HONEYWELL CONNECTED LIFE SAFETY SERVICES

CIBERSEGURIDAD

Versión:1.0

Honeywell

ÍNDICE

ACERCA DE ESTE DOCUMENTO

Este documento está dirigido principalmente a losclientes, integradores de sistemas y técnicos de Connected Life Safety Services (CLSS) de Honeywell que estén interesados en
comprender el enfoque adoptado por Honeywell para asegurar la solución CLSS. Este documento también proporciona detalles sobre la arquitectura de seguridad, los procedimientos y los controles de seguridad que describen cómo configurar la pasarela CLSS de forma segura en la instalación.

Descargo de responsabilidad:

El material contenido en este documento tiene carácter meramente informativo. El contenido y el producto descrito están sujetos a cambios sin previo aviso.
Honeywell no ofrece declaraciones ni garantías con respecto a este documento. En ningún caso Honeywell será responsable por omisiones o errores técnicos o editoriales en este documento, ni será responsable por ningún daño, directo o incidental, que surja o esté relacionado con el uso de este documento. Queda prohibida la reproducción total o parcial de este documento, en cualquier forma o por cualquier medio, sin la autorización previa por escrito de Honeywell.

INTRODUCCIÓN A CLSS

CLSS es una innovadora plataforma en la nube todo en uno que permite a los integradores de sistemas y gestores de instalaciones ofrecer un servicio de seguridad contra incendios mejorado, al tiempo que maximizar la eficiencia de rendimiento que ofrecen los fiables sistemas de detección y alarma de Honeywell.

PASARELA CLSS

La pasarela CLSS sirve de puente entre la central de alarmas contra incendios y la plataforma CLSS en la nube. Proporciona una forma de conectar de forma segura la central de alarmas contra incendios local a la nube, y proporciona una ruta única desde el sitio a la nube que garantiza que todos los servicios y aplicaciones en la nube de CLSS utilicen el mismo método auditado y supervisado para acceder a la red de control de alarmas contra incendios local.

CLSS WEB APP (GESTOR DE SITIOS)

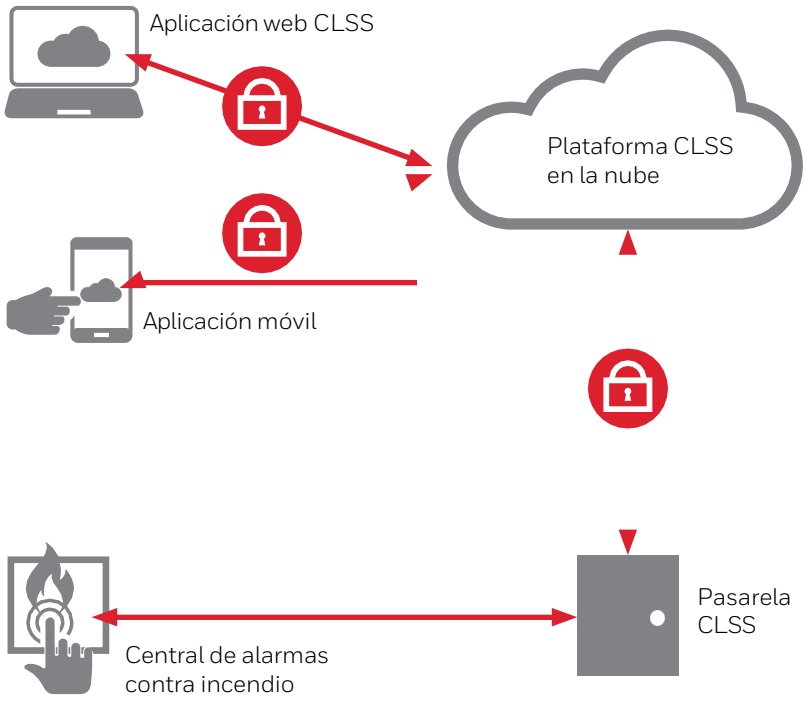
CLSS Site manager (Gestor de sitios) es una aplicación web que utilizan instaladores/mantenedores de sistemas y los técnicos para realizar actividades administrativas y de gestión de back-office. Proporciona una visión consolidada de los sistemas de sus clientes. Permite a los instaladores dar de alta los edificios de sus clientes, sus usuarios y técnicos, así como configurar los privilegios de acceso de sus técnicos.

APLICACIÓN MÓVIL CLSS

Los técnicos utilizan la aplicación móvil de CLSS para configurar la pasarela durante la instalación y realizar pruebas de funcionamiento periódicas de los dispositivos conectados y no conectados. La aplicación también se utiliza para generar informes de conformidad.

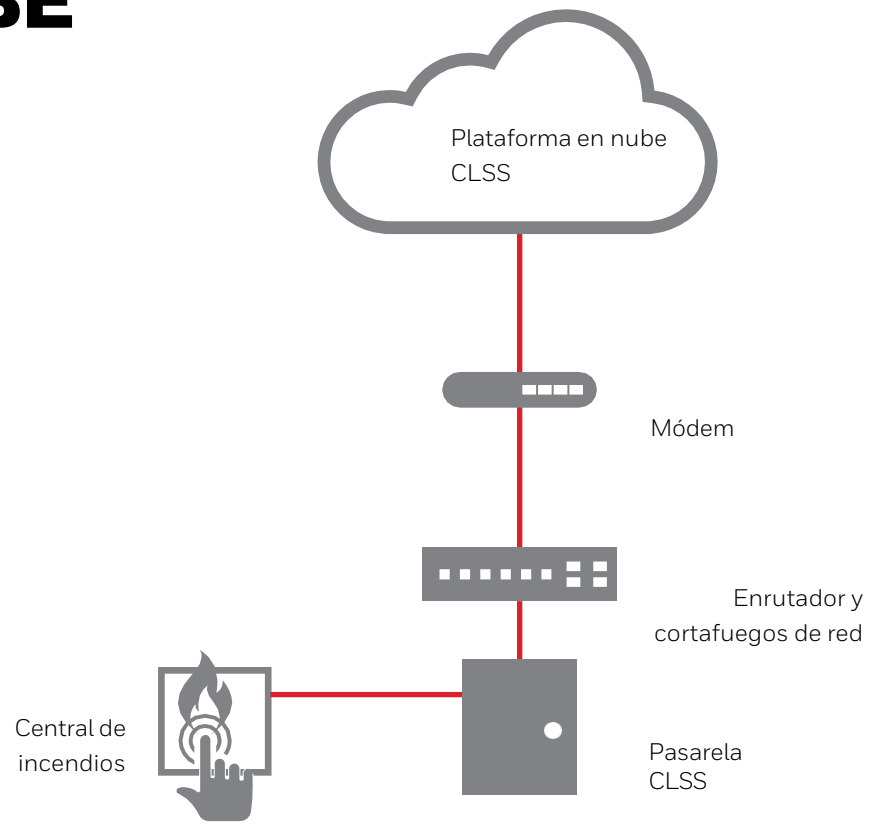
PLATAFORMA EN NUBE CLSS

La plataforma CLSS Cloud contiene varios microservicios para dar soporte a las funcionalidades de la pasarela CLSS, la aplicación móvil y la aplicación web. Es segura, escalable, basada en estándares y construida sobre la plataforma de gestión empresarial Honeywell Forge.

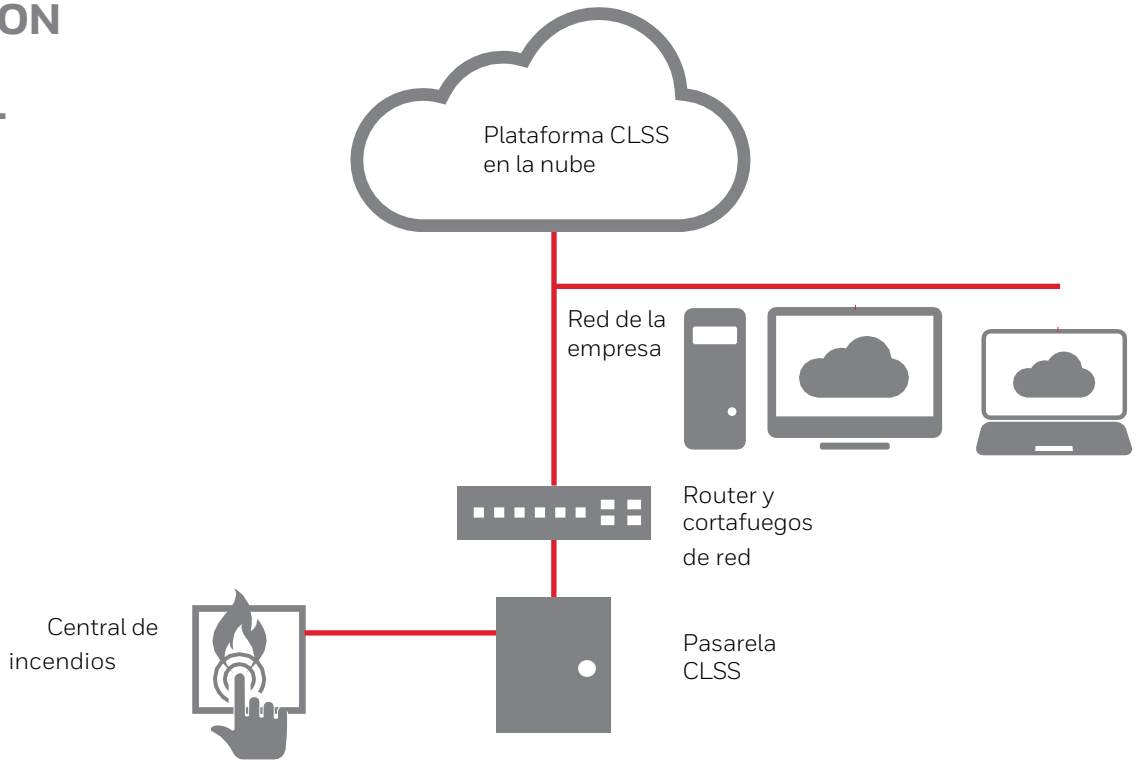


CONEXIÓN DE LA PASARELA CLSS A LA NUBE

ENFOQUE 1 CON MÓDEM



ENFOQUE 2 CON RED EMPRESARIAL



QUÉ DATOS SE TRANSMITEN DESDE EL SISTEMA IN SITU ¿A LA NUBE?

Para lograr los casos de uso de las funcionalidades de la aplicación móvil y la aplicación web de CLSS (gestor de inspecciones y gestor de obras), se transmiten a la nube los siguientes datos de la pasarela in situ:

- Inventario de dispositivos recibido de la central de incendios
- Eventos, alarmas y problemas recibidos de la central de incendios
- Eventos, alarmas y problemas generados por la puerta de enlace
- Registros de inspección de la pasarela con marca de tiempo.

El inventario de dispositivos contiene todos los dispositivos (por ejemplo, detectores, módulos), incluida la central de incendios, conectados a la red del sistema de alarma de incendios.

ASEGURAR LA TRANSMISIÓN DE DATOS

Para gestionar la superficie del sistema desde el punto de vista de la seguridad, el conector en la nube de la pasarela CLSS sólo realiza llamadas salientes y no se acepta ninguna comunicación entrante. Las conexiones salientes realizadas se limitan a HTTPS para iniciar la comunicación y, a continuación, AMQP sobre HTTPS para la mensajería con cifrado TLS1.2 y superior. AMQP es un protocolo de mensajería estándar de OASIS diseñado para una mensajería fiable y robusta que se adapta bien a escenarios en los que se requiere la confirmación de comandos y la transferencia de datos.

La autenticación basada en certificados se utiliza entre la pasarela local y la plataforma en la nube CLSS.

NECESIDADES DE INFRAESTRUCTURA PARA LA TRANSMISIÓN DE DATOS

La conexión a la nube desde la pasarela local puede lograrse utilizando dispositivos de seguridad estándar. La pasarela CLSS utiliza únicamente comunicación saliente con cifrado HTTPS/TLS. Los requisitos detallados son:

Puerto de entrada (Inbound): Un puerto de entrada es un puerto que otro ordenador utiliza para conectarse a la pasarela para acceder a la funcionalidad de la pasarela; es decir, una aplicación

en la pasarela estará escuchando activamente en este puerto para conexiones de clientes.

Puerto de salida (Outbound): La pasarela utiliza puertos de salida para conectarse a la plataforma de Internet/CLSS Cloud; es decir, los servicios en la nube estarán a la escucha en estos puertos esperando una conexión desde la pasarela.

Por defecto, bloquea todas las conexiones entrantes y salientes y sólo permite los puertos listados en la siguiente tabla:

NÚMERO DE PUERTO	TIPO	ENTRADA / SALIDA	OBJETIVO / OBSERVACIONES
443	TCP	En	Comunicación https a la plataforma en nube CLSS
53	UDP	En	Búsqueda de cliente a servidor DNS
2020	TCP	En	Transmisión de alarmas

A continuación se muestra la lista de puntos finales para comunicarse con la plataforma CLSS Cloud:

REGIÓN	TODOS LOS PUNTOS FINALES
Global	https://gaprodpkisystemauthenticationv2.sentience.honeywell.com/ https://gaprodregui.sentience.honeywell.com/ https://sentgaprod.blob.core.windows.net
Europa	https://t02aprodfileupload.sentience.honeywell.com/ https://sentt02aprodfu.blob.core.windows.net https://sentt02aprodv2.azure-devices.net/ https://t02aprodcloudapp.sentience.honeywel.com
US	https://t01aprodfileupload.sentience.honeywell.com/ https://sentt01aprodfu.blob.core.windows.net https://sentt01aprodv2.azure-devices.net/ https://t01aprodcloudapp.sentience.honeywell.com
Transmisión US-Alarm	https://honprodeast.rrmsalarm.com https://honprodwest.rrmsalarm.com

ARRANQUE SEGURO Y ACTUALIZACIÓN SEGURA DEL FIRMWARE

El arranque seguro es el proceso de validar la firma del firmware antes de ejecutarlo. La **actualización segura del firmware es** el proceso de validación del nuevo firmware antes de sustituir la versión que se está ejecutando. La **firma de firmware es** un proceso de cálculo de la firma digital del firmware durante la compilación del firmware y garantizar que no pueda alterarse sin ser detectado.

Honeywell publica periódicamente revisiones de seguridad y paquetes de actualización del firmware de la pasarela. Los paquetes liberados están cifrados y firmados digitalmente por Honeywell para garantizar la confidencialidad, integridad y autenticidad (es decir, el paquete
procedente de Honeywell) del paquete liberado. La pasarela verifica la firma durante los procesos de arranque seguro y actualización de firmware.

Los datos confidenciales, como la(s) clave(s) privada(s) del dispositivo, se gestionan mediante chips de seguridad de acuerdo con las prácticas y recomendaciones del sector de la seguridad comúnmente aceptadas.

APLICACIÓN MÓVIL CLSS Y PLATAFORMA EN LA NUBE

APLICACIÓN MÓVIL CLSS

Comunicación entre el móvil y la nube
Todas las comunicaciones procedentes del teléfono móvil a la plataforma en la nube CLSS se realizan a través de HTTPS con túnel cifrado TLS 1.2.

Comunicación entre el móvil y la pasarela
Aplicación móvil utilizada a través de una conexión BLE Link segura con la pasarela CLSS para la configuración de la pasarela. La conexión BLE sólo funciona cuando el usuario está cerca de la pasarela. Las claves de seguridad necesarias para emparejarse con la pasarela CLSS solo son accesibles para técnicos autorizados a través de la plataforma en la nube.

Datos almacenados e intercambiados a través de la aplicación móvil CLSS
La aplicación móvil intercambia datos con la plataforma CLSS en la nube para la configuración de la pasarela, para casos de uso de gestión de inspecciones. Los datos no se mantienen en el dispositivo móvil de forma permanente. Es sólo para uso temporal y los detalles se borran de la base de datos de la memoria de la aplicación cuando los datos se sincronizan con la nube.

PLATAFORMA EN LA NUBE CLSS

La implantación basada en la nube se gestiona de acuerdo con el marco de cumplimiento unificado de Honeywell, que está alineado con los principales estándares de la industria.

Marcos de seguridad de TI, incluidos

NIST SP 800-171 e ISO 27001.

Comunicación de datos dentro de la nube Todas las comunicaciones internas entre varios servicios en la nube utilizar HTTPS para la integridad y confidencialidad dentro de la nube.

Medidas de seguridad de la infraestructura en la nube

- En las aplicaciones móviles y web se utiliza una autenticación fuerte basada en contraseña e inicio de sesión.
- Aplicación de autorizaciones basadas en roles para acceder a diferentes datos.
- El cortafuegos en la seguridad perimetral se garantiza mediante IPS/IDS e inspección de paquetes.
- WAF (Web Application Firewall) está activado para las aplicaciones CLSS. Los WAF ofrecen protección contra ciberataques como inyecciones SQL, cross-site Scripting, carga de malware, DDoS de aplicaciones, etc.
- Los datos confidenciales, como los tokens de seguridad y las claves criptográficas, se gestionan a través de **Azure key** vault. Azure key vault proporciona módulos de seguridad de hardware (HSM) validados por FIPS 140-2 nivel 2 para almacenar los datos confidenciales.
- El refuerzo de la seguridad de todos los servidores se segmenta mediante redes virtuales y servidores virtuales

  Todas las máquinas virtuales en nube de CLSS están protegidas con antimalware.
- Proceso estándar para aplicar parches de seguridad periódicamente con disposiciones para agilizar la aplicación en función del riesgo.
- A nivel de aplicación, la autenticación y autorización sólidas se utilizan para restringir el acceso a cualquiera de los datos de la aplicación.
- El acceso a nivel de administrador del sistema está restringido al equipo de operaciones autorizado de Honeywell Digital. Copias de seguridad periódicas para restaurar el sistema a su estado normal en caso de pérdida accidental. En reposo, todos los datos se cifran mediante SSE (cifrado de estado sólido).
- La plataforma en la nube CLSS utiliza Honeywell Forge y está alojada en Microsoft Azure Cloud. La plataforma Honeywell Forge está auditada bajo SOC2 Tipo 1. Microsoft Azure Cloud está certificada con: SOC1 Tipo2, SOC2 Tipo2, ISO27001. Para consultar la lista completa, visite **aquí**.

DATOS PERSONALES

Los inicios de sesión y las contraseñas, así como otros datos personales, se gestionan en Active directory de forma encriptada. Los datos personales están protegidos de acuerdo con la normativa RGPD y los estándares de privacidad de Honeywell. Honeywell limita los datos personales que recopila y procesa al mínimo necesario para servir a un fin comercial legítimo.

CIBERSEGURIDAD EN EL DESARROLLO DE PRODUCTOS

Todo software debe incorporar las mejores prácticas de ciberseguridad y privacidad para minimizar los problemas de ciberseguridad que puedan surgir. Por eso creemos que hay que incluir la seguridad y la privacidad cuando se inicia el proceso de desarrollo del producto.

Los productos de Honeywell Building Technologies se someten a estrictas revisiones y pruebas de seguridad antes de ser aprobados para su comercialización, independientemente de dónde se fabriquen. Nuestros productos son

evaluados con arreglo a nuestras normas cibernéticas y requieren la aprobación de nuestro director técnico como parte de nuestro proceso estándar de introducción de nuevos productos.

Honeywell sigue el marco Building Security In Maturity Model (BSIMM) y garantiza normas y requisitos de ciclo de vida de desarrollo seguro para los productos.

La plataforma CLSS integra consideraciones de seguridad en todos los aspectos del desarrollo, la implantación y la gestión de riesgos. El sistema se desarrolló utilizando el ciclo de vida de desarrollo de software seguro (SSDLC) de Honeywell, que integra consideraciones de seguridad en

todas las etapas, desde los requisitos hasta el despliegue de pruebas y las operaciones en curso. El desarrollo de sistemas abarca todos los aspectos, desde la derivación de requisitos a partir de las normas ANSI/ISA 62443 y las mejores prácticas, la arquitectura y el diseño seguros mediante el análisis de riesgos arquitectónicos, el modelado de amenazas, las directrices de codificación segura y el análisis estático y dinámico del código, hasta las pruebas de seguridad mediante enfoques manuales y automatizados.

Toda la plataforma CLSS está desarrollada por Honeywell y el código fuente se gestiona según las políticas de gestión de código fuente de Honeywell. Se realizan revisiones del código para detectar lagunas de seguridad en el código fuente.

Las bibliotecas de código abierto utilizadas en el producto han pasado el control de seguridad

según la práctica estándar de Honeywell. Las herramientas de análisis estático de código y de exploración binaria están integradas en el proceso CI/CD (integración continua/entrega continua).

ejecutado cuando se genera cada compilación. Los riesgos de seguridad se registran en

herramientas JIRA con puntuación CVSS y reparación según planes acordados con arreglo a un calendario obligatorio basado en la gravedad.

Pruebas de penetración y eventos de inicio de pruebas

Las pruebas de penetración se realizan antes de cualquier lanzamiento importante y antes del despliegue de una nueva versión de los servicios en la nube en el entorno de producción. El equipo realiza pruebas de penetración en aplicaciones basadas en

vulnerabilidades y se volverán a probar después de la mitigación para verificar las correcciones. Los hallazgos se registran y se realiza un seguimiento para su cierre.

Las aplicaciones del producto se evalúan de acuerdo con la última guía de pruebas OWASP y la infraestructura subyacente del producto se evalúa según las directrices NIST 800-115.

SOPORTE DE HONEYWELL Y PROCESO DEVOPS

Todo el sistema de producción está gestionado por un equipo de asistencia 24/7 que supervisa tanto la infraestructura como las aplicaciones. Existen políticas internas detalladas que cubren cómo detectamos, investigamos y respondemos a los incidentes de seguridad y privacidad.

Honeywell utiliza varias herramientas de diagnóstico de aplicaciones para diferentes partes del sistema con el fin de supervisar los parámetros de salud del sistema. Mantenemos

seguimiento de la salud del sistema (por ejemplo, uso de CPU, uso de memoria, operaciones de E/S de disco) y cualquier desviación activaría una alerta.

CÓMO NOTIFICAR UNA VULNERABILIDAD DE SEGURIDAD

Honeywell cuenta con un equipo de respuesta a incidentes de seguridad de productos (PSIRT) para supervisar

y gestionar los incidentes y minimizar el riesgo de los clientes asociado a las vulnerabilidades de seguridad proporcionando información, orientación y soluciones oportunas a las vulnerabilidades de nuestros productos.

Haga clic **aquí** para obtener más información sobre el proceso PSIRT de Honeywell. Para informar de una posible vulnerabilidad de seguridad contra cualquier producto Honeywell, siga las instrucciones **aquí**.

Honeywell Fire
C/Pau Vila 15-19
08911 Badalona
(Barcelona) Spain
+34 932 715 570
www.honeywelllifesafety.es

HW_WP_CLSSCyberSec_ES | Rev 01 | 03/2023
2023 Honeywell International Inc.

THE FUTURE IS WHAT WE MAKE IT

Honeywell