centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1701

Procedimiento de empleo seguro
Proofpoint Security Awareness Training (PSAT)

Abril 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.04.18 12:00:33 +02'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: 083-22-126-7

Fecha de Edición: marzo de 2022

ÍNDICE

1. INTRODUCCIÓN

1. La solución de Proofpoint de capacitación en concienciación de seguridad, también conocida como Proofpoint Awareness Training o PSAT, 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. La plataforma, ofrecida en formato SaaS, cumple con los estándares WCAG 2.0 AA de accesibilidad para contenido web, autenticación unificada, así como las evaluaciones de seguridad y privacidad estadounidense y europeas, con cumplimiento GDPR.
4. A alto nivel, las funcionalidades que ofrece son las siguientes:

    a) 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.

    b) 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.

c) 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 de Proofpoint, para obtener un informe en tiempo real de las amenazas sospechosas informadas por los usuarios, ahorrando tiempo a los equipos de respuesta.

d) 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.

e) 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*) 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.

f) 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 concientización 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

5. El presente documento se desarrolla para la solución de concienciación de Proofpoint PSAT, o Proofpoint *Security Awareness Training*. Se centra en la **configuración segura de la solución**, por lo que no se incluye información detallada de instalación y configuración de elementos adicionales.
6. 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

7. El presente documento dispone de la siguiente estructura de apartados:

- **Apartado 4**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.
- **Apartado 5**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- **Apartado 6**. En este apartado se resumen un *checklist* de referencia.
- **Apartado 7**. En este apartado se recogen las referencias a otros documentos utilizadas.
- **Apartado 8**. En este apartado se recogen las distintas abreviaturas usadas.

4. FASE DE DESPLIEGUE E INSTALACIÓN

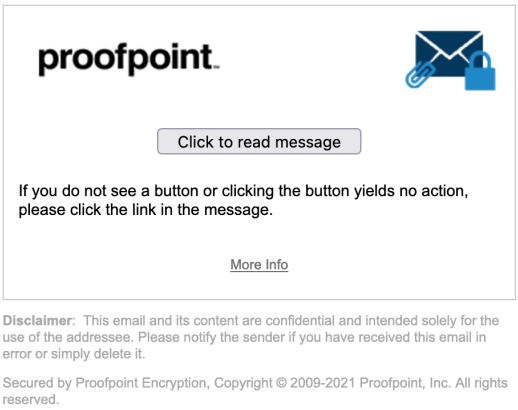
4.1 ENTREGA SEGURA DEL PRODUCTO

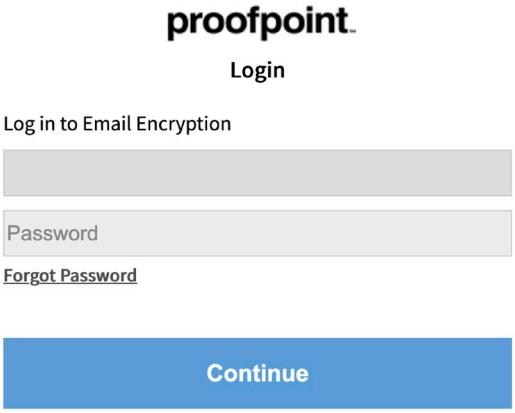
8. Proofpoint realiza la provisión de recursos para ofrecer la plataforma de concienciación PSAT en formato SaaS ofreciendo el acceso a los sistemas a través de una única URL personalizada.

9. La información acerca de la URL, así como la autenticación del usuario administrador, se realiza a través de un email. Este mensaje, se realiza desde una dirección de Proofpoint (no-reply@proofpoint.com) y con destinatario, la persona contacto del cliente y asunto, "*Welcome to Proofpoint Security Awareness Training!*".

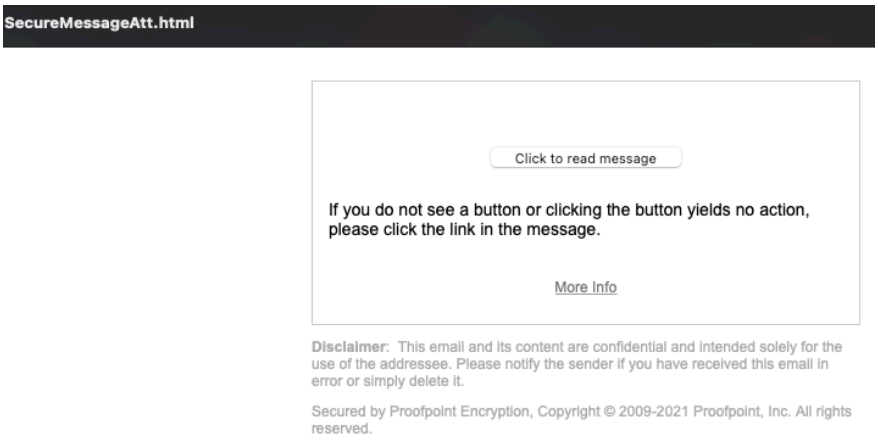
10. El mensaje se encuentra cifrado a través de la plataforma *Email Encryption* de Proofpoint. El usuario destinatario podrá acceder a la información a través del link "*Click here*" para acceder a la interfaz web de *Secure Reader* de Proofpoint para mensajes cifrados, donde podrá registrarse con su cuenta de email, utilizar unas credenciales creadas previamente, o recuperar su contraseña en caso de olvido (vía email).

11. A continuación, se muestran unas imágenes orientativas:





12. 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*.



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

Hi [redacted]

Thank you for choosing Proofpoint Security Awareness Training! Your new licenses are now active. To get started, log into your Platform account using the following credentials:

URL: https://[redacted].ws02-securityeducation.com
Username: [redacted]
Please set your password by following the steps below:

1. Access Platform URL above.
2. Select *Forgot your password?*
3. Enter **Email Address** which is your username listed above.
4. You will receive an email with a link to reset your password.
5. Click on the link in your email.
6. You will be redirected to the *Change Password* page.
7. Enter new password into the *Password* and *Confirm Password* fields.
8. Click **Submit.**

Once you have accessed your Platform account using the credentials above:

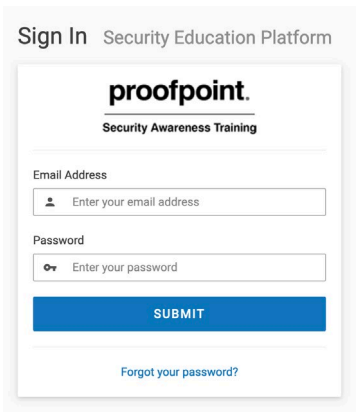
1. Click on the **Community** link in the top right corner of the page.
2. Visit our **Getting Started** page for all onboarding materials, including **Level Up! Training** and **OnDemand Workshop** videos.
3. You can also view licensing information by selecting your name in the upper right hand corner, navigating to **My Account** > **Related** and then clicking on the link under **Provisioning Name**. You will be able to see what products you have licensed, any domains that are active on your account and your Level Up! access code.
4. As a reminder, if you are currently hosting the PSAT training modules in your LMS system, you will need to re-download the SCORM files from the PSAT Security Education Platform and re-upload to your LMS.

In addition, **End User Sync** and **Single Sign-On (SSO)** features are enabled on your account. If you would like to use either feature, please contact Customer Support for additional information.

Please let us know if we can be of any further assistance.

Best Regards,

Customer Support
Proofpoint Security Awareness Training



4.2 ENTORNO DE INSTALACIÓN SEGURO

14. Proofpoint ofrece la plataforma de concienciación PSAT en formato SaaS (*Software as a Service*) mantenido con recursos gestionados por Proofpoint, por lo que el entorno de despliegue es responsabilidad del proveedor de la infraestructura.

4.3 REQUISITOS DE LOS PUESTOS DE TRABAJO

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

16. 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 10, 8.1 Android Mac OS & iOS	Windows 10, 8.1 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	

4.4 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 es debido, 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 la guía *Safelisting Guide* [REF.1].

5. FASE DE CONFIGURACIÓN

5.1 ADMINISTRACIÓN DEL PRODUCTO

5.1.1 ADMINISTRACIÓN REMOTA

19. La administración de PSAT es remota, a través de la interfaz web o webUI. Esta conexión se realiza a través del protocolo https (tcp#443) y cifrada con un certificado TLS.

5.1.2 CONFIGURACIÓN DE ADMINISTRADORES

20. 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.
21. El usuario inicial de acceso a la plataforma PSAT, dispone del rol especial denominado *Super Administrator*, que le permite un acceso sin restricción, y puede gestionar contraseñas de otros usuarios y eliminar usuarios y toda su información). Solo se puede asignar este rol o quitarlo, a través del soporte de la herramienta de Proofpoint.
22. Los roles que seleccionar en la edición de los usuarios son:
    - *Training Administrator*: permite un acceso sin restricción a la plataforma, pero no puede destruir usuarios o gestionar contraseñas; puede acceder a la gestión de usuarios y notificaciones, personalizar módulos de formación, así como sus asignaciones, pero no acceder a la sección de simulaciones de *phishings* o configuraciones de *PhishAlarm*, así como los informes relacionados con esta categoría.
    - *User Administrator*: puede acceder a la gestión de usuarios, pero no puede destruirlos; puede gestionar contraseñas, pero no acceder a la sección de simulaciones de *phishings* o configuraciones de *PhishAlarm*, así como los informes relacionados con esta categoría.
    - *Phishing Administrator*: puede acceder a la gestión de usuarios, pero no puede destruirlos ni gestionar contraseñas; puede editar y lanzar simulaciones de *phishing*, y configurar *PhishAlarm*, pero no puede acceder a los informes de otras categorías.
    - *Reporting Administrator*: no puede gestionar contraseñas, pero puede acceder a todos los informes de la plataforma.
23. Se debe crear el mínimo número de usuarios con rol de administrador, siguiendo los principios de mínimo privilegio.

5.2 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

24. Proofpoint ofrece la plataforma de concienciación PSAT en formato SaaS (*Software as a Service*) mantenido con recursos gestionados por Proofpoint y accesible a través de su interfaz web, tanto en el acceso de usuario consumidor, como del usuario administrador. Esta conexión se realiza a través del protocolo https (tcp#443) y cifrada con un certificado TLS (*TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*, TLS 1.2). Esta configuración no es editable.

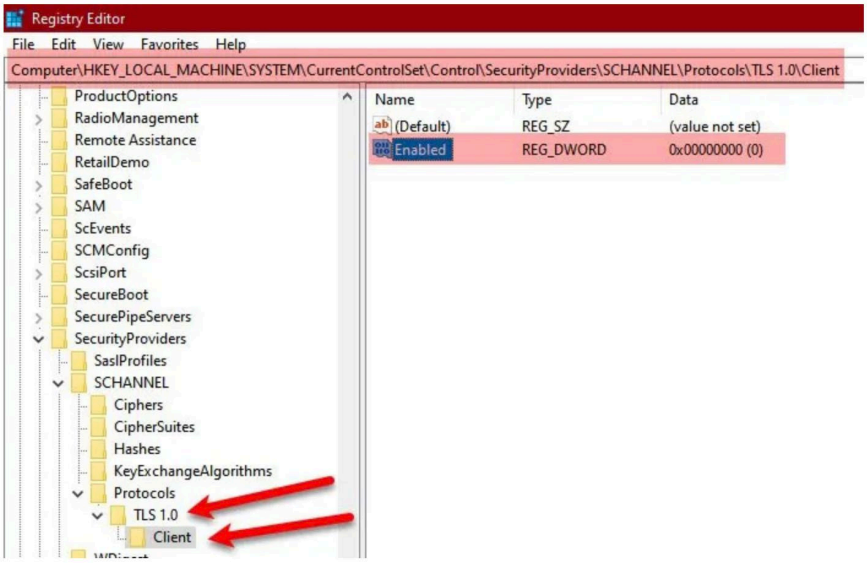
25. Se deben deshabilitar los protocolos TLS 1.0 y TLS 1.1 en los dispositivos de acceso a la plataforma PSAT. Para poder realizarlo, se deben seguir los siguientes pasos:

    a) Acceder al editor de registro de un dispositivo Windows (*Registry Editor*).

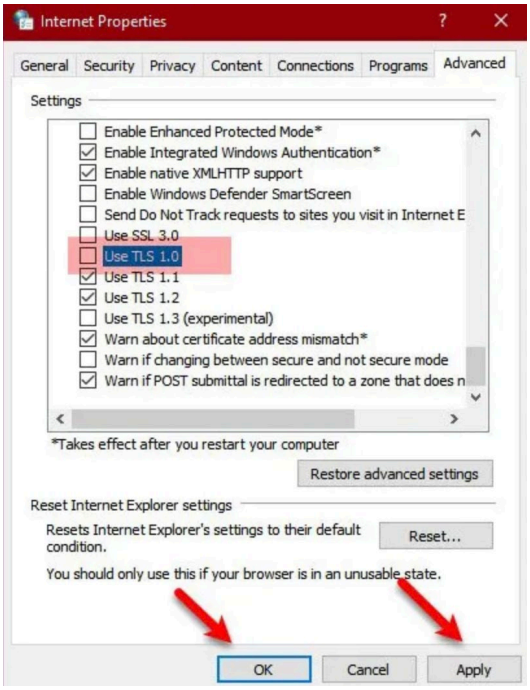
    b) Localizar la clave:

    Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

    y añadir dos (2) nuevas *keys* de tipo DWORD (32-bit) llamadas TLS 1.0 y 1.1 y generar en su interior una *key* llamada *Client* que contendrán una nueva *key* DWORD (32 bit) llamada *Enabled* con el valor a 0, en cada una de ellas.



26. También se puede deshabilitar los protocolos TLS 1.0 y 1.1 a través de las propiedades de los navegadores, concretamente usando el botón "*Internet Properties*" (ubicada de forma general en el menú avanzado de *Opciones de Internet* de los navegadores más comunes):



5.3 AUTENTICACIÓN

27. Los mecanismos de autenticación de usuarios de PSAT son los siguientes:

    - Credenciales locales: los usuarios que accedan a la plataforma pueden realizar la autenticación mediante el uso de un usuario local, consistente en una cuenta de correo electrónico para su identificación, así como una contraseña alfanumérica. Los usuarios podrán establecer sus propias contraseñas, así como solicitar un reinicio de estas. Podrán aplicarse configuraciones de complejidad y expiración.
    - Acceso directo: los usuarios reciben un link único a la formación asignada, que les permite el acceso a la plataforma. Este método permite a cualquier usuario hacer clic y acceder como si fuera el usuario original y receptor del enlace.
    - *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.

28. Proofpoint ofrece la posibilidad de realizar la sincronización de usuarios de forma automatizada, tanto local (*Microsoft Active Directory*) como remota (Micro*soft Azure Active Directory*).

29. 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*) [REF.2].

5.4 POLÍTICA DE CONTRASEÑAS

30. La plataforma PSAT cuenta con una política predefinida de contraseñas locales, que dispone de los siguientes requisitos:

    - Longitud de 8 caracteres (configurable entre 6 y 30). Se deben configurar contraseñas de mínimo 12 caracteres.

- **Complejidad**. La contraseña debe tener, al menos, un carácter en minúscula, un carácter en mayúscula, un número y un símbolo.
- Expiración:
    - Debe **comprobar las últimas 3 contraseñas introducidas** para que no se repitan (configurable entre 1 y 25).
    - Debe poder **bloquear la cuenta del usuario tras 3 intentos erróneos** de autenticación (configurable entre 1 y 20)
    - Debe obligar a cambiar la contraseña cada 365 días (configurable entre 1 y 365). **Se deben configurar 60 días, como máximo.**
    - Debe bloquear la cuenta de un usuario inactivo tras 90 días (configurable entre 1 y 365)

5.5 ACTUALIZACIONES

31. Proofpoint ofrece la plataforma de concienciación PSAT en formato SaaS (*Software as a Service*) mantenido con recursos gestionados por Proofpoint, por lo que la gestión de las actualizaciones de firmware y software 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.
32. Proofpoint mantiene una web de comprobación en tiempo real del estado de los servicios de la plataforma PSAT, accesible a través de *https://status.wombatsecurity.com/* y que permite la suscripción por correo de mensajes.

5.6 AUDITORÍA

33. 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*.
34. Los *tokens* de autenticación API, permiten el acceso a la información de *reporting* de PSAT, y permite 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.
35. La plataforma PSAT no dispone de la posibilidad de envío de información o registros de forma externa a un servidor *syslog*.

6. *CHECKLIST*

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Verificar los requisitos de los *endpoints*	☐	☐	
Verificar la accesibilidad a todos los recursos	☐	☐	
CONFIGURACIÓN			
Aplicar una configuración segura de contraseñas	☐	☐	
Aplicar el principio de mínimo privilegio	☐	☐	
Deshabilitar el uso de TLS1.0 y TLS1.1 en los *endpoints*	☐	☐	
Considerar las ventanas de trabajo de *Proofpoint*	☐	☐	
Configurar fecha de expiración de registros	☐	☐	

7. REFERENCIAS

REF1 *Safelisting Guide*

REF2 *End-User Synchronization - Administrator Guide*

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.

8. ABREVIATURAS

API *Application Programming Interface*

CLEAR *Closed Loop Email Analysis and Response*

GDPR *General data Protection Regulation*

LDAP *Lightweight Directory Access Protocol*

NPRE *Nexus People Risk Explorer*

PSAT *Proofpoint Security Awareness Training*

SaaS *Software as a Service*

SAML *Security Assertion Markup Language*

SASL *Simple Authentication and Security Layer*

SSL *Secure Sockets Layer*

SSO *Single Sign-On*

TAP *Targeted Attack Protection*

VAP *Very Attack People*

WCAG *Web Content Accessibility Guidelines*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL