durante todo el año. Anualmente, una salida de todos los resultados de las pruebas de penetración se agrega al informe anual de pruebas de penetración de Instructure y se proporciona a los clientes tanto públicamente en nuestro sitio web como directamente cuando lo solicitan. Instructure publica estos resultados porque estamos anclados en la apertura y transparencia a nuestros clientes.

Para los clientes que estén interesados en realizar su propia auditoría de seguridad de los productos de Instructure, Instructure, previa solicitud, permitirá la prueba de un entorno que no sea de producción en condiciones establecidas y/o configurará un entorno en el que puedan realizar escaneos de vulnerabilidades automatizados y manuales.

Cumplimiento de SOC 2

Instructure produce, anualmente, informes SOC2 Tipo II para nuestros productos que cubren los siguientes principios: seguridad, disponibilidad, confidencialidad, integridad de procesamiento y privacidad. Estos informes están disponibles bajo NDA mutuo.

Cumplimiento de la norma ISO 27001

Instructure cuenta con la certificación ISO 27001:2013 para productos que incluyen Canvas LMS, Canvas Studio, Mastery Connect e Impact.

Respuesta de Instructure a las alertas de seguridad

Todos los productos de la suite Instructure Learning Platform son servicios en la nube con una sola versión del código base y el entorno de producción, por lo que las actualizaciones de seguridad se aplican de forma inmediata y automática para toda la base de clientes como parte de los servicios de alojamiento de Instructure.

Las exploraciones periódicas de vulnerabilidades de las aplicaciones y la infraestructura se realizan utilizando herramientas de terceros, scripts personalizados y herramientas de código abierto. Si se detecta alguna vulnerabilidad, los equipos de seguridad e ingeniería de Instructure trabajan juntos para analizar, diseñar y desarrollar el parche requerido. Los parches relacionados con la seguridad para el sistema operativo, el software de la aplicación y las bibliotecas se aplican dentro de una (1) semana, excepto en aquellos casos en los que se ha determinado que son de alta gravedad. Si se detecta una vulnerabilidad de seguridad de alta gravedad, los equipos de seguridad e ingeniería de Instructure otorgan la máxima prioridad a la reparación de la vulnerabilidad. Los parches de seguridad de alta gravedad se aplicarán dentro de las veinticuatro (24) horas con los mejores esfuerzos comerciales. En la mayoría de los casos, la vulnerabilidad se puede solucionar mediante un parche en caliente sin incurrir en tiempo de inactividad en los entornos de producción.

Instructure, en coordinación con AWS, adopta un enfoque proactivo para hacer cumplir los controles SOC 2. Las retrospectivas se completan después de cualquier problema operativo significativo, independientemente del impacto externo, y se redactan documentos retrospectivos (análisis de causa raíz) para que se capture la causa raíz y se tomen medidas preventivas en el futuro. La implementación de las medidas preventivas se rastrea durante las reuniones de operaciones semanales de Instructure.

Política y plan de respuesta a incidents

Instructure ha implementado un conjunto integral de tecnologías de seguridad, políticas de administración y revisión, operaciones de monitoreo y procedimientos de cumplimiento para garantizar que nuestro sistema y seguridad de datos cumpla o supere los estatutos y regulaciones gubernamentales, estándares de la industria y requisitos institucionales. Instructure se da cuenta de que ninguna organización es impenetrable y, en consecuencia, prepara planes para ayudar a facilitar de manera más efectiva un incidente de seguridad.

Política de respuesta a incidents

Al respaldar estas medidas preventivas, Instructure ha establecido un conjunto de respuestas prescriptivas que deben ejecutarse en caso de una exposición de datos no autorizada. La exposición a los datos ocurre cuando la información restringida o confidencial se divulga, se expone o se considera razonablemente que se reveló o se expuso a una persona, proceso o sistema no autorizado. La política de exposición de datos de Instructure ha sido diseñada para garantizar:

- La detección más temprana posible de una violación de seguridad del sistema o de los datos;
- Rápido aseguramiento del sistema y los datos para evitar una exposición no autorizada adicional;
- Notificación a los usuarios y otras partes afectadas de que la información confidencial o personal ha sido o puede haber sido expuesta o comprometida por una violación de la seguridad del sistema.

Plan de respuesta a incidents

En caso de una violación de la seguridad y una posible exposición de datos no autorizada, el director de seguridad de la información (CISO) de Instructure supervisará y ejecutará un plan de acción que se



ajuste a las pautas descritas en las subsecciones a continuación. El plan de acción exacto a ejecutar y la secuencia de las acciones tomadas dependerán del tipo y alcance de la brecha en la seguridad.

Determinar el alcance de la violación de seguridad

En todos los casos, el Head de Seguridad y el personal de Instructure evaluarán rápidamente el estado de la infracción para determinar si la actividad está en curso. Si la actividad está en curso, el personal de seguridad tomará las medidas necesarias inmediatas para detener la actividad no autorizada con el fin de evitar cualquier pérdida adicional de datos. Una vez que se haya aislado y detenido la violación, el Head de Seguridad y el personal de Instructure comenzarán a determinar el alcance de la violación, la fuente y el tipo de datos involucrados, la cantidad de datos y las personas afectadas y los recursos del sistema.

Ensamble el Equipo de Respuesta a Incidentes

El CISO de Instructure reunirá al equipo de respuesta a incidentes a través de nuestro sistema de pager (que también envía alertas las 24 horas del día, los 7 días de la semana a los equipos de Seguridad y DevOps sobre cualquier alerta o advertencia activada).. La composición y el cargo del equipo dependerán del tipo de violación y la exposición de datos resultante. El equipo lleva a cabo una evaluación preliminar para ayudar a desarrollar una respuesta personalizada. Una vez contenido el incidente, este equipo también evaluará los cambios en los procesos, sistemas y/o políticas para evitar que se repita el evento.

Control de la difusión de la información

Para garantizar que solo se publique información precisa y oportuna que no interfiera con la investigación en curso, solo el CISO de Instructure estará autorizado a proporcionar información a cualquier parte fuera del equipo de respuesta a incidentes.

Equipo administrativo de alerta

El CISO de Instructure alertará a los administradores senior apropiados, incluido el equipo ejecutivo de Instructure, los funcionarios de la institución cliente, los ingenieros de sistemas y otros actores clave, según se justifique.

Identificar personas afectadas

El CISO de Instructure trabajará con los funcionarios de la institución, incluidos el vicepresidente senior de ingeniería y el vicepresidente de operaciones de Instructure, y el equipo de respuesta a incidentes para determinar las identidades de las personas afectadas y determinar el alcance de la exposición de datos.

Notificar a las personas afectadas

El CISO de Instructure trabajará con el vicepresidente senior de ingeniería, el abogado general, el vicepresidente de operaciones y el equipo de respuesta a incidentes para redactar y ejecutar un plan de notificación. El propósito del plan es proporcionar una notificación completa, precisa y oportuna que cumpla o supere todos los requisitos legales. En el caso de problemas de seguridad de alta gravedad, las partes afectadas serán alertadas de inmediato, mientras que las partes indirectamente afectadas serán alertadas dentro de las cuarenta y ocho (48) horas. Estos requisitos legales variarán según el estado. Trabajando con las partes apropiadas, el CISO de Instructure y el equipo de respuesta a incidentes notifican a todas las personas afectadas y desarrollan estrategias de remediación apropiadas y suficientes para la situación.

Administrar la resolución de incidentes y consecuencias

El CISO de Instructure y el equipo de respuesta a incidentes continuarán actualizando y comunicando el estado de la respuesta, determinarán los próximos pasos y desarrollarán un plan post mortem para revisar la eficiencia y eficacia de la respuesta y desarrollar futuros procesos y procedimientos de prevención y/o mitigación.

Normas de seguridad de datos de la industria de tarjetas de pago ("PCI") ("DSS")

Nuestros productos no almacenan, procesan ni transmiten datos de tarjetas de crédito y, como tales, no están obligados a cumplir con PCI DSS. Sin embargo, nuestro producto Canvas Catalog redirige a los usuarios a pasarelas de pago integradas configuradas por la institución cliente. Catalog cumple con PCI DSS como lo demuestra el formulario D del cuestionario de autoevaluación (SAQ) de Instructure que está disponible a pedido.

General Data Protection Regulation (GDPR)

GDPR significa el Reglamento General de Protección de Datos de la UE. El GDPR es una ley de la Unión Europea ("UE") que regula los datos personales de las personas en la UE. El GDPR armonizó la ley de protección de datos en toda la UE e introdujo cambios radicales que requieren que las empresas realicen actualizaciones significativas en sus políticas y prácticas de privacidad y seguridad. Instructure se compromete a ayudar a nuestros clientes a cumplir con el GDPR.

Instructure ha cumplido con el GDPR desde la fecha de entrada en vigor (25 de mayo de 2018).

Para garantizar el cumplimiento continuo del GDPR, Instructure hace lo siguiente:

- Educa a la organización sobre el GDPR y sus requisitos.
- Ha realizado un análisis de brechas de GDPR con la ayuda de un bufete de abogados externo acreditado con experiencia en GDPR, y ha cerrado esas brechas.
- Mantiene una lista actualizada de los datos personales que posee Instructure, de dónde provienen y con quién Instructure puede compartirlos.
- Mantiene actualizados los avisos de privacidad que cumplen con el GDPR.

- Garantiza que los procedimientos existentes cubran todos los derechos que tienen las personas en virtud del GDPR.
- Identifica nuestra base legal para procesar datos personales, documentarlos y actualizar nuestro aviso de privacidad para explicárselo a las personas.
- Revisa cómo Instructure obtiene, registra y gestiona el consentimiento.
- Revisa y actualiza los contratos con terceros para garantizar que nuestras obligaciones de privacidad estén actualizadas.
- Garantiza que se implementen los procedimientos correctos para detectar, informar e investigar una violación de datos personales.
- Mantiene procesos para las Evaluaciones de Impacto de Protección de Datos.
- Ha designado un Delegado de Protección de Datos.

Salvaguardias para la transferencia de datos transfronterizos

Uno de los requisitos del RGPD es que cualquier dato personal transferido "transfronterizo", es decir, fuera de la UE, solo se pueda mover de conformidad con un mecanismo legal. Instructure utiliza las cláusulas contractuales estándar de la Comisión Europea (cláusulas modelo) como un método legal para transferir datos personales fuera de la UE. Al incorporar las cláusulas modelo en el Apéndice de procesamiento de datos de Instructure ("DPA"), tanto los controladores de datos (clientes de Instructure en la UE) como los procesadores de datos (Instructure) están obligados contractualmente a ciertas salvaguardas técnicas y organizacionales relacionadas con los derechos de privacidad de cada persona.

Conclusión

Sabemos que la seguridad es primordial para nuestros clientes en un mundo impulsado por SaaS. Por eso, ponemos mucho cuidado en implementar tanto mecanismos preventivos como de detección, así como procesos, controles y herramientas en capas, lo que ayuda a mitigar los riesgos que pueden afectar los datos, las personas, los sistemas, las operaciones, los productos y nuestra misión como empresa. Como se describe en este documento, nuestro equipo de seguridad dedicado está lleno de profesionales de seguridad apasionados, capacitados y experimentados que, además de garantizar el cumplimiento de la evaluación de terceros, como el marco de control de la organización de servicios, se enfocan en detectar y proteger contra la maldad, y ganar y mantener su confianza.



© 2024 Instructure Inc. All rights reserved.