





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

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

NIPO: 083-24-200-8.

Fecha de Edición: mayo de 2024.



CENTRO CRIPTOLOGICO
NACIONAL
cn=CENTRO CRIPTOLOGICO
NACIONAL, 2.5.4.97=VATES-
S2800155J, ou=CENTRO
CRYPTOLOGICO NACIONAL,
o=CENTRO CRIPTOLOGICO
NACIONAL, c=ES
2024.05.31 13:27:11 +02'00'

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

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

ÍNDICE

ÍNDICE.....	2
1. INTRODUCCIÓN	3
2. OBJETO Y ALCANCE	4
3. ORGANIZACIÓN DEL DOCUMENTO	5
4. FASE PREVIA A LA INSTALACIÓN.....	6
4.1 ENTREGA SEGURA DEL PRODUCTO	6
4.2 ENTORNO DE INSTALACIÓN SEGURO	6
4.3 REGISTRO Y LICENCIAS	6
5. FASE DE CONFIGURACIÓN	7
5.1 AUTENTICACIÓN.....	7
5.2 ADMINISTRACIÓN DEL PRODUCTO.....	7
5.2.1 ADMINISTRACIÓN LOCAL Y REMOTA.....	7
5.2.2 CONFIGURACIÓN DE ADMINISTRADORES	7
5.3 SERVIDORES DE AUTENTICACIÓN	7
5.4 ACTUALIZACIONES	8
5.5 AUDITORÍA	8
6. FASE DE OPERACIÓN	9
7. REFERENCIAS	10
8. ABREVIATURAS.....	11

1. INTRODUCCIÓN

1. Kymatio es una plataforma de gestión del ciberriesgo, la monitorización de exposición de credenciales y la concienciación en ciberseguridad, ofrecida en formato SaaS. Kymatio tiene como objetivo fortalecer el personal de las empresas, identificar posibles riesgos, señalar áreas críticas a trabajar y comprobar el nivel de alerta de los empleados.
2. Kymatio permite emprender acciones automáticas de sensibilización mediante el uso de plantillas para prevenir incidentes internos.
3. Los usuarios son proporcionados con un espacio propio en el que acceder a todos los recursos educativos facilitados por la plataforma. La solución de Kymatio permite a la empresa evaluar el conocimiento de los empleados mediante una serie de exámenes disponibles en la plataforma denominados “sesiones”. Los empleados son después asignados con una puntuación denominada “estado de alerta”, en base a los resultados de estas sesiones.
4. Los usuarios son agrupados en departamentos. Desde la plataforma puede consultarse tanto información sobre cada empleado y departamento como el estado de alerta, campañas de seguridad activas de las que forman parte y brechas de seguridad en las que han estado involucrados.
5. Es posible realizar simulaciones de ataques sobre los empleados y departamentos con el fin de evaluar la reacción de estos. El usuario operador puede comprobar el estado de todas las campañas activas desde la plataforma.

2. OBJETO Y ALCANCE

6. El objeto del presente documento es servir como guía de configuración segura para la solución de concienciación Kymatio.
7. Esta solución ha sido incluida en la familia “Formación y Concienciación de la Ciberseguridad” de Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC), en el listado de productos y servicios de “Conformidad y Gobernanza”.

3. ORGANIZACIÓN DEL DOCUMENTO

9. Este documento se compone de los siguientes apartados:

- 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 las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- c) Apartado **6**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
- d) Apartado **7**. En este apartado se recogen las referencias utilizadas a otros documentos.
- e) Apartado **8**. En este apartado se recogen las distintas abreviaturas usadas y su significado.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. Kymatio proporciona acceso a sus recursos a través de su aplicación web, otorgando a los usuarios cuentas y roles personalizados, para su autenticación en la misma.
11. El alta de una organización en la plataforma se puede realizar siguiendo dos métodos: solicitud vía email o desde la plataforma <https://app.kymatio.com/> con un perfil de administrador (rol distinto al rol de administrador proporcionado a los usuarios). Ambos métodos aparecen descritos en las páginas 8 y 9 del documento *Kymatio – Onboarding* [REF1].

4.2 ENTORNO DE INSTALACIÓN SEGURO

12. Kymatio ofrece su solución en formato SaaS (*Software as a Service*), por lo que el entorno de despliegue es responsabilidad del proveedor de la infraestructura.

4.3 REGISTRO Y LICENCIAS

13. Para obtener información acerca del acuerdo de licencia de la aplicación de Kymatio, consultar sección 2 del documento *Kymatio – Onboarding* [REF1].

5. FASE DE CONFIGURACIÓN

5.1 AUTENTICACIÓN

15. Se utilizan contraseñas alfanuméricas como mecanismo de autenticación para los tres tipos de usuario disponibles (usuario, operador y administrador). Los usuarios pueden elegir cambiar su contraseña desde su perfil.
16. El usuario administrador puede configurar:
 - a) Días de vigencia de las contraseñas.
 - b) Número de veces que la contraseña no puede ser igual a las anteriores.

5.2 ADMINISTRACIÓN DEL PRODUCTO

5.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

17. La administración de Kymatio se realiza de forma remota mediante la interfaz web. Esta conexión se realiza a través del protocolo HTTPS.

5.2.2 CONFIGURACIÓN DE ADMINISTRADORES

18. La aplicación de Kymatio cuenta con un único rol administrador, el cual se encarga de la gestión de usuarios, departamentos y compañía.
19. Respecto a la gestión de la compañía, el usuario administrador puede modificar los siguientes aspectos de la política de contraseña que tiene estos valores por defecto:
 - a) Histórico de contraseñas: 10 contraseñas anteriores.
 - b) Vigencia de la contraseña: 90 días.
20. Para ello, el administrador ha de acceder al Dashboard (<https://app.kymatio.com/admin/dashboard/>), y editar la compañía que este administra.
21. Por defecto, la fortaleza de la contraseña ya cumple con los requisitos mínimos, puesto que esta requiere de: 12 caracteres, compuestos por mayúsculas, minúsculas, números y caracteres especiales.

5.3 SERVIDORES DE AUTENTICACIÓN

22. Kymatio permite el uso de los siguientes servidores externos de autenticación:

Federación SAML 2.0.
23. Para su configuración, consultar la guía *Manual Federación y Provisión Automática – Azure AD* [REF2].

5.4 ACTUALIZACIONES

24. Kymatio ofrece su solución en formato SaaS, mantenido con recursos gestionados y proporcionados por Kymatio, por lo que la gestión de actualizaciones es realizada por parte de Kymatio, sin requerir acciones por parte del usuario.

5.5 AUDITORÍA

25. Kymatio no ofrece la capacidad de consultar registros de eventos de auditoría a ninguno de sus usuarios.
26. De igual manera, Kymatio no ofrece la posibilidad de configuración de servidores externos *syslog*.

6. FASE DE OPERACIÓN

28. Kymatio ofrece distintos roles de usuarios, diferenciados entre sí por las acciones que estos pueden realizar:
 - a) Rol administrador: Encargado de la gestión de la compañía, usuarios y departamentos.
 - b) Rol operador: Encargado de la visualización e interpretación de la información de los servicios ofertados por la aplicación, así como de la creación y gestión de campañas de simulación de ataques.
 - c) Rol usuario: Rol más básico, cuyas funcionalidades se limitan a participar en campañas de concienciación y servicios formativos.
29. El usuario administrador es el único usuario que dispone de los permisos necesarios para llevar a cabo las siguientes funcionalidades:
 - a) Creación y gestión de usuarios. Para obtener información respecto a esta funcionalidad, consultar las páginas 4 y 5 de la guía *Kymatio – Manual de Administración* [REF3].
 - b) Creación y gestión de departamentos. Para obtener información respecto a esta funcionalidad, consultar páginas 6 y 7 de la guía *Kymatio – Manual de Administración* [REF3].
 - c) Gestión de la información de la organización que administra. Dentro de esta funcionalidad, destaca la gestión de algunos parámetros de la política de contraseñas de dicha organización, los cuales están descrito en la sección 5.2.2 de este mismo documento.
30. De forma adicional, la creación de usuarios y departamentos también se puede llevar a cabo de las siguientes maneras:
 - a) Carga mediante Excel/CSV: Rellenando la **plantilla de carga en Excel** accesible desde la página 10 del documento *Kymatio – Onboarding* [REF1], y realizando la petición a Soporte Usuarios de Kymatio (soporte_usuarios@kymatio.com).
 - b) Provisión automática mediante protocolo SCIM: Proceso descrito en la guía *Manual Federación y Provisión Automática – Azure AD* [REF2].
31. Para obtener información acerca de la operación del rol operador, consultar manual *Kymatio – Manual de Operador de Plataforma* [REF4].
32. Para obtener información acerca de la operación del rol usuario, consultar manual *Kymatio – Manual del Empleado* [REF5].

7. REFERENCIAS

- REF1** Kymatio – *Onboarding*. Versión 1.4.1
- REF2** Manual Federación y Provisión Automática – Azure AD. Versión 1.2
- REF3** Kymatio – Manual de Administración. Versión 1.1
- REF4** Kymatio – Manual de Operador de Plataforma. Versión 2.1
- REF5** Kymatio - Manual del Empleado. Versión 1.2

8. ABREVIATURAS

AD	<i>Active Directory</i>
CPSTIC	Catálogo de Productos y Servicios STIC
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
SaaS	<i>Software as a Service</i>
SAML	<i>Security Assertion Markup Language</i>
STIC	Seguridad de las Tecnologías de la Información y la Comunicación

