Guía de Seguridad de las TIC
CCN-STIC 1008

Procedimiento de Empleo Seguro
Proactivanet OnPremise



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 5
4.4 CONSIDERACIONES PREVIAS 5
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 6
5 FASE DE INSTALACIÓN 7
6 FASE DE CONFIGURACIÓN 8
6.1 AUTENTICACIÓN 8
6.2 ADMINISTRACIÓN DEL PRODUCTO 10
6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA 10
6.2.2 CONFIGURACIÓN DE ADMINISTRADORES 10
6.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 10
6.4 GESTIÓN DE CERTIFICADOS 11
6.5 SERVIDORES DE AUTENTICACIÓN 11
6.6 SINCRONIZACIÓN 11
6.7 ACTUALIZACIONES 12
6.8 ALTA DISPONIBILIDAD 12
6.9 AUDITORÍA 12
6.9.1 REGISTRO DE EVENTOS 12
6.9.2 ALMACENAMIENTO LOCAL 14
6.9.3 ALMACENAMIENTO REMOTO 14
6.10 BACKUP 14
7 REFERENCIAS 15
8 ABREVIATURAS 16

ÍNIDCE DE TABLAS

Tabla 1. Requisitos mínimos de instalación 3
Tabla 2: Componentes entorno de operación 6

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Verificación firma instalador 4
Ilustración 2. Evento de login en portal de usuarios 12
Ilustración 3. Evento de acción en portal de usuarios 13
Ilustración 4. Evento de login de técnico 13
Ilustración 5. Evento de acción de técnico 13
Ilustración 6. Histórico de eventos en incidencia 13
Ilustración 7. Histórico de cambios en incidencia 13

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 On Premise de Proactivanet 10, instalada sobre servidores Windows server 2012 o superior y SGBD Microsfot SQL Server 2014 o superior, siendo los requisitos mínimos:

Componente	Uso Básico	Uso Medio	Uso Elevado	Uso Intensivo
Edición de BBDD mínima	Microsoft SQL Server 2014 Express Edition	Microsoft SQL Server Standard 2014	Microsoft SQL Server Standard 2014	Microsoft SQL Server Standard 2014
Nº de núcleos de CPU	2	4	8	16
Memoria RAM (GB)	8	8	16	16
Almacenamiento (GB)	100	240	480	480

Tabla 1. Requisitos mínimos de instalación

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 [REF5].

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

El producto se comercializa asociado a los servicios profesionales, entre los que se encuentra la asistencia en el proceso de instalación en los sistemas proporcionados por el cliente.

Para la realización de dicha instalación se facilitará previamente al cliente una copia del fichero instalador mediante una URL de descarga segura, cuya integridad podrá ser verificada a través de la firma digital del mismo.

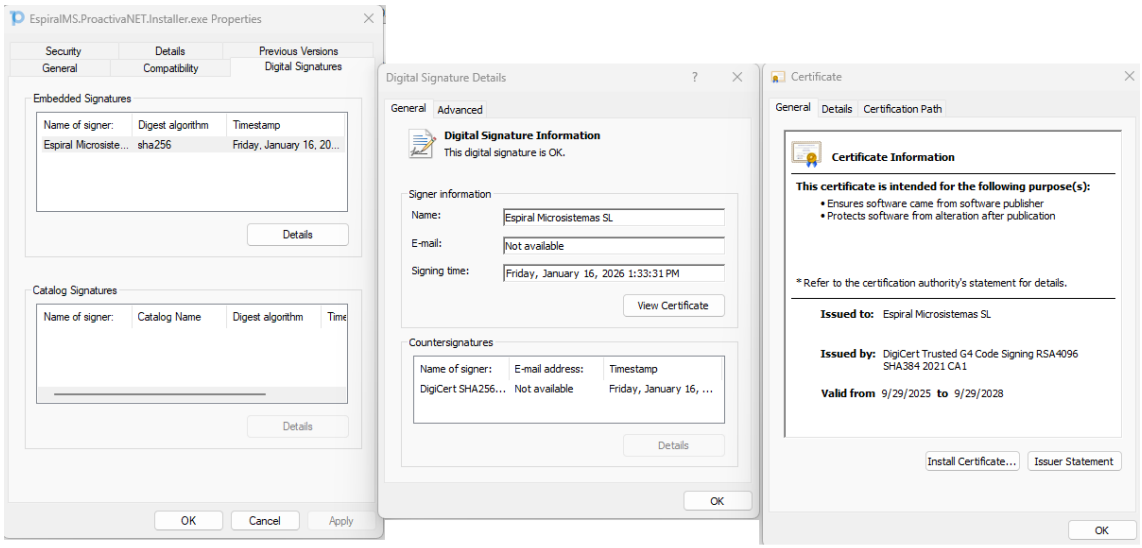


Ilustración 1. Verificación firma instalador

4.2 ENTORNO DE INSTALACIÓN SEGURO

El producto Proactivanet se compone principalmente de dos componentes servidor. El primero es un servidor IIS (*Internet Information Services*) sobre Windows server en el que se ejecuta la aplicación principal, y que gestiona tanto los ficheros de configuración como los ficheros generados y administrados desde el propio producto.

El segundo componente es un servidor de base de datos MS SQL Server, que podrá ubicarse en el mismo servidor que la aplicación web o, preferiblemente, en un servidor independiente por razones de rendimiento, seguridad y mantenibilidad.

Se recomienda que ambos componentes se instalen en el CPD (Centro de Procesamiento de Datos) del cliente, entorno en el que sea posible garantizar las medidas de seguridad física necesarias, así como las condiciones de continuidad de servicio adecuadas: sistemas de alimentación ininterrumpida (SAI), soluciones de backup, control ambiental, acceso restringido, etc.

La comunicación entre ambos servicios debe garantizar alta disponibilidad, baja latencia y persistencia de conexión, condiciones indispensables para asegurar el correcto funcionamiento del producto. En caso de que los dos componentes se ubiquen en servidores distintos, deberá verificarse la conectividad entre ellos antes del inicio de la instalación.

4.3 REGISTRO Y LICENCIAS

Las licencias de Proactivanet se proveen y activan durante la fase de instalación, 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, podrá hacerlo en cualquier momento mediante contacto directo con el fabricante.

4.4 CONSIDERACIONES PREVIAS

Existe un conjunto de configuraciones y decisiones que deben adoptarse antes de iniciar la instalación, ya que condicionan directamente la forma en que el producto quedará configurado de forma segura.

Obtención e instalación del certificado TLS (obligatorio antes de la instalación): Para garantizar la seguridad del producto instalado, Proactivanet debe servirse exclusivamente a través de HTTPS. El certificado debe estar instalado en el servidor IIS antes de configurar la aplicación, pudiendo generarse el certificado en base a alguna de las siguientes opciones:

a) Certificado emitido por una CA pública: Su adquisición debe gestionarse por parte del cliente, asociado a la URL de acceso al futuro servicio.

b) Certificado emitido por una CA interna corporativa: Esta opción debe considerase solamente si se puede garantizar la confianza de los equipos clientes en dicha CA.

En ambos casos será necesario disponer de un nombre DNS a asociar al servicio, así como la publicación del mismo en los servidores DNS públicos o privados, según proceda.

Para garantizar la seguridad del cifrado en tránsito el servidor debe disponer de TLS 1.2 como versión mínima aceptada, así como una configuración actualizada de suites de cifrado, siendo la configuración recomendada a fecha de creación de este documento:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128/256_GCM_SHA256/384
- TLS_ECDHE_ECDSA_WITH_AES_256/128_CCM
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

Deben deshabilitarse explícitamente protocolos obsoletos (SSL 3.0, TLS 1.0, TLS 1.1) y suites de cifrado débiles (RC4, DES, 3DES, etc).

La compatibilidad con el formato de nombres de archivo DOS (8.3) debe encontrarse deshabilitada en el volumen de instalación de Proactivanet.

Verificación en el registro del sistema:

HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation

El valor debe ser 1 (deshabilitado en todos los volúmenes). Si el valor es 0 o 2, debe corregirse antes de la instalación. Si la instalación ya se hubiera realizado en un disco con nombres cortos activos, puede procederse a su eliminación con:

```
fsutil.exe 8dot3name strip /s /v E:\...
```

Esta operación requiere autorización expresa del administrador del sistema del cliente.

4.5 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
Servidor de aplicaciones Proactivanet (Windows Server + IIS)	Aloja la aplicación web principal y los ficheros relacionados con la misma.	BASE
Servidor de base de datos (MSSQL)	Almacena la información gestionada por Proactivanet, así como sus parametrizaciones.	BASE
Servicio DNS	Necesario para la resolución del nombre del servicio de Proactivanet por parte de los equipos clientes.	BASE
Certificado	Proporciona el certificado TLS que permite servir la aplicación por HTTPS. Puede ser una CA pública o una CA interna corporativa.	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 2: Componentes entorno de operación

5 FASE DE INSTALACIÓN

La instalación de Proactivanet en modalidad on premise 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.

El proceso se inicia con el envío al cliente del documento de requisitos de hardware y software, siendo la preparación y provisión de dicha infraestructura responsabilidad exclusiva del cliente, si bien el técnico de Proactivanet prestará el asesoramiento necesario para resolver cualquier duda durante esta fase.

Los requisitos que debe cumplir el entorno de instalación son los marcados como BASE en el punto 4.5 del presente documento

Una vez que el cliente comunica la disponibilidad del entorno, y verificado el cumplimiento de los requisitos se procederá a planificar la sesión de instalación, en la que el técnico de Proactivanet, conectándose de forma remota, realizará la instalación del servicio.

Una vez concluida la instalación, se realizará una batería de verificaciones funcionales conforme a una checklist estandarizada que cubre el acceso a la aplicación, el correcto funcionamiento de los principales módulos, la integración con el sistema de autenticación corporativo y la comprobación del envío de notificaciones. Solo tras superar satisfactoriamente estas verificaciones se da por finalizado el servicio de instalación, quedando el entorno listo para la fase de configuración inicial y puesta en marcha operativa.

6 FASE DE CONFIGURACIÓN

Una vez finalizada la instalación, 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, configuradas conforme a los requisitos de instalación del producto, 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:

- Administrador del Service Desk: Quien por defecto dispone de una serie de capacidades que le permiten parametrizar la herramienta.
- 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 servidor de la aplicación se realiza únicamente a través de protocolo HTTPS con TLS 1.2. El acceso mediante HTTP sin cifrar debe ser deshabilitado

durante el proceso de instalación y configuración del producto, manteniéndose únicamente la configuración segura HTTPS que ha sido definida en la fase de instalación.

Configuración TLS: La comunicación HTTPS se establece empleando las versiones y suites de cifrado especificadas en el apartado 4.1 del presente documento. Las versiones de protocolo y algoritmos no contemplados deben ser deshabilitados en el servidor web subyacente.

Certificados: El servidor deberá presentar un certificado válido, emitido por una Autoridad de Certificación reconocida o, en entornos corporativos, por la PKI interna de la organización, con algoritmo de firma acorde a los requisitos indicados en el apartado 4.1.

6.4 GESTIÓN DE CERTIFICADOS

Proactivanet no emite ni gestiona el ciclo de vida de los certificados utilizados, siendo el servidor IIS y el sistema operativo subyacente los encargados de la gestión del certificado.

En la fase de instalación debe proveerse un servidor IIS con un certificado válido configurado, cuyas especificaciones cumplan las descritas en la guía CCN-STIC-807 [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.

Durante el ciclo de vida de la instancia instalada, podría ser necesario realizar actualizaciones sobre el certificado, debiendo gestionarse a nivel organizativo la solicitud del nuevo certificado actualizado y su despliegue en el servidor IIS provisto.

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

No se contemplan configuraciones de sincronización de tiempo a nivel de aplicación, sin embargo, se recomienda que tanto el servidor web utilizado como el de BBDD compartan una configuración NTP.

6.7 ACTUALIZACIONES

La disponibilidad de los paquetes aplicables será trasladada al cliente a través de las vías de comunicación acordadas, coordinándose la fecha en base a las necesidades del cliente y las condiciones previamente acordadas.

De forma similar al proceso de instalación, el proceso de actualización del software se realizará con la colaboración del personal técnico de Proactivanet, quien se encargará de proveer el paquete de actualización con los mismos requisitos de seguridad descritos en el punto 4.1 del presente documento.

6.8 ALTA DISPONIBILIDAD

Proactivanet puede operar en un entorno de **alta disponibilidad (activo/activo)** siempre que la infraestructura del cliente cumpla con los requisitos necesarios, entre los que destacan: disponer de un **sistema de almacenamiento compartido** con replicación en tiempo real, una **base de datos con replicación activo/activo** que permita conexión simultánea desde múltiples instancias, y un **balanceador de carga** capaz de gestionar la persistencia de sesiones y tomar decisiones de conmutación basadas en respuestas HTTP. En este escenario, el componente web opera en modo activo/activo con failover automático.

Es importante señalar que **todas las medidas de seguridad recogidas en el presente documento son plenamente aplicables a este escenario de alta disponibilidad**, debiendo garantizarse su cumplimiento en cada uno de los nodos desplegados, así como en los elementos de infraestructura compartida como el sistema de ficheros y la base de datos replicada.

Los clientes de Proactivanet disponen de accesos a un sistema de ayuda donde se aclaran los detalles de la instalación en alta disponibilidad de Proactivanet: [REF3]

6.9 AUDITORÍA

6.9.1 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.

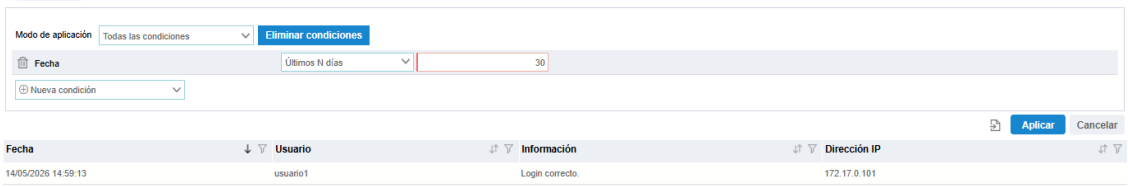


Ilustración 2. Evento de login en portal de usuarios

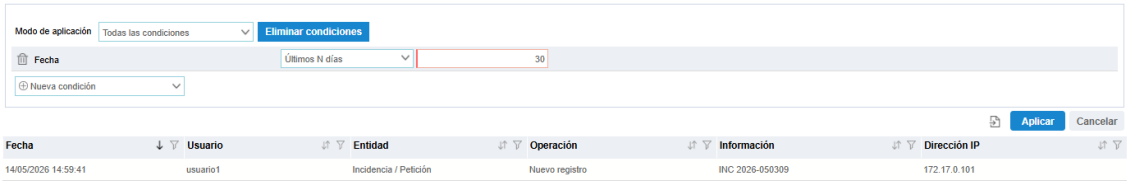


Ilustración 3. Evento de acción en portal de usuarios

Ejemplo registro de eventos acceso de técnicos

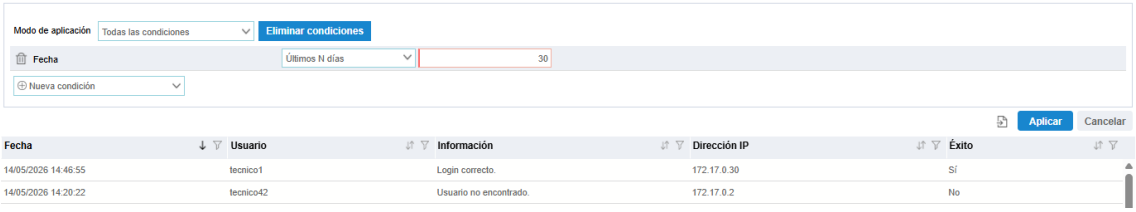


Ilustración 4. Evento de login de técnico

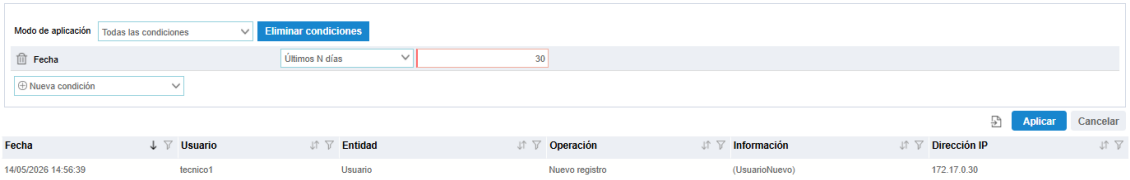


Ilustración 5. Evento de acción de técnico

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.

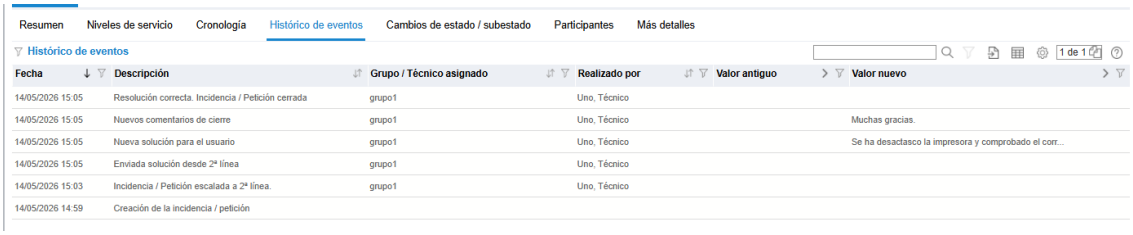


Ilustración 6. Histórico de eventos en incidencia

Ejemplo histórico de cambios incidencia.

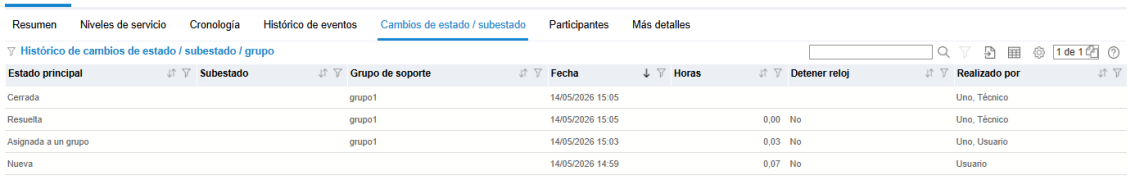


Ilustración 7. Histórico de cambios en incidencia

6.9.2 ALMACENAMIENTO LOCAL

El registro de eventos de Proactivanet se almacena en la base de datos del producto, por lo que tanto su disponibilidad como la disponibilidad de copias de seguridad será la misma que se haya definido en la gestión de copias de seguridad.

6.9.3 ALMACENAMIENTO REMOTO

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

6.10 BACKUP

Para garantizar la continuidad del servicio y la recuperación ante posibles desastres, es imprescindible mantener una política de backup que contemple los siguientes aspectos:

Elementos a respaldar:

a) Directorios de aplicación, que contienen tanto la aplicación web como los ficheros adjuntos gestionados por usuarios y técnicos.

b) Base de datos.

Frecuencia mínima recomendada:

Tanto para los directorios como para la base de datos se recomienda realizar, como mínimo, un backup diferencial diario y un backup completo semanal, pudiendo cada organización establecer una frecuencia superior según sus necesidades.

Almacenamiento y retención:

- Se recomienda aplicar un periodo mínimo de retención es de 3 meses.
- Al menos una copia debe almacenarse en una ubicación geográfica distinta al CPD que alberga los servidores de Proactivanet.

Verificación:

El sistema de backups debe ser verificado al menos una vez al año, planificando simulaciones periódicas de restauración para garantizar la integridad y validez de las copias.

Errores frecuentes a evitar:

- Respaldar únicamente la base de datos sin incluir los ficheros en disco.
- No sincronizar las copias de base de datos y ficheros.
- Almacenar los backups en el propio servidor de producción o en el mismo CPD.
- Mantener un histórico insuficiente de copias (inferior a 3 meses).
- No realizar pruebas periódicas de restauración.

Los clientes de Proactivanet disponen de accesos a un sistema de ayuda donde se enumeran las recomendaciones de backup: [REF4]

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 Ayuda clientes: Instalación Proactivanet Alta Disponibilidad
https://proactivanet.helpjuice.com/alta-disponibilidad/instalacion-de-proactivanet-en-alta-disponibilidad?from_search=228305479&swifty_search_highlight=alta+disponibilidad

REF4 Ayuda clientes: Copias de seguridad de Proactivanet
https://proactivanet.helpjuice.com/infraestructura-on-premises/como-hago-copias-de-seguridad-de-proactivanet

REF5 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.
CPD	Centro de Procesamiento de Datos.
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.
IIS	Internet Information Services. Servidor web de Microsoft para Windows Server.
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.
SAI	Sistema de Alimentación Ininterrumpida.
SAML	Security Assertion Markup Language. Lenguaje de Marcado para Aserciones de Seguridad.
SGBD	Sistema Gestor de Bases de Datos.
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.