Documentación técnica de seguridad de Hach Claros

Descripción general ejecutiva

Claros, the Water Intelligence System de Hach®, está diseñado para permitir a las organizaciones del sector del agua transformar los datos del laboratorio y los procesos en información práctica para lograr mejores resultados empresariales. Claros integra las soluciones Instrument Management, Data Management y Process Management de Hach en una única plataforma. Hach es consciente de que ayudar a proteger los datos de nuestros clientes, garantizar el cumplimiento de las mejores prácticas de seguridad y mitigar los riesgos potenciales es esencial para generar confianza y ofrecer un elevado nivel de servicio. Hach asume un enfoque de seguridad basado en el riesgo, y en este artículo se detallan las medidas y tecnologías que usa Claros para proteger los datos de nuestros clientes.

Este documento describe cómo Claros aborda los objetivos fundamentales de información segura: confidencialidad, integridad y disponibilidad, así como el enfoque de Hach con respecto a la arquitectura de la seguridad y las responsabilidades de nuestros clientes. Dentro de este contexto de seguridad, definimos la confidencialidad como el conjunto de reglas que controlan el acceso a la información; la integridad como medio para la información precisa y de confianza; y la disponibilidad como el acceso fiable a la información por parte de los usuarios autorizados.

Consulte el siguiente apéndice sobre los temas que trataremos en el presente documento:

Enfoque de Hach

Defensa en profundidad (Defense-in-Depth)

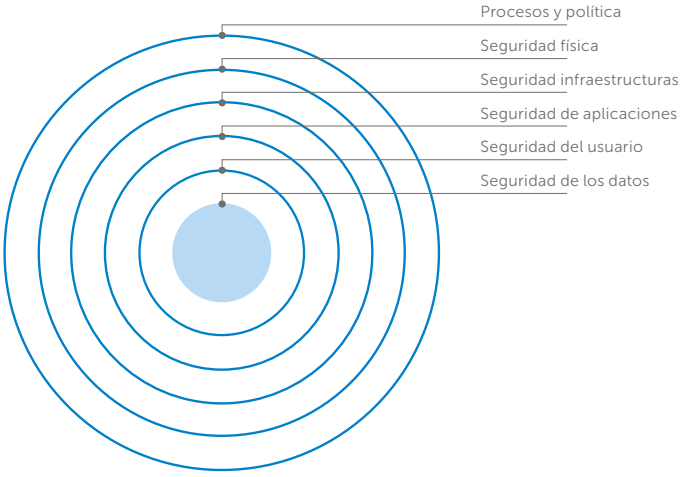
En Claros no hay un nivel único de protección de los datos de los clientes, sino una solución con una arquitectura sólidamente diseñada que tiene en cuenta cada nivel, desde las medidas de seguridad físicas del centro de datos, hasta los privilegios de acceso que determinan los datos a los que puede acceder un usuario individual. Hach utiliza esta estrategia de seguridad basada en varios niveles para proteger los datos del cliente.

La defensa en profundidad (Defense-in-Depth) consiste en el uso coordinado de varias contramedidas de seguridad para proteger la integridad de los activos de información de una empresa. La estrategia se basa en el principio militar de que es más difícil para un enemigo eludir un complejo sistema de defensa de varios niveles que penetrar una única barrera.

-TechTarget

Procesos y política

El primer nivel de defensa consiste en tener un conjunto de procesos y políticas de seguridad amplio y bien definido para garantizar la seguridad de los datos de nuestros clientes y usuarios. El sistema de gestión de seguridad de la información (ISMS, por sus siglas en inglés) de Hach utiliza diversas medidas para los procesos y las políticas que garantizan que la seguridad sea una prioridad esencial, empezando por nuestro personal.



Formación

Los empleados de Hach están autorizados para acceder a formación continua de Claros que les permite cumplir con las políticas de seguridad corporativa de Hach. Por ejemplo, el personal de Hach Development Operations, Research & Development, y Technical Support and Services, que puede gestionar información y datos confidenciales de los clientes, se somete a una formación continua de concienciación sobre seguridad y cumplimiento para reconocer amenazas de seguridad patentes y emergentes.

Acceso autorizado

Además de restringir al personal la entrada al área de producción, el acceso operativo a Claros se limita a solo un grupo reducido de empleados de Hach Development Operations. El acceso se controla a través de la red corporativa de Hach, que garantiza que solo el personal autorizado pueda acceder a los datos. Todo el personal de Hach con acceso físico u operativo a entornos de producción recibe formación, y todas las actividades se registran con fines de auditoría.

Control de cambios

El proceso formal de control de cambios de Hach reduce al mínimo el riesgo asociado con los cambios y las actualizaciones de Claros. Este proceso permite el seguimiento de los cambios realizados en Claros y verifica que se ha efectuado una evaluación de los riesgos, se han examinado las interdependencias y se han tenido en cuenta y aplicado las políticas y procedimientos necesarios antes de autorizar ningún cambio. Hach registra todos los cambios en las notas de actualización, que se distribuyen a los clientes antes de cualquier cambio o actualización del sistema.

Endurecimiento de los sistemas

Claros utiliza muchas tecnologías para ofrecer nuestro servicio, pero puede haber diversas funciones que no son necesarias. De conformidad con las prácticas recomendadas del sector, Claros Development Operations lleva a cabo una completa inspección de toda la solución para identificar servicios innecesarios y eliminar o deshabilitar estas funciones con el fin de reducir las vulnerabilidades a las amenazas de seguridad.

Pruebas de penetración y análisis de vulnerabilidad periódicos

De acuerdo con las políticas internas y las normas sobre ciberseguridad internacional, Hach realiza pruebas periódicas de vulnerabilidad y penetración que cubren fallos de seguridad importantes, incluidos los 10 principales de OWASP, para estar un paso por delante de las amenazas de seguridad.

Parches de seguridad

Hach dispone de políticas y procedimientos rigurosos para actualizar todos los componentes de Claros, incluidos sistemas operativos, hipervisores de VM (máquinas virtuales), middleware, bases de datos, aplicaciones móviles, etc. con los parches de seguridad del vendedor. Estas actividades relativas a los parches de seguridad están sujetas a auditorías sobre el ciclo de vida del desarrollo seguro de productos IEC62443-4-1, así como a rigurosas normas.

Confidencialidad

Autenticación

La organización de Claros se basa en un marco de seguridad de autenticación y autorización centralizadas para controlar el acceso al servicio y los dispositivos de campo. Este marco de seguridad permite imponer el cumplimiento de las políticas de seguridad al solicitar algoritmos de robustez de contraseña para establecer la longitud y complejidad mínimas de contraseña.

Cifrado en tránsito

El tráfico de entrada y salida de Claros se encuentra cifrado para proporcionar seguridad en las comunicaciones. Este cifrado utiliza un protocolo TLS/SSL (Transport Layer Security/ Secure Sockets Layer) que aprovecha el algoritmo SHA-2 (Secure Hash Algorithm 2) o el algoritmo AES (Advanced Encryption Standard). Esto significa que todos los datos que entren o salgan por alguno de los puntos finales de confianza estarán siempre cifrados en su recorrido por Internet.

Cifrado de datos almacenados

Como nos tomamos en serio la protección de los datos de nuestros clientes, todos los datos de Claros se almacenan en los servidores de Microsoft Azure y se cifran mediante el cifrado AES de 256 bits.

Integridad

Acceso controlado y basado en funciones

El acceso del cliente a Claros se controla a través de interfaces de usuario (IU), API (Interfaz de programación de aplicaciones) y herramientas específicas. El uso de cualquiera de estos métodos de acceso requiere un nombre de usuario y contraseña con los privilegios adecuados para el acceso solicitado. Los administradores de cuenta de Claros utilizan el Control de acceso basado en funciones (Role Based Access Control, RBAC) para hacer cumplir los permisos apropiados en toda la infraestructura de Claros. Los clientes no tienen acceso raíz ni administrativo a la capa física de Claros y el acceso se permite a través de la capa de aplicación de Claros (IU o API).

Acceso a la aplicación

Puede accederse a los datos de cliente a través de la aplicación Claros. Tanto si este acceso es a través de las interfaces de usuario como a través de las API disponibles, el RBAC se encarga de regular el acceso a los datos de los clientes para que solo puedan acceder los usuarios y el personal autorizados. De este modo, Claros no proporciona acceso directo a ninguna base de datos. Este enfoque evita que servicios o sistemas no autorizados recuperen o modifiquen de forma accidental o malintencionada los datos de los clientes.

Comunicación

Los dispositivos de campo inician la comunicación con Claros, de forma que el cliente pueda hacer un seguimiento de los intentos de comunicación desde su red al mundo exterior y añadir medidas de seguridad adicionales a su red circundante. Cada intento de comunicación desde los dispositivos de campo y hacia ellos relacionado con datos de Claros se somete a una verificación de autenticidad.

Cortafuegos

Todo acceso a la red hacia y desde los dispositivos de campo está protegido por un cortafuegos de varias capas que funciona en modo de denegación por defecto (deny-all). El acceso a Internet solo se permite en puertos abiertos explícitamente para un subconjunto de hosts virtuales específicos. Para ofrecer una capa de seguridad adicional, todos los servidores de bases de datos están protegidos por un cortafuegos adicional.

Puertos y servicios innecesarios

Los puertos y servicios de cualquier servidor y dispositivo de campo que no sean necesarios para el funcionamiento de Claros están desactivados, lo que reduce las posibilidades de intrusión. Para utilizar Claros, solo es preciso abrir un número reducido de puertos y puntos finales en la red del cliente. La siguiente tabla proporciona una descripción de los puertos y servicios que utiliza Claros:

Puerto	Dirección	Servicio	Finalidad
1194 (UDP)	Salida	VPN	Acceso remoto para un técnico de servicio de Hach
5671 (TCP)	Salida	AMQPS	Enviar/recibir mensajes a/de Claros
123 (UDP)	Entrada/salida	NTP	Recibir hora y fecha actuales desde un servidor de horario externo
80 (TCP)	Salida	HTTP	Actualizaciones de firmware cifradas y firmadas del repositorio
443 (TCP)	Salida	HTTPS	Acceder a la IU de Claros

Disponibilidad

Microsoft Azure

Claros aprovecha la computación en la nube de Microsoft Azure para ofrecer sus servicios, por lo que todos los clientes de Claros se benefician del Acuerdo de nivel de servicio (Service Level Agreement, SLA) de Microsoft Azure, que se compromete a un tiempo de disponibilidad del 99,95 % o superior en los principales servicios de Azure.

Infraestructura

La infraestructura que da apoyo a nuestra solución se encuentra entre el nivel del centro de datos físicos y el nivel de la aplicación de Claros. La seguridad se implanta de un modo completo y coordinado por toda la infraestructura para mejorar la seguridad de los datos del cliente.

Cumplimiento normativo

Para ayudar a nuestros clientes a cumplir los requisitos específicos nacionales, regionales y sectoriales que regulan la recopilación y el uso de datos individuales, Microsoft Azure proporciona el conjunto de ofertas de cumplimiento más completo de cualquier proveedor de referencia de servicios en la nube.

Todos los centros de datos de Microsoft Azure cuentan con las principales certificaciones de normativa de seguridad de la información, enumeradas en la siguiente tabla:

CDSA	Azure dispone del certificado Content Delivery and Security Assoc. Protección de contenido y seguridad estándar.
Certificación CSA STAR	Azure e Intune recibieron la certificación de Cloud Security Alliance STAR basada en una auditoría independiente.
GxP (Buenas prácticas clínicas, de laboratorio y de fabricación)	Los servicios en la nube de Microsoft se adhieren a las buenas prácticas clínicas, de laboratorio y de produccción (GxP).
ISO 9001	Microsoft tiene certificación por su implantación de estos estándares de gestión de calidad.
ISO 20000-1:2011	Microsoft tiene certificación por su implantación de estos estándares de gestión de servicios.
ISO 22301	Microsoft tiene certificación por su implantación de estos estándares de gestión de continuidad empresarial.
ISO 27001	Microsoft tiene certificación por su implantación de estos estándares de gestión de la seguridad de la información.
ISO 27017	Los servicios de Microsoft en la nube han implementado este código de prácticas para los controles de seguridad de la información.
ISO 27018	Microsoft fue el primer proveedor de servicios en la nube que se adhirió a este código de prácticas para la privacidad en la nube.
MPAA	Azure completó satisfactoriamente una evaluación oficial de la Motion Picture Association of America.
Evaluaciones compartidas	Microsoft demuestra la alineación de Azure con este programa a través de la versión 3.0.1 de CSA CCM.
SOC 1	Los servicios en la nube de Microsoft cumplen con las normas sobre controles en la organización de servicios para la seguridad operacional.
SOC 2	Los servicios en la nube de Microsoft cumplen con las normas sobre controles en la organización de servicios para la seguridad operacional.
SOC 3	Los servicios en la nube de Microsoft cumplen con las normas sobre controles en la organización de servicios para la seguridad operacional.
WCAG 2.0	Los servicios en la nube de Microsoft cumplen con Web Content Accessibility Guidelines 2.0.

Implantaciones regionales

Microsoft Azure tiene más regiones globales que ningún otro proveedor de la nube, lo que ofrece la adaptabilidad necesaria para hacer llegar las aplicaciones de Claros a los usuarios de todo el mundo, preservando la conservación de datos y ofreciendo opciones de cumplimiento y resiliencia flexibles para los clientes. Para ayudar a los clientes a conservar la propiedad de sus datos y cumplir las normativas regionales, Hach utiliza los centros de datos de Microsoft Azure para clientes en sus regiones o lo más cerca posible.

50 Regiones en el mundo **140** Disponible en 140 países

Fuente: Microsoft

Todos estos centros de datos también incorporan sistemas de climatización en configuración redundante N+1 y sistemas de alimentación ininterrumpida (SAI).

La seguridad física sigue las mejores prácticas del sector e incluye:

- Protocolos de tarjetas de acceso, protocolos de análisis biométricos y vigilancia interior y exterior ininterrumpida
- Acceso limitado al personal del centro de datos autorizado: nadie puede acceder a la zona de producción sin autorización previa ni sin un acompañante adecuado
- Todos los empleados del centro de datos se someten a controles de seguridad exhaustivos

Responsabilidades del cliente

Acceso y configuración controlado

Para que Hach pueda mantener los datos seguros, esperamos que nuestros clientes respeten también las normas de seguridad. Hach confía en nuestros clientes para garantizar que cada cuenta de Claros esté configurada con los permisos y el acceso único adecuado para cada usuario. Es responsabilidad de cada cliente identificar quién tiene acceso administrativo dentro de la planta y quién gestiona las cuentas con el tiempo.

Protección física

Los clientes son responsables de la protección física de sus instrumentos de Hach y la infraestructura de seguridad. Cada planta es responsable del acceso controlado a la planta, los instrumentos de Hach pertinentes (por ejemplo, controladores y sensores) y las redes de comunicaciones.

Conectividad

La conectividad de los instrumentos de Hach con Claros en cada ubicación del cliente es responsabilidad del cliente. Para que Claros trabaje de forma eficaz, la instrumentación normalmente necesita conexión de móvil o de red que el cliente debe mantener y proteger lo suficiente.

DOC180.61.10159.July20