centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1007

Procedimiento de Empleo Seguro
Proactivanet SaaS



Noviembre 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 3
2 OBJETO Y ALCANCE 3
3 ORGANIZACIÓN DEL DOCUMENTO 3
4 FASE PREVIA A LA INSTALACIÓN 4
4.1 ENTREGA SEGURA DEL PRODUCTO 4
4.2 ENTORNO DE INSTALACIÓN SEGURO 4
4.3 REGISTRO Y LICENCIAS 4
4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN 4
5 FASE DE INSTALACIÓN 6
6 FASE DE CONFIGURACIÓN 7
6.1 AUTENTICACIÓN 7
6.2 ADMINISTRACIÓN DEL PRODUCTO 9
6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA 9
6.2.2 CONFIGURACIÓN DE ADMINISTRADORES 9
6.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 9
6.4 GESTIÓN DE CERTIFICADOS 10
6.5 SERVIDORES DE AUTENTICACIÓN 10
6.6 SINCRONIZACIÓN 10
6.7 ACTUALIZACIONES 10
6.8 AUDITORÍA 10
6.8.1 REGISTRO DE EVENTOS 10
6.8.2 ALMACENAMIENTO LOCAL 12
6.8.3 ALMACENAMIENTO REMOTO 12
6.9 BACKUP 12
7 REFERENCIAS 13
8 ABREVIATURAS 14

ÍNDICE DE TABLAS

Tabla 1: Componentes entorno de operación 5

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Evento de login en portal de usuarios 11
Ilustración 2. Evento de acción en portal de usuarios 11
Ilustración 3. Evento de login de técnico 11
Ilustración 4. Evento de acción de técnico 11
Ilustración 5. Histórico de eventos en incidencia 12
Ilustración 6. Histórico de cambios en incidencia 12

1 INTRODUCCIÓN

Proactivanet es una solución integral para la gestión de servicios (ITSM) y activos de TI (ITAM), diseñada para ofrecer una visión unificada y control completo del entorno tecnológico. Con un enfoque sólido en ITSM alineado con ITIL, permite gestionar de forma eficiente incidencias, problemas, cambios y catálogo de servicios. A su vez, incorpora capacidades avanzadas de ITAM e inventario, con descubrimiento automático, gestión del ciclo de vida de activos y CMDB. Su principal valor reside en la integración nativa entre ITSM e ITAM, que permite relacionar servicios y activos en una única plataforma, mejorando la trazabilidad, la automatización y la toma de decisiones basada en datos fiables.

2 OBJETO Y ALCANCE

El presente documento tiene como objetivo presentar las configuraciones de seguridad existentes en Proactivanet, y que permiten su operación acorde al nivel de seguridad esperado.

Todos los puntos de este documento son aplicables en la modalidad SaaS de Proactivanet, comercializada como servicio en la nube.

El producto Proactivanet ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF3].

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Una vez contratado el servicio de Proactivanet SaaS se facilitará el acceso a una instancia dedicada del mismo.

El acceso de realizará a través de protocolo seguro HTTPS, utilizando la URL específica facilitada durante el proceso de contratación.

El producto se comercializa asociado a los servicios profesionales, entre los que se encuentra la asistencia en el proceso de entrega y configuración inicial del servicio.

4.2 ENTORNO DE INSTALACIÓN SEGURO

El producto Proactivanet en modalidad SaaS no requiere la provisión de un entorno de despliegue por parte del cliente, siendo tanto la provisión como la administración del entorno computacional subyacente responsabilidad de Proactivanet.

4.3 REGISTRO Y LICENCIAS

Las licencias de Proactivanet se proveen y activan durante la fase de despliegue, la cual se lleva a cabo como un servicio profesional gestionado en el que un técnico especializado de Proactivanet acompaña al cliente durante todo el proceso, desde la planificación hasta la verificación final. En este contexto, el licenciamiento contratado queda configurado y operativo como parte de dicho servicio, sin que el cliente deba realizar gestiones adicionales de activación de forma autónoma.

En caso de que la organización requiera ampliar el número de licencias contratadas, esto es posible en cualquier momento mediante contacto directo con el fabricante.

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

A continuación, se describen los componentes involucrados en el entorno de operación de Proactivanet, etiquetándose como BASE aquellos que corresponden a requisitos de la instalación básica y como OPCIONAL aquellos que corresponden a configuraciones concretas.

Componente	Función	BASE / OPCIONAL
Infraestructura del servicio SaaS	Aloja la aplicación web principal y los ficheros relacionados con la misma. Incluye servidores de aplicaciones, bases de datos, registros DNS y gestión de certificados. Es operado y mantenido por Proactivanet.	BASE

Servicio SSO SAML	Permite la autenticación de usuarios y técnicos mediante el protocolo SAMLv2.	OPCIONAL
Servicio de e-mail	Necesario para el envío de notificaciones automáticas a usuarios y técnicos, así como para la recepción de correos que creen o actualicen tickets. Debe permitir envío externo con autenticación y cifrado TLS/SSL.	OPCIONAL

Tabla 1: Componentes entorno de operación

5 FASE DE INSTALACIÓN

La contratación del servicio SaaS de Proactivanet no conlleva fase de instalación, sino que la misma se sustituye por la provisión de instancia, la cual es gestionada en la fase de adquisición del producto.

6 FASE DE CONFIGURACIÓN

Una vez finalizada la provisión, es posible configurar el producto para que sus requisitos de seguridad se adecuen a los requeridos por la organización.

6.1 AUTENTICACIÓN

El acceso a la interfaz de Proactivanet se realiza en todos los casos desde un navegador utilizando HTTPS TLSv1.2.

El acceso a Proactivanet se distingue en dos grandes grupos, Técnicos y Usuarios, siendo necesario en ambos casos el acceso autenticado, para lo que es posible configurar las siguientes opciones:

a) Credenciales de Proactivanet: Este método requiere la definición y uso de un juego de credenciales, formado por un nombre de usuario y una contraseña definida en Proactivanet.

   Aunque Proactivanet ya propondrá una configuración por defecto de cada una de las configuraciones de seguridad abajo descritas, se recomienda consultar el siguiente punto para que pueda entender cada una de ellas y así configurar la complejidad de las contraseñas de Proactivanet de manera adecuada a la política general de la organización.

   i) Activar expiración de contraseñas, para que de manera recurrente se les solicite al usuario y al técnico el cambio de su contraseña de manera forzosa.

   ii) Definir parámetros de complejidad de las contraseñas, pudiendo establecer longitud mínima y obligatoriedad de uso de mayúsculas, minúsculas, números y caracteres especiales.

   iii) Definir parámetros de reutilización de las contraseñas, estableciendo el número máximo de contraseñas que se recordarán para que no puedan ser reutilizadas.

   iv) Limitación de número de intentos: En caso de utilizarse credenciales de Proactivanet, será posible definir una limitación en el número máximo de intentos de login, siendo configurable tanto el número de intentos como el tiempo de bloqueo.

   v) Uso de captcha: Con el fin de proteger el formulario de login, es posible añadir un captcha al mismo, estando disponibles las opciones de captcha interno de Proactivanet y Google recaptcha, siendo esta última la opción recomendada.

   vi) Cambio de contraseñas: La configuración del cambio de contraseña por parte del usuario es configurable a través de un mecanismo basado en el envío de email. El email de cambio de contraseña se enviará utilizando la cuenta configurada por cada cliente en la herramienta a tal propósito.

b) Single Sign-On (SSO): Proactivanet también permite la configuración de autenticación y acceso vía Single Sign-On usando el protocolo SAMLv2.

Es posible realizar esta configuración con cualquier proveedor de identidades (IdP) que soporte dicho estándar.

El proceso de configuración se puede realizar completamente desde la interfaz web de configuración de Proactivanet.

En este caso, Proactivanet delega las políticas de credenciales de los usuarios al IdP utilizado, y será tarea del administrador configurar el mismo según las políticas de seguridad aplicables.

Por motivos de seguridad la configuración de SAML debe requerir la validación de firmas.

Es posible que dos o más tipos de autenticación para el acceso a Proactivanet estén configurados al mismo tiempo, generando una configuración mixta de acceso. Siempre que sea posible, es recomendable usar el método de SSO como autenticación de acceso a la herramienta.

Independientemente del modo de acceso configurado en Proactivanet, se recomienda que cada cliente configure una política de acceso acorde a los estándares y normativas internas de la organización, utilizando las configuraciones proporcionadas por la herramienta en el caso de utilizar las credenciales propias de Proactivanet, o aquellas que proporcione el proveedor de autenticación utilizado. Como norma general se darán las siguientes directrices:

a) Configuración de una política de contraseñas robusta, teniendo en cuenta tanto la complejidad como la reutilización y la caducidad de las mismas. A continuación, se propone las recomendaciones para cada una de las opciones disponibles:

   i) Impedir contraseñas en blanco: Activo.

   ii) Longitud mínima: 12 caracteres.

   iii) Obligatorio mayúsculas: Activo.

   iv) Obligatorio minúsculas: Activo.

   v) Obligatorio carácter especial: Activo.

   vi) Obligatorio números: Activo.

   vii) Impedir reutilizar contraseñas: Activo.

   viii) Nº de contraseñas almacenadas: 10

b) Uso de políticas de bloqueo de usuarios en base al número de intentos de login infructuosos. Se recomienda configurar 3 intentos como máximo de intentos fallidos de acceso y una duración del bloqueo de la cuenta de 15 minutos.

c) Configuración del doble factor de autenticación proporcionado por el proveedor de autenticación. Aunque es una configuración que debe hacerse en el sistema de autenticación que se haya usado para el acceso mediante SSO, es recomendable que no se active como 2FA la confirmación por SMS ya que es considerada un 2FA débil.

Se recomienda utilizar una política de privilegios acorde al nivel de acceso necesario en cada punto del ciclo de vida del usuario/técnico.

En cuanto a la gestión de usuarios y accesos de estos al sistema se deben considerar los siguientes puntos:

a) Retirada de acceso: Una vez finalizada la necesidad de acceso del usuario/técnico, debe denegársele el acceso a la aplicación.

b) Desactivación del usuario/técnico.

c) Deshabilitación del inicio de sesión.

Auditoría de acceso:

A través del menú de 'Histórico de accesos y modificaciones', Proactivanet ofrece a los usuarios con los privilegios adecuados un listado de los logins realizados y denegados en el sistema. Se recomienda realizar tareas de revisión de accesos a Proactivanet de forma periódica.

Además, es recomendable activar el histórico de registro de logins para generar la evidencia de accesos correctos e incorrectos a Proactivanet, así como activar la purga automática de estos registros.

6.2 ADMINISTRACIÓN DEL PRODUCTO

6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

La administración de Proactivanet se realiza a través de un rol específico habilitado dentro del propio producto, que otorga acceso a las funcionalidades de configuración, gestión y mantenimiento de la plataforma. No existe un canal de administración remota independiente; toda la operación administrativa se lleva a cabo desde la misma interfaz de la aplicación, bajo control de acceso basado en roles (RBAC).

El acceso a dicha interfaz se realiza exclusivamente a través de conexiones HTTPS, garantizando el cifrado en tránsito de toda la comunicación entre el cliente y el servidor.

6.2.2 CONFIGURACIÓN DE ADMINISTRADORES

El rol de administrador de Proactivanet se divide en dos niveles principales:

a) Administrador del Service Desk: Quien por defecto dispone de una serie de capacidades que le permiten parametrizar la herramienta.

b) Administrador de usuarios y grupos: Dispone de permisos específicos para configurar los perfiles y grupos de los usuarios, así como sus mecanismos de acceso.

Cabe destacar que los permisos de usuario de Proactivanet son granulares y basados en roles, por lo que sobre estos perfiles básicos es posible parametrizar el acceso a diferentes puntos de la herramienta.

Los clientes de Proactivanet disponen de accesos a un sistema de ayuda donde se aclaran los detalles de la gestión de roles: [REF1]

6.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

La comunicación entre los clientes y el servicio se realiza únicamente a través de protocolo HTTPS con TLS 1.2. o superior.

Configuración TLS: La comunicación HTTPS se establece empleando las versiones y suites de cifrado seguras, cuya idoneidad es revisada dentro del proceso de mejora continua de seguridad del servicio.

Certificados: El servicio presentará un certificado HTTPs válido, emitido por una Autoridad de Certificación reconocida.

6.4 GESTIÓN DE CERTIFICADOS

Proactivanet gestiona el ciclo de vida de los certificados utilizados bajo su propio dominio proactivanet.com, dichos certificados cumplen las especificaciones descritas en la guía [REF2].

- RSA con claves de, al menos, 3072 bits de longitud.
- ECDSA con curvas P-256 o superior.
- DSA con claves de, al menos, 3072 bits de longitud.
- Funciones Hash SHA-256 o superior.

6.5 SERVIDORES DE AUTENTICACIÓN

En caso de configurarse el uso de autenticación SAML contra un IdP del cliente, deben tenerse en cuenta las siguientes consideraciones de seguridad.

a) Se debe utilizar exclusivamente SAML 2.0 como versión del protocolo.

b) Todas las comunicaciones con el IdP deben realizarse sobre TLS 1.2 como mínimo y para la firma de aserciones SAML se debe emplear el algoritmo RSA-SHA256 o superior. Los certificados utilizados para firma y cifrado deben emplear claves RSA de al menos 2048 bits, emitidos por una autoridad de certificación de confianza, con monitorización activa de su caducidad y rotación periódica.

c) Se debe habilitar la firma de las solicitudes de autenticación (AuthnRequest) desde Proactivanet hacia el IdP, de modo que este pueda verificar el origen legítimo de cada solicitud.

6.6 SINCRONIZACIÓN

La sincronización horaria entre los diferentes componentes del servicio es inherente a la propio modalidad SaaS, siendo esta una parte de la gestión del servicio realizada exclusivamente por el proveedor.

6.7 ACTUALIZACIONES

La gestión de actualizaciones es gestionada por Proactivanet como parte del servicio SaaS.

6.8 AUDITORÍA

6.8.1 REGISTRO DE EVENTOS

Los administradores de Proactivanet disponen de acceso a un detallado registro de eventos, en el que se incluyen tanto los registros de login como las modificaciones de parametrización

realizadas. Cada una de las entradas generadas en dicho registro incluyen tanto la referencia temporal del evento como la dirección IP de cada petición registrada.

El tiempo de retención de los eventos, tanto de acceso como de modificación, es configurable a nivel de instancia, recomendándose configurar este valor con el periodo de retención acordado en su organización.

Ejemplo registro de eventos portal de usuarios.

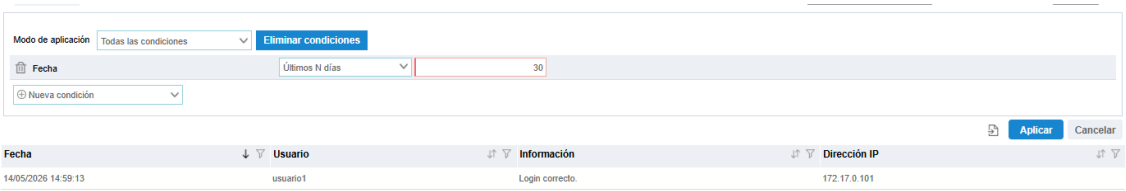


Ilustración 1. Evento de login en portal de usuarios

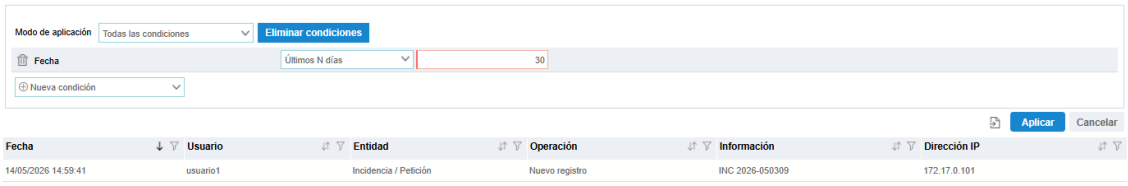


Ilustración 2. Evento de acción en portal de usuarios

Ejemplo registro de eventos acceso de técnicos

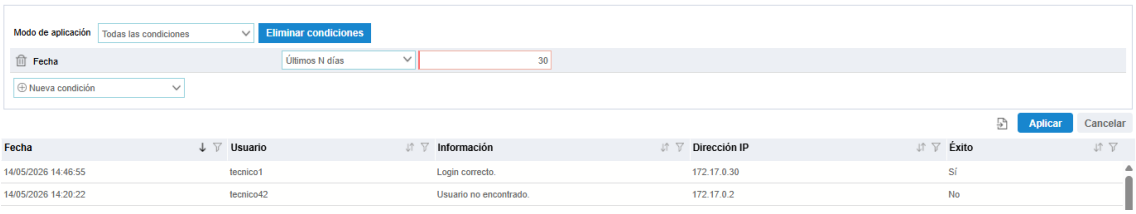


Ilustración 3. Evento de login de técnico

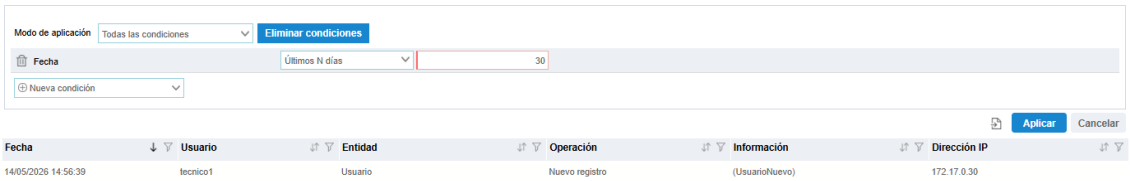


Ilustración 4. Evento de acción de técnico

Al registro general de eventos se unen los históricos de eventos y cambios de cada ítem, a los que el técnico podrá acceder desde la página del propio elemento.

Ejemplo histórico de eventos incidencia.

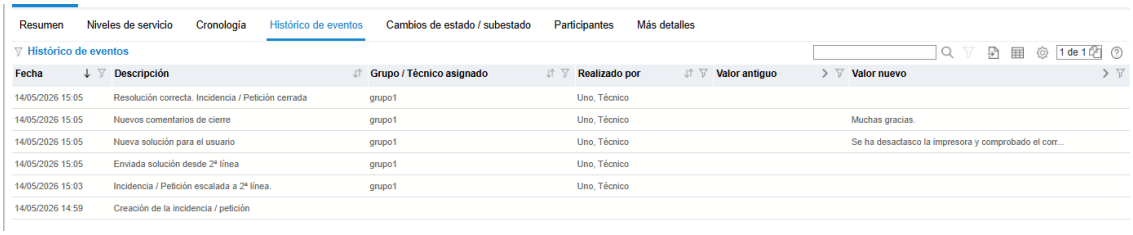


Ilustración 5. Histórico de eventos en incidencia

Ejemplo histórico de cambios incidencia.

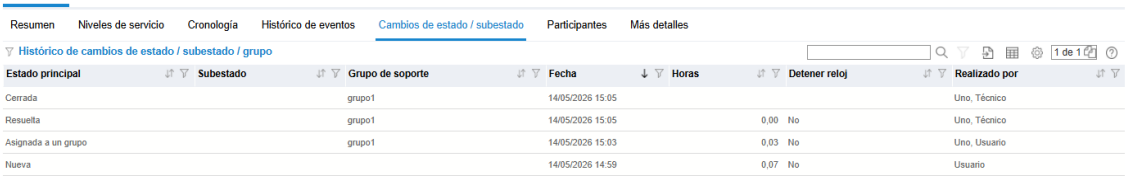


Ilustración 6. Histórico de cambios en incidencia

6.8.2 ALMACENAMIENTO LOCAL

El registro de eventos de Proactivanet en el propio servicio, por lo que este se entrega como un componente más del servicio que no requiere acciones adicionales por parte del cliente.

6.8.3 ALMACENAMIENTO REMOTO

No se contempla el almacenamiento remoto de registros de cambios y eventos.

6.9 BACKUP

Proactivanet en modalidad SaaS incorpora de forma nativa un sistema gestionado de copias de seguridad y un plan de recuperación ante desastres (DRP), sin que sea necesaria intervención alguna por parte del cliente. Las copias de seguridad se realizan de manera automatizada y periódica, garantizando la integridad y disponibilidad de los datos almacenados. La responsabilidad íntegra de la operación, supervisión y prueba de dichos procesos recae sobre Proactivanet como proveedor del servicio.

7 REFERENCIAS

REF1	Ayuda clientes: Gestión de accesos - cómo se configura https://proactivanet.helpjuice.com/es_ES/gestion-de-accesos-en-proactivanet
REF2	Ayuda clientes: CCN-STIC-807 https://www.ccn-cert.cni.es/es/series-ccn-stic/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html
REF3	CPSTIC https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

8 ABREVIATURAS

2FA	Two-Factor Authentication. Autenticación de Doble Factor.
CA	Certification Authority. Autoridad de Certificación.
CMDB	Configuration Management Database. Base de Datos de Gestión de la Configuración.
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las TIC (CCN).
DNS	Domain Name System. Sistema de Nombres de Dominio.
DSA	Digital Signature Algorithm. Algoritmo de Firma Digital.
ECDSA	Elliptic Curve Digital Signature Algorithm. Algoritmo de Firma Digital sobre Curva Elíptica.
ENS	Esquema Nacional de Seguridad.
Hash SHA-256	Secure Hash Algorithm 256 bits. Función resumen criptográfica de 256 bits de la familia SHA-2.
HTTPS	Hypertext Transfer Protocol Secure. Protocolo de Transferencia de Hipertexto Seguro.
IdP	Identity Provider. Proveedor de Identidad.
IP	Internet Protocol. Protocolo de Internet.
ITAM	IT Asset Management. Gestión de Activos de Tecnologías de la Información.
ITIL	Information Technology Infrastructure Library. Biblioteca de Infraestructura de Tecnologías de la Información.
ITSM	IT Service Management. Gestión de Servicios de Tecnologías de la Información.
RBAC	Role-Based Access Control. Control de Acceso Basado en Roles.
RSA	Rivest-Shamir-Adleman. Algoritmo criptográfico asimétrico de clave pública.
SAML	Security Assertion Markup Language. Lenguaje de Marcado para Aserciones de Seguridad.
SSL	Secure Sockets Layer. Capa de Conexión Segura (protocolo predecesor de TLS, actualmente en desuso).
SSO	Single Sign-On. Inicio de Sesión Único.
TLS	Transport Layer Security. Seguridad de la Capa de Transporte
URL	Uniform Resource Locator. Localizador Uniforme de Recursos.