Señores,
Agrícola.

El siguiente documento especifica las consideraciones técnicas en materias de seguridad de la información con las que cuenta nuestro sistema de gestión agrícola Agri y los estándares de manejo de información que se utilizan en TCIT para el desarrollo y mantención de servicios tecnológicos.

Contexto

Agri es una aplicación cloud usada por agricolas de diferentes tamaños para hacer control de gestión en los principales procesos agrícolas y está disponible para todo el mundo, pero ha sido principalmente implementado en sudamérica. Nuestra plataforma permite que las agrícolas se concentren principalmente en la operación y estrategia mientras que Agri se preocupa de automatizar y digitalizar los principales procesos agrícolas y de todos los aspectos técnicos relativos al manejo de información, mantención de infraestructura tecnológica, mejoras de los procesos agrícolas e incorporación de mejores prácticas según van cambiando las necesidades de esta industria. Agri además aplica las mejores prácticas en el desarrollo y administración del sistema informático para que nuestro clientes pueden enfocarse en su negocio. Nuestra plataforma está diseñada para proteger a nuestros clientes de amenazas al aplicar controles de seguridad en cada capa de nuestro servicio informático, desde la capa física hasta la capa de aplicación, aislando a cada ambiente de Agri provisto a nuestros clientes y su información, y con nuestra habilidad de rápidamente poder desplegar mejoras de seguridad sin que sea necesario interactuar con nuestros usuarios ni interrumpir el servicio.

Compromiso para la confianza de Agri

"Nada es más importante para nuestra empresa que la privacidad de los datos de nuestros clientes" - Tomás Charad, Gerente General de TCIT.

La confianza es un principio nuclear en TCIT y Agri. Es este compromiso hacia la privacidad de nuestros clientes e inspiración de confianza lo que hace tomar decisiones en una base diaria. La confianza es responsabilidad de todos y cada uno de los empleados de TCIT y algo que nos tomamos muy seriamente.

Para saber más acerca de los esfuerzos de TCIT para proteger la privacidad de sus clientes y acciones que los clientes puedes hacer para proteger mejor sus datos por favor escriban a contacto@tcit.cl para saber acerca de las políticas de confianza y compliance de TCIT.

Evaluaciones de seguridad y compliance

Centros de datos

La infraestructura tecnológica de Agri reside y es administrada dentro de los seguros centros de datos de Amazon y usa la tecnología de Amazon Web Services (AWS). Amazon contínuamente administra el riesgo y se somete recurrentemente a evaluaciones para asegurar el cumplimiento con estándares de seguridad. Las operaciones de los centros de datos de Amazon han sido acreditados bajo:

1. ISO 27001
2. SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)

3. PCI Level 1
4. FISMA Moderate
5. Sarbanes-Oxley (SOX)

Tests de penetración y evaluaciones de vulnerabilidad

Pruebas de seguridad por terceros en la aplicación Agri son realizadas por empresas independientes y de alta reputación. Los resultados de cada evaluación son revisados por los asesores, rankeados por riesgos y asignados al equipo responsable.

Seguridad Física

Agri usa ISO 27001 y centros de datos administrados por Amazon certificados por FISMA. Amazon tiene muchos años de experiencia diseñando, construyendo y operando centros de datos de gran escala. Esta experiencia ha sido aplicada a la plataforma e infraestructura de AWS. Los centros de datos de AWS están alojados en instalaciones anodinas y las instalaciones más críticas tienen un amplio aislamiento y bermas de control con un perímetro de control de grado militar como también otras barreras naturales de protección. El acceso físico está estrictamente controlado en el perímetro y en los puntos de ingresos de la construcción por el personal de profesionales de la seguridad usando videos de vigilancia, sistemas de detección de intrusos de última generación y otros medios electrónicos. El personal autorizado y proveedores se les solicita mostrar identificación y son firmados y contínuamente escoltados por el personal autorizado.

Amazon solo provee acceso e información de sus centros de datos a sus empleados quienes tengan una necesidad de negocio legítima para tener aquellos privilegios. Cuando un empleado ya no tenga una necesidad de negocio para tener ese privilegio, su acceso es revocado automáticamente, incluso si ellos continúan siendo empleados de Amazon o Amazon Web Services. Todos los accesos de los empleados de Amazon a sus centros de datos, ya sea electrónico o físico es registrado y auditado contínuamente.

Para mayor información por favor revisar: https://aws.amazon.com/security

Salvaguardas ambientales

Detección y supresión de fuego

Detección y supresión de equipamiento de fuego ha sido instalado para reducir el riesgo. El sistema de detección de incendios usa sensores de detección de humo en todos los entornos de los centros de datos, espacio de infraestructura eléctrica y mecánica, piezas de enfriamiento y salas de equipos de generadores. Estas áreas son protegidas por canalización húmeda,

Poder

Los sistemas de poder de los centros de datos están diseñados para ser completamente redundantes y mantenibles sin impactar operaciones 24 horas al día, siete días a la semana. Unidades de fuentes de poder ininterrumpibles (UPS) proveen poder de respaldo en los eventos de una falla eléctrico para las cargas críticas o esenciales de las instalaciones. Los generadores de los centros de datos proveen un respaldo de poder de la instalación completa.

Control de clima y temperatura

Es necesario mantener un control de clima para proveer una temperatura constantemente operativa para los servidores y hardware, lo que previene el recalentamiento y reduce la posibilidad de cortes de servicio. Los centros de datos son acondicionados para mantener condiciones atmosféricas a niveles óptimos. El monitoreo de sistemas y el personal de los centros de datos aseguran que la humedad y temperatura estén en niveles apropiados.

Administración

Personal de los centros de datos monitorea sistemas de soporte eléctrico, mecánico y de vida para que los problemas sean inmediatamente identificados. Mantención preventiva es realizada para mantener la operación continuada del equipamiento.

Para mayor información por favor revisar: https://aws.amazon.com/security

Seguridad de redes

Cortafuegos

En Agri los cortafuegos son utilizados para restringir el acceso a los sistemas desde redes externas y entre los sistemas internamente. Por defecto todos los accesos son denegados y solo puertos y protocolos explícitamente permitidos son autorizados en base a las necesidades de negocio. Cada sistema es asignado a un grupo de seguridad de los cortafuegos basado en la función del sistema. Los grupos de seguridad restringen el acceso solo a los puertos y protocolos requeridos para una función específica del sistema para mitigar el riesgo.

Cortafuegos *host-based* restringen los ambientes de Agri de establecer conexiones localhost sobre la interfaz de red *loopback* para aislar aplicaciones de cliente. Los cortafuegos *host-based* también proveen la habilidad para limitar las conexiones de entrada y salida según se necesite.

Mitigación DDoS

Nuestra infraestructura provee técnicas de mitigación DDoS incluyendo cookies TCP Syn y restricción del ratio de conexión además de mantener múltiples conexiones de tipo backbone y ancho de banda interno con capacidad de exceder el ancho de banda del carrier de internet. Trabajamos muy de cerca con nuestros proveedores para responder rápidamente a los eventos y habilitar avanzadas técnicas de control de mitigación DDoS cuando lo necesitamos.

Protecciones spoofing (Suplantación de identidad) y sniffing

Firewalls administrados previenen IP, MAC y ARP spoofing en la red entre los host virtuales para asegurar que el spoofing no sea posible. El olfateo de paquetes es prevenido por infraestructura incluyendo el hypervisor el cual no permitirá el tráfico a una interfaz que no haya sido asignada. Agri usa aislamiento de aplicación, restricciones de sistema operativos y conexiones encriptadas para asegurar que el riesgo sea mitigado en todos sus niveles.

Escaneo de puertos

El escaneo de puertos está prohibido y todos nuestros ambientes son investigados por nuestro proveedor de infraestructura. Cuando un escaneo de puerto es detectado, estos son detenidos y el acceso es bloqueado.

Seguridad de la información

Ambientes

Cada ambiente en Agri corre su propio y aislado ambiente y no puede interactuar con otras aplicaciones o áreas del sistema a no ser de que sea explícitamente permitido. Este ambiente de operación restringido está diseñado para prevenir problemas de seguridad o estabilidad del servicio. Estos ambientes auto contenidos aíslan procesos, memoria y el sistema de archivos usando LXC mientras los cortafuegos *host-based* restringen los ambientes de establecer conexiones de red locales.

Base de datos PostgresSQL

Los datos de nuestros ambientes es guardado en una base de datos con control de accesos separado e independiente por cada aplicación. Cada base de datos solicita un único nombre de usuario y password que es solo válido para esa base de datos en específico y es único para cada aplicación. Los clientes que tengan más de un ambiente con nosotros les son asignadas bases de datos separadas por cada unidad administrativa y por ambiente para mitigar el riesgo de acceso no autorizado entre ambientes.

Las conexiones realizadas por nuestros ingenieros a las bases de datos requieren encriptamiento SSL para asegurar un alto nivel de seguridad y privacidad. Cuando desplegamos nuevas versiones, estos también se realizan mediante conexiones encriptadas a la base de datos.

Los clientes que lo soliciten pueden contar con una base de datos encriptada con encriptación a nivel de bloque de almacenaje AES-256. Las llaves son administradas por Amazon y las llaves de volumen individuales son estables durante la vida del ambiente. Agri no encripta nada a nivel de Postgres, si el cliente lo necesita, se pueden utilizar métodos a la medida para hacer encriptamiento.

Para mayor información acerca de encriptamiento de EBS por favor revisar aquí:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

Seguridad de sistemas

Configuración de sistema

La configuración de sistema y su consistencia es mantenida por imágenes actualizadas estándar, software de administración de configuración y por el reemplazo de sistemas con despliegues actualizados. Los sistemas son desplegados usando imágenes actualizadas que son actualizadas con cambios en la configuración y con actualizaciones de seguridad antes de los despliegues. Una vez realizado el despliegue, los sistemas son desmantelados y reemplazados por sistemas actualizados.

Aislamiento de ambientes

Los ambientes de Agri corren sobre su propio ambiente aislados y no pueden interactuar con otras aplicaciones o áreas del sistema (A no ser de que sea explícitamente definido) para prevenir problemas de seguridad y estabilidad. Estos ambientes auto contenidos aíslan procesos, memoria y el sistema de archivos mientras que los cortafuegos *host-based* restringen a las aplicaciones de establecer conexiones locales con la red.

Autenticación de los ambientes

El sistema operativo está limitado al equipo de ingenieros de Agri y requiere nombre de usuario y llave de autentificación. Los sistemas operativos no permiten autentificación por contraseña para prevenir ataques por fuerza bruta, robo o compartirlas.

Administración de vulnerabilidad

Nuestro proceso de vulnerabilidad está diseñado para remediar riesgos sin interacción con los clientes o impacto. Agri es notificado de sus vulnerabilidad por evaluaciones internas y externas, monitoreo de parches de los sistemas operativos y listas de correos y servicios provistas por terceros. Cada vulnerabilidad es revisada para determinar si aplica para el ecosistema de tecnología de Agri, ranqueado por riesgo y asignado al equipo respectivo para su resolución.

Los nuevos sistemas son desplegados con las últimas actualizaciones, mejoras de seguridad y cada configuración del ambiente de Agri es desmantelada cada vez que estas se despliegan a nuevas versiones de los sistemas operativos. Este proceso le permite a Agri mantener su ecosistema de tecnologías al día. Debido a que los ambientes corren aisladamente, ellos no son afectados por estas actualizaciones del núcleo de los sistemas operativos.

Para mitigar aún más el riesgo, cada tipo de componente es asignado a un grupo de seguridad único. Este grupo de seguridad está diseñado para solo ser accedido a puertos y protocolos que requieran un tipo de componente específico. Por ejemplo, los ambientes que corren en Agri no son capaces de acceder a la capa de administración del sistema o a los servicios de envío de correo automatizados, ya que cada uno está en su propio grupo de seguridad y el acceso no está permitido entre ellos.

Seguridad de aplicación de Agri

Realizamos tests de penetración, evaluaciones de vulnerabilidad y revisiones de código para asegurar la seguridad de nuestra aplicación, arquitectura e implementación. Nuestras evaluaciones de seguridad por terceros cubren todas las áreas de nuestra plataforma incluyendo las pruebas de los primeros 10 riesgos de seguridad de aplicaciones web definidas en OWASP y aislamiento de ambientes. Agri trabaja en conjunto con asesores de seguridad externos quienes revisan la seguridad del ecosistema de tecnologías de Agri y sus microservicios para aplicar mejores prácticas.

Los problemas encontrados en Agri son ranqueados por riesgo, priorizados y asignados al equipo responsable para su elaborar un plan de mitigación y el equipo de seguridad de Agri revisa cada plan de mitigación para asegurar una resolución apropiada.

Respaldos

Ambientes

Cada ambiente de Agri es automáticamente respaldado como parte del proceso de despliegue en un almacenaje seguro, controlado y redundante. Usamos respaldos para desplegar su ambiente en toda nuestra plataforma y para automáticamente estar denuevo en línea en el escenario de alguna interrupción del servicio.

Base de datos de cada ambiente

Protección continua mantiene los datos seguro en Agri. Cada cambio en sus datos es escrito en registros *write-ahead*, los que son entregados a un almacenamiento multi centro de datos, de alta durabilidad. En el poco

probable evento de una falla de hardware no recuperable, estos logs pueden ser automáticamente reproducidos para recuperar la base de datos en segundos desde su último estado desconocido. También respaldamos su base de datos periódicamente para cumplir con sus respaldos o con otras necesidades de retención de datos que usted necesite.

Configuración de ambiente y meta-información

La configuración y meta-información es respaldada cada minuto a la misma infraestructura de alta durabilidad, redundante que es usada para almacenar la información de su base de datos. Estos respaldos frecuentes permiten capturar cambios realizados a la versión de agri que corre bajo la configuración agregada después del despliegue inicial.

Plataforma de arquitectura

Desde nuestras imágenes de instancias hasta nuestras bases de datos, cada componente es respaldado a una unidad de almacenamiento segura, controlada por acceso y redundante. Nuestra plataforma permite recuperar bases de datos en segundos desde el último estado conocido, recuperar instancias de los sistemas desde templates estándar y hacer despliegue de datos y ambientes. Además de nuestras prácticas de respaldo regulares, la infraestructura de Agri está diseñada para escalar y ser tolerante a fallas a partir del reemplazo de instancias fallidas y reducir la probabilidad de necesitar de restaurar desde un respaldo de base de datos.

Plan de contingencia ante catástrofes

Ambientes y bases de datos

Nuestra plataforma restaura automáticamente ambientes de las bases de datos de nuestro ambientes en caso de falla. La plataforma de Agri está diseñada para dinámicamente desplegar aplicaciones en nuestro ambiente cloud, monitorear errores y recuperar componentes con problemas de nuestra plataforma incluyendo ambientes y bases de datos.

Plataforma de arquitectura

La plataforma de arquitectura de Agri está diseñada para estabilidad, escalamiento e inherentemente mitiga algunos problemas comunes que generen fallas manteniendo las capacidades de recuperamiento. Nuestra plataforma mantiene redundancia para prevenir puntos de falla únicos, está habilitada para reemplazar componentes con problemas y utiliza múltiples centros de datos diseñados para ser resilientes. En el caso de falla, la plataforma es desplegada en múltiples centros de datos usando las imágenes actuales de los sistemas y los datos restaurados desde los respaldos. Agri revisa los problemas de las plataformas para entender la causa raíz de los problemas, el impacto a los clientes y la mejora de la plataforma y procesos.

Retención de datos de clientes y destrucción

En Agri definimos los datos que son almacenados y tenemos la habilidad de purgar datos desde nuestras bases de datos para consentir con los requerimientos de mantención de datos que nos soliciten fuera de los estándares que solemos definir. Incluso cuando deprovisionemos su ambiente, mantenemos el volumen de almacenamiento de la base de datos por una semana, momento en el cual es automáticamente destruido dejando los datos irrecuperables

El decomisionamiento de hardware es administrado por nuestro proveedor de infraestructura usando un proceso diseñado para prevenir la exposición de datos de nuestros clientes. AWS usa técnicas descritas en DoD 5220.22-M o NIST 800-88 para la eliminación de datos.

Para información adicional por favor revisar: https://aws.amazon.com/security

Privacidad

Las políticas de privacidad de Agri aún están pendientes de elaboración.

Acceso a datos de clientes

El personal de Agri no accede o interactúa con los datos de clientes o de aplicaciones como parte de su operación regular. Pueden haber casos en los que a Agri le sea solicitado interactuar con los datos de clientes o de aplicaciones por solicitud de algún cliente, por fines de soporte o por requerimientos de la ley. Los datos de los clientes están controlados por acceso y todos los accesos por el personal de Agri es seguido de la aprobación de sus clientes o por mandato del gobierno.

Evaluación de empleados y políticas

Como condición para trabajar en TCIT y Agri tienen revisiones de su carrera y contexto profesional y aceptan las políticas de la empresa incluyendo seguridad y acuerdos de confidencialidad.

Mejores prácticas de seguridad

Encriptamiento de datos en tránsito

Todos los ambientes productivos de agri tienen habilitado HTTPS para sus ambientes y conexiones SSL para las bases de datos para proteger datos sensibles transmitidos desde y hacia las aplicaciones.
Enable HTTPS for applications and SSL database connections to protect sensitive data transmitted to and from applications.

Encriptamiento de datos sensibles en reposo

Los clientes con datos sensibles pueden solicitar encriptar sus datos en sus bases de datos para cumplir con requerimientos de seguridad de información. La encriptación de datos puede será desplegada usando los mejores estándares de encriptación.

Prácticas de desarrollo seguras

En Agri aplicamos las mejores prácticas para mitigar vulnerabilidad como las expuestas en los primeros 10 riesgos de seguridad de aplicaciones web definidas en OWASP.

Autentificación

Para prevenir accesos no autorizados usamos credenciales fuertes para las cuentas de Agri como también nuestras llaves SSH para comunicarnos con nuestros servicios en la nube. Guardamos además claves SSH seguramente para prevenir exposición de datos y reemplazamos las llaves si son perdidas o expuestas. Por último usamos el modelo de acceso RBAC para permitir agregar nuevos miembros al equipo de desarrollo.

Registros

Los registros son críticos para resolver problemas e investigar errores. Contamos con las tres opciones principales para interactuar con nuestros sistemas de arquitectura, aplicaciones y logs. Podemos recibir los tres tipos de logs vía syslog desde la plataforma de arquitectura de Agri, elegir enviar estos registros a fuentes externas si se nos fuera requerido o interactuar con estos registros en tiempo real a través de nuestra plataforma de arquitectura.