

Guía de Seguridad de las TIC

CCN-STIC 1655

Procedimiento de Empleo Seguro

Email Guardian



Octubre 2025



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

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2025
NIPO: 083-26-137-2



Fecha de Edición: Octubre de 2025

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.05.05 13:11:50 +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

1 INTRODUCCIÓN	3
2 OBJETO Y ALCANCE	5
3 ORGANIZACIÓN DEL DOCUMENTO	6
4 FASE PREVIA A LA INSTALACIÓN	7
4.1 ENTREGA SEGURA DEL PRODUCTO	7
4.2 ENTORNO DE INSTALACIÓN SEGURO	7
4.3 REGISTRO Y LICENCIAS	7
4.4 CONSIDERACIONES PREVIAS	7
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN	7
5 FASE DE INSTALACIÓN	8
5.1 FILTRADO DE CORREO ENTRANTE	8
5.2 FILTRADO DE CORREO SALIENTE	8
6 FASE DE CONFIGURACIÓN	9
6.1 MODO DE OPERACIÓN SEGURO	9
6.2 AUTENTICACIÓN	9
6.3 ADMINISTRACIÓN DEL PRODUCTO	9
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA	9
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES	9
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS	10
6.5 GESTIÓN DE CERTIFICADOS	10
6.6 SERVIDORES DE AUTENTICACIÓN	10
6.7 SINCRONIZACIÓN	10
6.8 ACTUALIZACIONES	11
6.9 AUTO-CHEQUEOS	11
6.10 ALTA DISPONIBILIDAD	11
6.11 AUDITORÍA	11
6.11.1 REGISTRO DE EVENTOS	11
6.11.2 ALMACENAMIENTO LOCAL	11
6.11.3 ALMACENAMIENTO REMOTO	11
6.12 BACKUP	11
6.13 FUNCIONES DE SEGURIDAD	12
7 FASE DE OPERACIÓN	13
8 REFERENCIAS	14
9 ABREVIATURAS	15

1 INTRODUCCIÓN

1. El servicio **EMAIL GUARDIAN**, del fabricante español IBERLAYER, en adelante referido como TOE, es una solución SaaS basada en la nube diseñada para proteger a las organizaciones frente a una variedad de amenazas digitales, optimizando la seguridad a través de la nube sin necesidad de hardware adicional.
2. AMBAR®, el núcleo tecnológico de **EMAIL GUARDIAN**, es un sistema de detección y filtrado de correo electrónico no deseado que analiza miles de elementos en cada mensaje para evaluar su seguridad. Esta tecnología permite al TOE lograr una tasa de detección y bloqueo de correos “basura” y maliciosos, asegurando así la integridad y la seguridad de las comunicaciones por correo electrónico.
3. El TOE proporciona un amplio abanico de funciones que son utilizadas para la gestión de detecciones de incidencias y sus posibles soluciones:
 - **Análisis de Reputación:** Monitorea y controla IPs y dominios para determinar su ubicación, uso y propósitos.
 - **Análisis del Contexto:** Investiga el propósito y contenido de los correos electrónicos para identificar quién los envía y por qué.
 - **Análisis de Adjuntos:** Utiliza múltiples motores antivirus para detectar malware en archivos adjuntos, incluso los cifrados.
 - **Sandbox de Tiempo-Real:** Proporciona un entorno de pruebas para identificar amenazas no detectadas por los antivirus en menos de tres segundos.
 - **Protección Anti-Fraude y Anti-Phishing:** Protege contra fraudes específicos y phishing, analizando técnicas de suplantación y controlando protocolos como SPF, DKIM y DMARC.
 - **Análisis de Enlaces e Imágenes:** Evalúa URLs y escanea textos, metadatos y códigos en imágenes para determinar seguridad y riesgos.
 - **IA Aplicada a la Seguridad:** Emplea inteligencia artificial para analizar el comportamiento de los usuarios y la gramática de los textos.
 - **Parches Virtuales:** Ofrece soluciones de seguridad para dispositivos no actualizados, protegiéndolos de vulnerabilidades.
 - **Data Loss Prevention (DLP):** Ayuda a prevenir la fuga de datos a través del correo electrónico y archivos adjuntos.
 - **Consola Web y Servicio desde la Nube:** Proporciona una interfaz en tiempo real accesible desde cualquier lugar, sin instalaciones complicadas y con un soporte técnico 24/7 en múltiples idiomas.
4. Por último, **EMAIL GUARDIAN** implementa las siguientes funciones de seguridad:
 - **Administración confiable:** El TOE puede ser gestionado por usuarios (clientes del servicio), con distintos tipos de roles y permisos, mediante HTTPS. Por otro lado, existe un rol de administrador de servicio, únicamente disponible para empleados de Iberlayer, que se encargan de la gestión y configuración a nivel de máquina de los componentes del TOE a través de SSHv2.
 - **Identificación y autenticación:** El TOE realiza una identificación y autenticación en todas sus interfaces. Para la consola web (HTTPS), se usa un mecanismo de autenticación basado en usuario y contraseña. Para los administradores del servicio, los cuales acceden a nivel de máquina a los componentes del TOE (SSHv2), además del mecanismo de usuario y contraseña, disponen de una restricción basada en IP.

- **Auditoría:** El TOE genera, almacena y protege los registros de auditoría relativos a su funcionalidad y configuración.
 - **Canales seguros:** El TOE establece canales de comunicación seguros para el intercambio de información sensible, a través de los protocolos SSHv2 y TLS 1.3, tanto en los canales de administración como en la comunicación entre distintas partes del TOE.
 - **Instalación y actualización confiables:** Al tratarse de un producto SaaS, el TOE no permite a sus usuarios (clientes) realizar actualizaciones sobre él. No obstante, esta actualización es realizada por parte de los administradores del servicio (empleados de Iberlayer).
 - **Protección de credenciales y datos sensibles:** El TOE protege sus datos críticos mediante el uso de protecciones criptológicas y controles de acceso.
 - **Requisitos criptográficos:** El TOE implementa funciones y algoritmos criptográficos que cumplen con lo establecido en la guía [CCN-STIC-807], impidiendo el acceso en claro a parámetros de seguridad del sistema. En este contexto, las credenciales del TOE se encuentran en forma de funciones resumen para su protección.
5. **Protección de correo electrónico:** El TOE implementa las siguientes funciones relativas a la protección de correo electrónico:
- Análisis de correo tanto entrante como saliente.
 - Análisis completo de: cabecera, cuerpo y adjuntos.
 - Múltiples técnicas de análisis de correo electrónico.
 - Uso de reglas para la detección de patrones de texto.
 - Permitir al usuario elegir entre distintas acciones tras detectar correo malicioso.
 - Uso de listas blancas y negras.

2 OBJETO Y ALCANCE

6. El objeto del presente documento es servir como guía para realizar una instalación, configuración y operación segura del producto Email Guardian.
7. El servicio Email Guardian ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTA en la familia “Protección de correo electrónico”.

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.
- d) Apartado 7. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. Dado que el producto Email Guardian se trata de un producto SaaS, no se realiza una entrega como tal del producto. No obstante, para dar de alta a sus clientes en el servicio de Email Guardian, el fabricante, Iberlayer, proporciona un documento de alta que debe de ser rellenado por el cliente. En este mismo documento, se proporcionará al cliente las cuentas para acceder a la consola de administración del producto.

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. IBERLAYER ofrece la plataforma de protección de correo Email Guardian en formato SaaS (Software as a Service), el cual se encuentra mantenido por los recursos propios de IBERLAYER, no siendo necesaria la instalación de componentes adicionales.

4.3 REGISTRO Y LICENCIAS

10. IBERLAYER ofrece la plataforma de protección de correo Email Guardian en formato SaaS (Software as a Service). Por tanto, el cliente no realiza una gestión de licencias, las cuales son gestionadas por los propios empleados de IBERLAYER.

4.4 CONSIDERACIONES PREVIAS

11. Durante la instalación del producto, dependiendo del tipo de cliente de correo del que se disponga, será necesario aplicar una configuración u otra. Por este motivo, y debido a la constante actualización de dichos clientes de correo, los administradores de Iberlayer ayudarán al cliente, mediante una sesión en conjunto, a configurar aquellos parámetros específicos de cada entorno.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

12. El servicio es formado por los siguientes componentes:
 - **Admin Center:** Consola de administración accesible vía navegador web, protegida mediante el protocolo TLS 1.3.
 - **Servidores de filtrado:** Servidor en los que se realiza el análisis del correo entrante y/o saliente del cliente. El intercambio entre estos servidores se encuentra protegido mediante TLS 1.3.

5 FASE DE INSTALACIÓN

13. Al tratarse de un producto SaaS, lo único que se requiere para ser utilizado es realizar la siguiente configuración:

5.1 FILTRADO DE CORREO ENTRANTE

14. Para que Email Guardian realice el filtrado del correo entrante, es necesario introducir los registros MX en nuestro servidor DNS. Estos registros MX serán proporcionados por Iberlayer a la hora de rellenar el formulario de alta del cliente.

5.2 FILTRADO DE CORREO SALIENTE

15. Para que Email Guardian realice el filtrado del correo saliente, es necesario añadir lo siguiente a nuestra configuración de cliente de correo:
 - Smarthost.
 - Registro SPF.
16. Esta configuración será proporcionada por Iberlayer a la hora de rellenar el formulario de alta del cliente. Además, en caso de que sea necesario, los empleados de Iberlayer asistirán al cliente en la configuración de dichos registros.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

17. IBERLAYER ofrece la plataforma de protección de correo Email Guardian en formato SaaS (Software as a Service), el cual se encuentra mantenido por los recursos propios de IBERLAYER, no siendo necesaria ninguna configuración específica para operar en el modo de cumplimiento de la certificación funcional.

6.2 AUTENTICACIÓN

18. El proceso de autenticación de usuarios de *Email Guardian* se realiza mediante el uso de credenciales almacenadas en los servidores de la plataforma. Dichas credenciales constan de un nombre, para identificación de usuario, y una contraseña, para su autenticación.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

19. El proceso de administración de *Email Guardian* se realiza de forma remota, mediante la interfaz web, *Admin Center*, accesible a través del protocolo HTTP sobre TLS 1.3.
20. Los certificados usados por el servidor usan RSA con una longitud de clave de 3072 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

21. La consola web, *Admin Center*, es accesible por usuarios autorizados con los permisos adecuados, basado en un control de acceso por roles. Dichos roles, así como los permisos de cada uno, se detallan en la siguiente tabla:

ROL	LECTURA COMPLETA	ESCRITURA COMPLETA	LECTURA SOLO CABECERAS	ESCRITURA SOLO CABECERAS	ACCESO MAPA MUNDI
Administrador con Restricción de RGPD			✓	✓	✓
Administrador sin Restricción de RGPD	✓	✓			✓
Helpdesk con Restricción de RGPD			✓		✓
Helpdesk sin Restricción de RGPD				✓	✓
Kiosko					✓

Tabla 1. Roles y permisos

22. Cabe destacar que la asignación de roles es realizada por parte de los administradores del servicio, empleados de Iberlayer, durante el proceso de alta en el servicio.
 - Por otro lado, *Admin Center* cuenta con la siguiente política de contraseñas:
 - Longitud mínima: 12 caracteres.
23. Composición de la contraseña: letras mayúsculas, letras minúsculas, números y caracteres especiales [“!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, “”].
24. Las contraseñas iniciales son proporcionadas por Iberlayer durante el proceso de alta del cliente. Una vez se realice el primer inicio de sesión en la consola web, se solicita el cambio de las mismas.
25. El cambio de contraseña de la consola web se realiza accediendo al perfil del usuario dentro de la misma. Para ello, acceder *Admin Center* y pulsar sobre el perfil en la esquina superior derecha. A continuación, hacer click sobre el botón “Change password”.
26. Para finalizar, la sesión de *Admin Center* cuenta con los siguientes parámetros de protección:
 - Tiempo de inactividad: 2 horas.
 - Tras 3 intentos fallidos: Solicita CAPTCHA.
 - Tras 5 intentos fallidos: bloqueo de sesión durante 5 minutos.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

27. El servicio no requiere que el cliente realice ninguna configuración adicional respecto a las interfaces, puertos y servicios.
28. La configuración requerida para que el servicio actúe como proxy ya se ha identificado en la sección 5 FASE DE INSTALACIÓN.
29. El acceso a *Admin Center* se realiza mediante el uso de HTTP sobre TLS 1.3. El intercambio de correos entre la infraestructura del cliente y la infraestructura del servicio se realiza mediante SMTP sobre TLS 1.3.

6.5 GESTIÓN DE CERTIFICADOS

30. La gestión de certificados forma parte de la infraestructura del servicio, por lo que el cliente no precisa de ninguna acción por su parte.
31. Los certificados usados por *Admin Center* usan RSA con una longitud de clave de 3072 bits.

6.6 SERVIDORES DE AUTENTICACIÓN

32. Dado que Email Guardian se trata de un producto SaaS, no se precisa ninguna configuración adicional.

6.7 SINCRONIZACIÓN

33. Dado que Email Guardian se trata de un producto SaaS, la sincronización horaria es gestionada por Iberlayer, sin que el usuario deba realizar ninguna acción.

6.8 ACTUALIZACIONES

34. Dado que Email Guardian se trata de un producto SaaS, la gestión de las actualizaciones es realizada por Iberlayer, sin que el usuario deba realizar ninguna acción.
35. Para consultar la versión actual, desde la consola web de Email Guardian, pulsar sobre el botón “Customer License”.

6.9 AUTO-CHEQUEOS

36. Dado que Email Guardian se trata de un producto SaaS, los recursos del servicio son mantenidos por parte de Iberlayer, por lo que no precisa ninguna acción por parte del usuario.

6.10 ALTA DISPONIBILIDAD

37. Dado que Email Guardian se trata de un producto SaaS, los recursos del servicio son mantenidos por parte de Iberlayer, garantizando la redundancia, protección y alta disponibilidad del servicio.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

38. Dado que Email Guardian se trata de un producto SaaS, los registros de eventos son gestionados por Iberlayer, sin que el usuario deba realizar ninguna acción.
39. No obstante, el cliente puede acceder a los registros generados por el filtrado de correos. Estos registros son accesibles desde la consola web de Email Guardian, dentro de la ventana “Search”.

6.11.2 ALMACENAMIENTO LOCAL

40. Dado que Email Guardian se trata de un producto SaaS, el almacenamiento local es gestionado por Iberlayer, sin que el usuario deba realizar ninguna acción.

6.11.3 ALMACENAMIENTO REMOTO

41. El cliente puede solicitar el envío de los registros de auditoría de manera remota a sus sistemas. Para ello, los empleados de Iberlayer asistirán al cliente en la configuración necesaria.

6.12 BACKUP

42. Dado que Email Guardian se trata de un producto SaaS, los procesos de backup son gestionados por Iberlayer, sin que el usuario deba realizar ninguna acción.

6.13 FUNCIONES DE SEGURIDAD

43. Dado que Email Guardian se trata de un producto SaaS, la configuración de las funciones de seguridad es gestionada por Iberlayer, sin que el usuario deba realizar ninguna acción.

7 FASE DE OPERACIÓN

44. Dado que Email Guardian se trata de un producto SaaS, los recursos del servicio son mantenidos por parte de Iberlayer, realizando una supervisión del correcto funcionamiento del servicio, sin necesidad de ninguna acción por parte del usuario.
45. Respecto a la funcionalidad de la consola web, Admin Center, cabe destacar lo siguiente:
- **Configuración de listas blancas y negras:** Se permite a los usuarios administradores la gestión de listas blancas y negras. Para ello, será necesario configurar, como mínimo, el remitente del correo y la duración de la lista creada. Esta configuración es accesible desde la consola web, dentro de la ventana “*Configuration > Lists*”. Una vez dentro, podremos rellenar campos como: dirección del remitente/destinatario, fecha de expiración de la regla (obligatoria para evitar que una regla persista infinitamente) y comentarios sobre la regla.
 - **Eventos sobre el filtrado de correos:** Se permite a los usuarios administradores realizar una búsqueda sobre los eventos de filtrado de correos generados durante la funcionalidad habitual del producto.

8 REFERENCIAS

46. Documento sin referencias.

9 ABREVIATURAS

SaaS	Software as a Service
TOE	Target of Evaluation
IP	Internet Protocol
IA	Inteligencia Artificial
DLP	Data Loss Prevention
HTTPS	HyperText Transfer Protocol Secure
SSHv2	Secure Shell version 2
TLS	Transport Layer Security
MX	Mail Exchange
SPF	Sender Policy Framework
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting & Conformance
RSA	Rivest–Shamir–Adleman
SMTP	Simple Mail Transfer Protocol
CCN-STIC	Centro Criptológico Nacional - Seguridad de las Tecnologías de la Información y las Comunicaciones

