centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1701

Procedimiento de Empleo Seguro
Proofpoint Security Awareness Training (PSAT)

Febrero 2026

Edita:

Fecha de Edición: Febrero de 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.02.18 15:58:11 +01'00'

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

ÍNDICE

1 INTRODUCCIÓN

1. La solución de Proofpoint de capacitación en concienciación de seguridad, también conocida como **Proofpoint Security Awareness Training** o **PSAT**, es ofrecida en formato SaaS (*Software as a Service*) e involucra a los usuarios de forma que estén preparados en la defensa de ciberataques del mundo real, a través de formaciones totalmente personalizadas basadas en la inteligencia de amenazas mundial de Proofpoint.
2. En lugar de tener un contenido único para todos los usuarios, PSAT ayuda a brindar la formación más adecuada a las personas apropiadas y de la forma correcta, evaluando el proceso en todo momento, para mantener un nivel de concienciación óptimo en la organización.
3. Ofrece las siguientes funcionalidades:
    - Identificación de vulnerabilidades.
        - A través de simulaciones de ataques de phishing, la plataforma identifica rápidamente a los usuarios vulnerables utilizando plantillas de mensajes de phishing del mundo real, provistos por la red de inteligencia de amenazas mundial de Proofpoint.
        - Amplía la capacidad de evaluación de riesgos, a través de simulaciones de ficheros maliciosos en memorias USB.
        - Usa las evaluaciones de conocimientos para conocer el nivel de concienciación de los usuarios en cada dominio de seguridad, utilizando preguntas de todos los ámbitos y permite crear consultas personalizadas para evaluar la comprensión de las políticas y procedimientos de la organización.
    - Formación a los usuarios.
        - La plataforma gestiona la inscripción automática de formaciones a partir de simulaciones de phishing fallidas o evaluaciones de conocimientos no superados. Utiliza la propuesta de itinerarios formativos de Proofpoint para mejorar los conocimientos de los usuarios, o usa otras rutas pedagógicas.
        - Aplica el currículum básico traducido y geolocalizado en más de 40 idiomas, ofreciendo de forma automática el idioma apropiado a cada usuario, utilizando dominios, nombre y referencias específicos de cada región.
        - Dispone de un amplio catálogo de materiales de concienciación que permiten mantener a los usuarios comprometidos con el contenido que se ofrece a través de mensajes coherentes y procesables en una amplia variedad de formatos. El repertorio está enfocado en la precisión de mensaje, su corta duración, en formaciones interactivas para mantener la atención, temática actualizada con el panorama actual de amenazas y flexibilidad de seguimiento desde cualquier dispositivo.
        - Las funcionalidades de personalización de la plataforma brindan la capacidad de editar los contenidos de formación para reflejar las necesidades únicas de cada compañía.
    - Reducción de la exposición.
        - La plataforma permite a los usuarios informar de los mensajes que les parezcan sospechosos de una forma cómoda y sencilla, a través del botón PhishAlarm en el cliente de correo o en el navegador, reforzando el comportamiento positivo mediante un agradecimiento inmediato a los usuarios.

  - Utiliza la potencia de análisis y clasificación del módulo *Analyzer*, para obtener un informe en tiempo real de las amenazas sospechosas informadas por los usuarios, ahorrando tiempo a los equipos de respuesta.
- Evaluación de riesgos.
  - Utiliza las funcionalidades de evaluación, simulación y formación, sin ningún límite y de forma recursiva, para extender el plan de formación de la compañía a lo largo del tiempo.
  - Dispone de visibilidad granular y de alto nivel, con los datos de los usuarios en sus evaluaciones, ataques simulados, tareas de formación e informes de phishing. Utiliza este Business Intelligence para identificar las áreas, temas y personas más vulnerables, y los usa para guiar la mejora continua del programa de concienciación.
  - Permite el uso de los datos en la propia plataforma o los exporta para añadirlos en herramientas de inteligencia externas.
- Orquestación de seguridad.
  - Utiliza la visibilidad de amenazas contra ataques dirigidos (TAP) de Proofpoint para identificar a las personas más atacadas (VAPs) y aquellas que hacen más veces clic en URLs de amenazas de phishing de credenciales, ransomware, etc., para asignar evaluaciones, simulaciones de phishing y formaciones personalizadas.
  - Automatiza la respuesta a los mensajes sospechosos que realmente son amenazas, utilizando la potencia de CLEAR (Closed Loop Email Analysis and Response) ofrecida por el módulo *Analyzer* para realizar las acciones de respuesta en el correo electrónico, poniendo en cuarentena dichos mensajes o eliminándolos de forma automática.
  - Emplea el panel de control de riesgos NPRE para CISOs de Proofpoint (Nexus People Risk Explorer) para planificar e implementar una estrategia de seguridad centrada en las personas. Analiza los datos de las herramientas de Proofpoint y de terceros, segmentando a los empleados por sus riesgos de seguridad y muestra sugerencias de los controles más apropiados para cada grupo.
- Servicio gestionado.
  - Permite que un equipo de expertos de Proofpoint que trabajan con cientos de organizaciones, ayude a reducir la carga de trabajo y administre un programa integral de concienciación sobre seguridad.
  - Puede elegir entre distintos programas establecidos u obtener una experiencia personalizada perfecta para las necesidades únicas de cada organización.
  - Recibe apoyo personalizado, informes integrales y se asegura de que el programa cumpla con las mejores prácticas para un cambio de comportamiento óptimo.

2 OBJETO Y ALCANCE

4. El presente documento se centra en la solución de concienciación de *Proofpoint Security Awareness Training* o *PSAT*. Al ser una solución ofrecida en formato SaaS, el presente documento se centra en la **configuración segura de la solución**.
5. Esta solución ha sido incluida en el CPSTIC en la familia "*Formación y Concienciación de la Ciberseguridad*", en la sección de productos y servicios de "*Conformidad y Gobernanza*".

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

6. Proofpoint realiza la provisión de recursos para ofrecer la plataforma de concienciación PSAT en formato SaaS, ofreciendo el acceso a los sistemas a través de una única URL personalizada.
7. La información acerca de la URL, así como la autenticación del usuario administrador, se realiza a través de un email. Este mensaje se envía desde una dirección de correo de Proofpoint (no-reply@proofpoint.com), con destinatario la persona de contacto del cliente y el asunto "*Welcome to Proofpoint Security Awareness Training!*".
8. El mensaje se encuentra cifrado a través de la plataforma *Email Encryption de Proofpoint*. El usuario destinatario podrá acceder a la información a través del link "Click here" para acceder a la interfaz web de *Secure Reader* de Proofpoint para mensajes cifrados, donde podrá registrarse con su cuenta de email, utilizar unas credenciales creadas previamente, o recuperar su contraseña en caso de olvido (vía email). El primer usuario creado por el cliente será de tipo Administrador, y será el encargado de solicitar posteriormente la activación de SSO (Single Sign On) para todas las autenticaciones.
9. A continuación, se muestran unas imágenes orientativas:

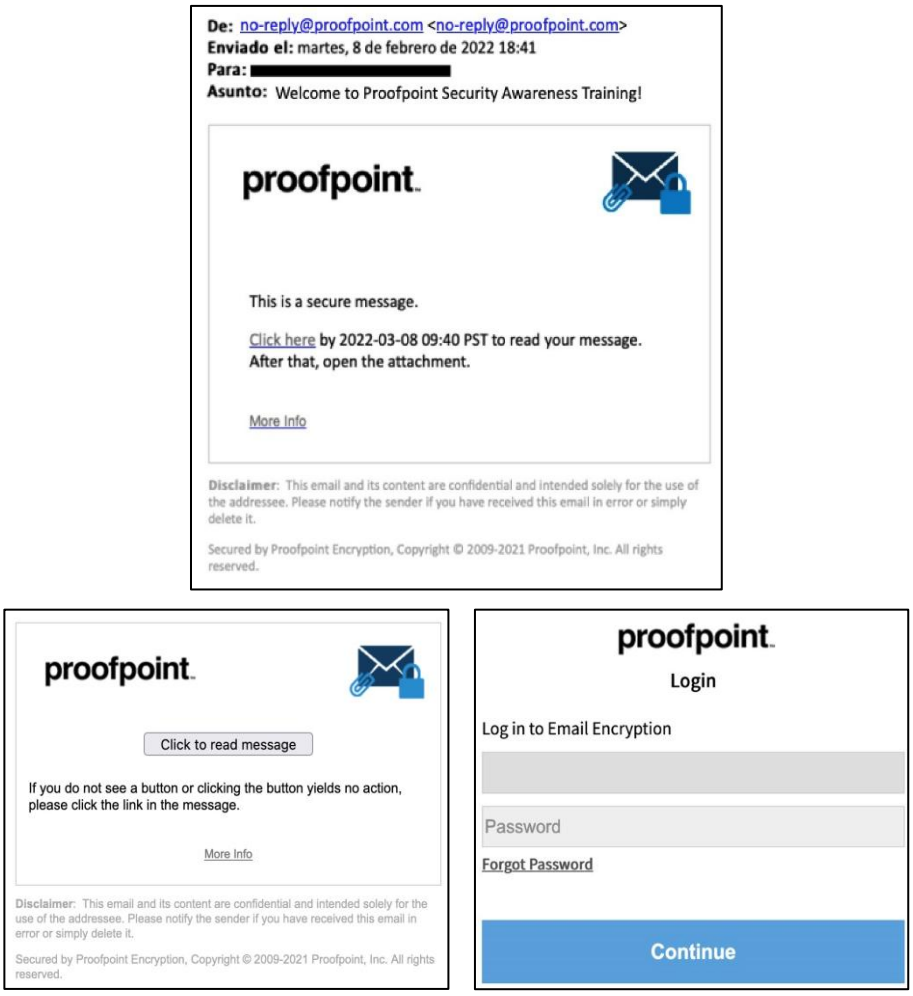

Ilustración 1. Registro de cuenta y credenciales

10. El mensaje enviado también incluye un fichero adjunto en formato .html, que permite leer la información haciendo clic en "*Click to read message*" e introduciendo las credenciales de *Secure Share*.

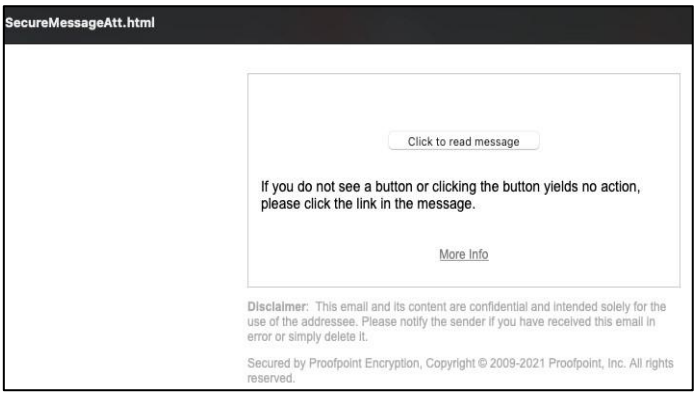

Ilustración 2. Instrucciones para leer mensaje cifrado

11. La información proporcionada será de la siguiente manera (URL de acceso, usuario o dirección de correo del contacto, y método de recuperación de contraseña):

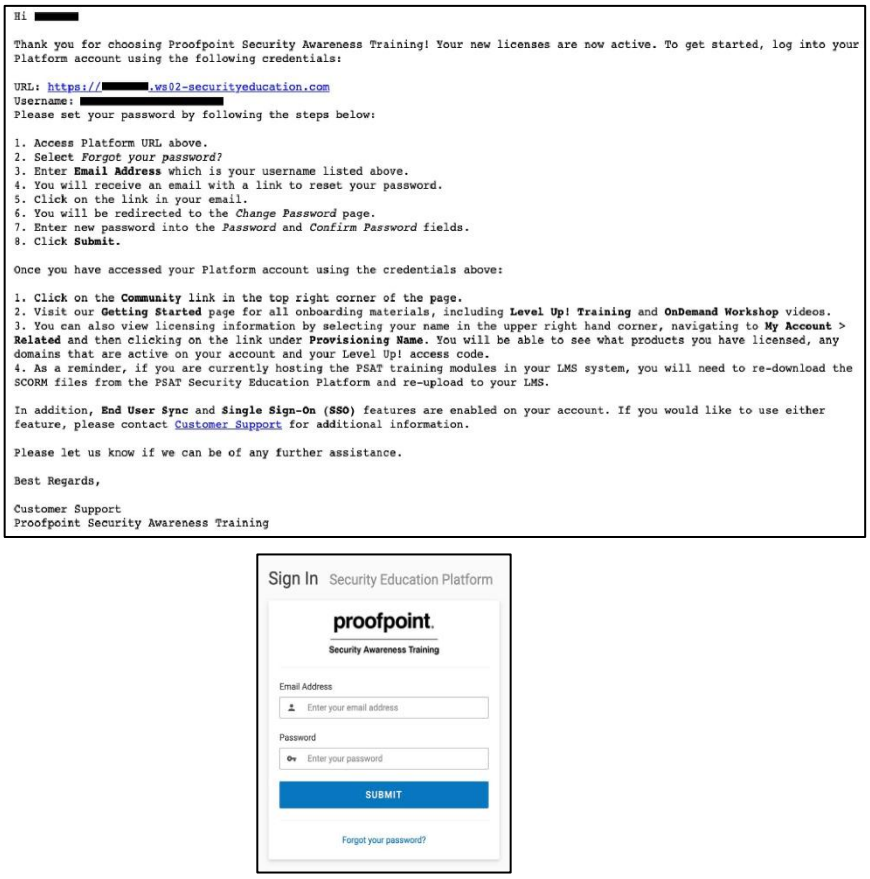

Ilustración 3. Instrucciones proporcionadas en mensaje cifrado

4.2 ENTORNO DE INSTALACIÓN SEGURO

12. Proofpoint ofrece la plataforma de concienciación PSAT en formato SaaS y es mantenido con recursos gestionados por Proofpoint, por lo que el entorno de despliegue es responsabilidad del proveedor de la infraestructura.

4.3 REGISTRO Y LICENCIAS

13. Proofpoint ofrece dos licencias distintas: **Standard** y **Enterprise**. Las diferencias entre ellas son:
    a) Número de módulos de concienciación disponibles.
    b) Número de idiomas.
14. La licencia adquirida por el usuario final no impacta en la funcionalidad de seguridad cualificada. Por tanto, ambas licencias se consideran bajo el alcance del presente documento.

4.4 REQUISITOS DE LOS PUESTOS DE TRABAJO

15. Proofpoint ofrece la plataforma de concienciación PSAT en formato SaaS mantenido con recursos gestionados por Proofpoint, por lo que no se necesita realizar consideraciones previas acerca de componentes adicionales o modelo de arquitectura.

16. Por su parte, se deberán tener en cuenta los requisitos aplicables a los puestos de trabajo que accederán a la plataforma:

Recurso	Usuario consumidor	Usuario administrador
Sistema Operativo	Windows 11 Android Mac OS & iOS	Windows 11 Mac OS
Navegador Web	Navegadores de escritorio: Firefox, Google Chrome, Internet Explorer 11, Microsoft Edge, Safari for Mac OS Navegadores móviles: Chrome para Android, Safari para iOS	Navegadores de escritorio: Firefox, Google Chrome, Internet Explorer 11, Microsoft Edge, Safari para Mac OS
Procesador	1 GHz	1.5 GHz
Memoria RAM	1 GB	2 GB
Ancho de banda	1 Mbps	
Espacio en disco	20 MB	
Lector de pantalla	NV Access NVDA Screen Reader	

Tabla 1. Requisitos de los puestos de trabajo

4.5 VERIFICACIÓN DE ACCESIBILIDAD

17. Los recursos de la plataforma de concienciación PSAT son gestionados por Proofpoint. No obstante, el usuario deberá comprobar su accesibilidad a un listado de URLs y direcciones IP de interés. Esto se debe a que, por ejemplo, una simulación de phishing manda un mensaje falso de phishing a los usuarios y, por tanto, se deberá permitir su tránsito hasta el buzón en cuestión, haciendo una excepción o lista blanca en los entornos de protección del correo electrónico. También se deben considerar las URLs concretas de las comunicaciones con la plataforma, sincronización de usuarios, funcionalidad PhishAlarm y Analyzer o notificaciones, para permitirlas en caso de estar bloqueadas y obtener un perfecto funcionamiento de la plataforma.
18. El detalle actualizado de las comunicaciones utilizadas por PSAT se encuentra en [REF1].

5 FASE DE INSTALACIÓN

19. El cliente no deberá llevar a cabo un proceso de instalación debido a que Proofpoint realiza la provisión de recursos en formato SaaS, ofreciendo el acceso a los sistemas a través de una única URL personalizada.

6 FASE DE CONFIGURACIÓN

6.1 AUTENTICACIÓN

20. La plataforma PSAT utiliza autenticación mediante Single Sign-On (SSO) con un proveedor de identidad corporativo (por ejemplo, Active Directory, Azure AD u otros). Las políticas de contraseñas, incluida una longitud mínima de 12 caracteres, la complejidad y la caducidad, se aplican en dicho proveedor de identidad, de acuerdo con los requisitos del Esquema Nacional de Seguridad (ENS) y las políticas internas de la organización. En el contexto cualificado de esta guía no se permitirá el uso de credenciales locales con políticas de contraseñas más débiles.
21. Por tanto, el mecanismo de autenticación de los usuarios de PSAT considerado como seguro bajo el alcance de este documento es el siguiente:
    - Single Sign-On (SSO): los usuarios podrán utilizar el método de autenticación de su empresa, integrada en PSAT a través de la federación de SAML 2.0.
22. Para habilitarlo e implementar la autenticación segura, tanto de los administradores como los usuarios finales de la plataforma, un contacto autorizado del cliente debe abrir un caso al soporte de Proofpoint en la página de Communities [REF5] con la siguiente información:
    - Prioridad: P3
    - Subject: Enable SSO
    - Description: Sistema a integrar con SSO (p. ej. ADFS, Azure AD, Okta, …) y cuál será el atributo utilizado (p. ej. correo electrónico)
    - Component: SSO
    - Sub-component: Implementation
23. Una vez creado el caso de soporte, se proporcionará documentación específica según tecnología y los metadatos asociados a PSAT para la implementación del SSO. La habilitación del SSO impedirá cualquier otro medio de autenticación.
24. Proofpoint ofrece la posibilidad de realizar la sincronización de usuarios de forma automatizada, tanto local (Microsoft Active Directory) como remota (Microsoft Azure Active Directory).
25. La funcionalidad de sincronización de usuarios con Microsoft AD y Azure AD, dispone de su guía de administración y configuración (End-User Synchronization - Administrator Guide) [REF2].

6.2 ADMINISTRACIÓN DEL PRODUCTO

6.2.1 ADMINISTRACIÓN REMOTA

26. La administración de PSAT es remota, a través de la interfaz web o webUI. Esta conexión se realiza a través del protocolo HTTPS (al puerto 443) y está protegida con TLS v1.2.

6.2.2 CONFIGURACIÓN DE ADMINISTRADORES

27. La plataforma PSAT permite el establecimiento de distintos usuarios administradores, con atribuciones diferenciadas. En caso de no seleccionarse ningún rol de administración, el

usuario tendrá por defecto el de User, que le permite acceder a la plataforma para consultar las formaciones asignadas y realizarlas.

28. El usuario inicial de acceso a la plataforma PSAT, dispone del rol especial denominado Super Administrator, que le permite un acceso sin restricción. Este usuario puede gestionar contraseñas de otros usuarios, además de eliminar usuarios y toda su información. Solo se puede asignar o desasignar este rol a través del soporte del servicio [REF6].

29. El usuario Super Administrator accede por primera vez mediante usuario y contraseña, como se indica en el apartado 4.1. Este usuario será el encargado de solicitar el cambio de método de autenticación a SSO, como se indica en el apartado 6.1. Y, una vez llevado a cabo el cambio a autenticación por SSO, todos los usuarios accederán al producto a través de SSO.

30. Los roles disponibles para asignar a los usuarios son:

    - *Training Administrator*: puede acceder a la gestión de usuarios y notificaciones, pero no puede eliminarlos ni gestionar contraseñas. Puede personalizar módulos de concienciación, asignarlos a usuarios y consultar los informes asociados.
    - *User Administrator*: puede acceder a la gestión de usuarios y gestionar contraseñas, pero no puede eliminar usuarios.
    - *Phishing Administrator*: puede acceder a la gestión de usuarios, pero no puede eliminarlos ni gestionar contraseñas. Puede editar y lanzar simulaciones de phishing, y configurar PhishAlarm y acceder a los informes de esta categoría.
    - *Reporting Administrator*: puede acceder a todos los informes de la plataforma.

31. Consulte [REF7] para más detalles sobre los privilegios disponibles en cada rol de usuario.

32. Se debe crear el mínimo número de usuarios con rol de administrador, siguiendo los principios de mínimo privilegio.

6.3 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

33. Proofpoint ofrece la plataforma de concienciación PSAT en formato SaaS mantenido con recursos gestionados por Proofpoint y accesible a través de su interfaz web. Esta conexión se realiza a través del protocolo HTTPS al puerto 443 y protegida con TLS v1.2, usando la cipher suite *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*. Esta configuración no es editable.

34. Se deben deshabilitar los protocolos TLS 1.0 y TLS 1.1 en los dispositivos de acceso a la plataforma PSAT. Para poder realizarlo, se deben seguir los siguientes pasos:

    a) Acceda a través de las propiedades de los navegadores, concretamente usando el botón "*Internet Properties*" (ubicado de forma general en el menú avanzado de *Opciones de Internet* de los navegadores más comunes):

35. Una vez desactivados los protocolos TLS 1.0 y TLS 1.1, también se deben limitar las cipher suites de TLS a aquellos considerados como Recomendados. Esta acción se puede hacer mediante GPO:

    a) Para editar la GPO, en el servidor de Active Directory, ir a Inicio > Herramientas Administrativas > Administración de Directivas de Grupo, hacer clic derecho en el GPO y seleccionar Editar.

b) En el Editor de Administración de Directivas de Grupo, navegar a Configuración del Equipo > Políticas > Plantillas Administrativas > Red > Configuración de SSL.

c) Hacer doble clic en "Orden de conjuntos de cifrado SSL".

d) En la ventana de "Orden de conjuntos de cifrado SSL", hacer clic en "Habilitado".

e) En el panel de Opciones, reemplazar todo el contenido del cuadro de texto de "Suites de Cifrado SSL" con la siguiente lista de cipher suites consideradas Recomendadas:

```
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_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CCM
TLS_ECDHE_ECDSA_WITH_AES_128_CCM
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
```

Nota: Las suites de cifrado aparecen en líneas separadas para facilitar la lectura. Cuando se pegue la lista en el cuadro de texto, las suites de cifrado deben estar en una sola línea sin espacios después de las comas.

f) Cerrar el Editor de Administración de Directivas de Grupo.

g) Para que la nueva política de grupo surta efecto, los equipos en el alcance deben ser reiniciados tras descargar la nueva GPO.

6.4 ACTUALIZACIONES

36. Proofpoint ofrece la plataforma de concienciación PSAT en formato SaaS mantenido con recursos gestionados por Proofpoint, por lo que la gestión de las actualizaciones es realizada por Proofpoint, sin que el usuario administrador deba realizar ninguna acción. Proofpoint informa a los usuarios administradores de las ventanas de trabajo y la posibilidad de la degradación del servicio (si lo hubiera), con la suficiente antelación para que se puedan reprogramar actividades que entren en conflicto.

37. Proofpoint mantiene una web de comprobación en tiempo real del estado de los servicios de la plataforma PSAT, accesible a través de [REF3] y que permite la suscripción por correo de mensajes.

6.5 AUDITORÍA

38. Proofpoint no suministra la capacidad de consultar el registro de eventos de auditoría a los usuarios administradores. Si se desea acceder a la información de auditoría, el usuario administrador deberá dirigirse al soporte de Proofpoint para su gestión ya que se permite la exportación de datos vía API con una autenticación usando *tokens*.

39. Los *tokens* de autenticación API, permiten el acceso a la información de *reporting* de PSAT, y permiten establecer una fecha de expiración (30, 90, 180, 365 días, fecha personalizada o nunca). Se recomienda establecer una fecha de expiración acorde a las políticas de retención de la organización. Cuando se genera un *token*, no podrá ser visualizado de nuevo, por lo que se recomienda guardarlo adecuadamente. Sólo se pueden disponer de 15 *tokens* activos simultáneamente.

40. La plataforma PSAT no dispone de la posibilidad de envío de información o registros de forma externa a un servidor *syslog*.

6.6 CONFIGURACIÓN DEL ANALYZER

41. En caso de utilizar el servicio de Analyzer, es necesario configurar correctamente dicha funcionalidad para asegurar que todos los datos son tratados dentro de la Unión Europea. Para ello:

    a) Acceder a la plataforma PSAT como Super Administrator.

    b) Navegar a PhishAlarm > Analyzer.

    c) Hacer clic en “Settings” en la esquina superior derecha.

    d) En la sección “Closed-Loop Email Analysis and Response (CLEAR) Settings”, configurar la opción “Analysis Location” a “European Union (EU)”.

6.7 DESPLIEGUE DE PHISHALARM

42. En caso de utilizar el servicio de notificación de correo sospechoso, PhishAlarm, es necesario configurar correctamente dicha funcionalidad para asegurar que todos los datos son tratados dentro de la Unión Europea. Para ello el método de despliegue a realizar es el despliegue PhishAlarm for Exchange mediante “Manifest Link”. Se pueden encontrar las instrucciones paso a paso de la configuración a realizar en la consola de Administración de Exchange en [REF4].

7 REFERENCIAS

Nota: El acceso a esta documentación se realiza desde el sitio web: https://community.securityeducation.com/, accesible desde la plataforma PSAT con un usuario autenticado. Para acceder, es necesario pulsar sobre el botón "*Community*", el cual redirige a la web mencionada. Desde ahí, ir a la sección de descargas para obtener el fichero en formato PDF de la guía deseada.

[REF1] Safelisting Guide

[REF2] End-User Synchronization - Administrator Guide

[REF3] https://status.wombatsecurity.com/

[REF4] https://community.securityeducation.com/s/article/PhishAlarm-Exchange

[REF5] https://community.securityeducation.com/

[REF6] https://www.proofpoint.com/es/support-services

[REF7] https://community.securityeducation.com/s/article/Platform-Administrator-Roles-and-Adding-Administrators

8 ABREVIATURAS

AD	Active Directory
ADFS	Active Directory Federation Services
AES	Advanced Encryption Standard
API	Application Programming Interface
CCM	Counter with CBC-MAC
CISO	Chief Information Security Officer
CLEAR	Closed Loop Email Analysis and Response
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad.
EU	European Union
GCM	Galois/Counter Mode
GPO	Group Policy Object
HTML	HyperText Markup Language
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
NPRE	Nexus People Risk Explorer
OS	Operating System
P3	Priority 3
PDF	Portable Document Format
PSAT	Proofpoint Security Awareness Training
RSA	Rivest-Shamir-Adleman
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
SSO	Single Sign-On
TAP	Targeted Attack Protection
TLS	Transport Layer Security
URL	Uniform Resource Locator
USB	Universal Serial Bus

VAP	Very Attacked People
webUI	web User Interface