centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 1647

# Procedimiento de Empleo Seguro
# Check Point Harmony Email & Collaboration


Mayo 2025

MINISTERIO DE DEFENSA

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

Edita:

Pº de la Castellana 109, 28046 Madrid


NIPO: 083-25-210-4
Fecha de Edición: Mayo de 2025

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2026.01.16 08:10:44 +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. Check Point Harmony Email & Collaboration es una solución de seguridad avanzada que protege correo electrónico y aplicaciones de colaboración contra phishing, malware, ransomware, pérdida de datos y toma de control de cuentas. Con capacidades avanzadas de emulación y reescritura de URL, análisis dinámico de ficheros en sandbox, limpiado de documentos, análisis de anomalías, análisis de comprimidos con contraseña, códigos QR, o añadido de banners inteligentes, entre otros, utiliza inteligencia artificial y aprendizaje automático para bloquear amenazas avanzadas y accesos no autorizados, además de gestionar DMARC para prevenir suplantación de identidad. Está integrado de forma nativa con Check Point ThreatCloud AI de forma que se retroalimenta de toda la plataforma de inteligencia de Check Point.
2. Harmony Email & Collaboration de Check Point es un servicio de protección en API en línea que protege sus aplicaciones SaaS contra amenazas avanzadas, como:
    - Amenaza de día cero.
    - Suplantación de identidad (phishing).
    - Toma de control de cuenta.
    - Fuga de datos.
    - Descubrimiento de Shadow IT.

## 2 OBJETO Y ALCANCE

3. El presente documento de Procedimiento de Empleo Seguro (PES) se ha escrito para la solución Harmony Email & Collaboration de Check Point Software Technologies, y no está orientado a constituir una guía completa para la instalación y configuración del producto. Su objetivo es indicar qué tareas concretas se deben realizar durante la instalación y configuración del producto, para conseguir una configuración segura y que el producto funcione en la configuración evaluada para su cualificación en el catálogo CPSTIC.
4. Harmony Email & Collaboration ha sido cualificado e incluido en el Catálogo de Productos y Servicios TIC (CPSTIC) en la familia “protección de correo electrónico”, con nivel ALTO.

# 3 ORGANIZACIÓN DEL DOCUMENTO

5. El presente documento se organiza en 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 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. Harmony Email & Collaboration es un producto SaaS, por lo que no es necesario realizar ninguna descarga previa de software ni recepción o preparación de hardware. El producto conecta con los entornos SaaS del cliente, como Microsoft 365, para implementar por API las configuraciones y medidas de seguridad necesarias.

## 4.2 ENTORNO DE INSTALACIÓN SEGURO

7. Se tienen las mismas consideraciones indicadas en el párrafo 6.

## 4.3 REGISTRO Y LICENCIAS

8. Las licencias de Harmony Email & Collaboration se entregan en una cuenta de www.checkpoint.com del cliente. Esta cuenta, comúnmente llamada Account en UserCenter (usercenter.checkpoint.com) aloja las licencias de este y otros productos de Check Point, y es necesario conectarlo al tenant o cuenta de Infinity Portal para que se active el producto.
9. Para conectar la cuenta de Infinity Portal (https://portal.checkpoint.com) con la cuenta de Usercenter (https://usercenter.checkpoint.com), basta con acceder a Infinity Portal y navegar al menú “Services & Contracts”.
10. Una vez en esta ventana, hacer clic en “Link a User Center account”, donde será necesario especificar las credenciales de usercenter.checkpoint.com para elegir la cuenta de la que se desea coger las licencias. Una vez hecho esto, la sincronización se hará de forma automática con periodicidad.

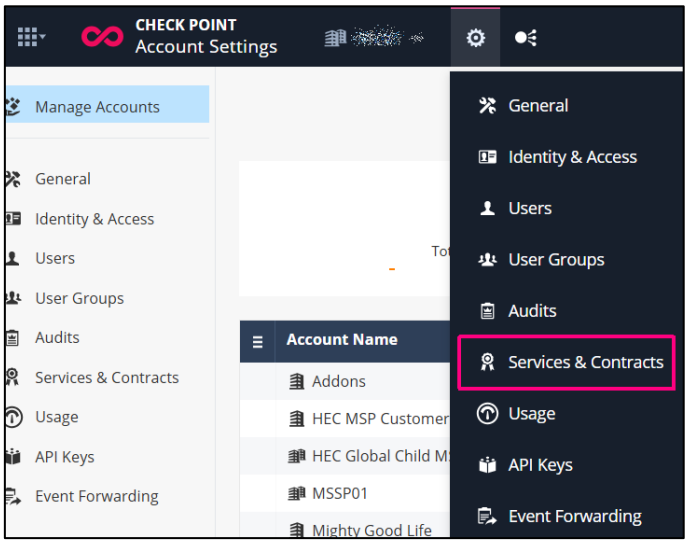



**Ilustración 1. Menú de "Services & Contacts en Infonity Portal**

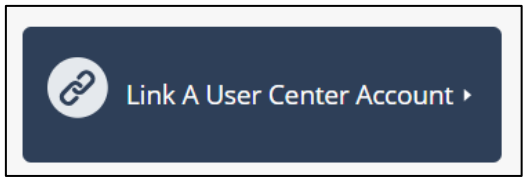



**Ilustración 2. Boton "Link a User Center Account"**

11. Este proceso se puede consultar en el manual de administración de Infinity Portal, concretamente en el siguiente enlace:

    https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Content/Topics-Infinity-Portal/Services-and-Contracts.htm?TocPath=Account%20Settings%7CServices%20%26%20Contracts%7C___0#Adding_Subscriptions_to_your_Infinity_Portal_Account

## 4.4 CONSIDERACIONES PREVIAS

12. Para la cualificación de Harmony Email & Collaboration en el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN (CPSTIC), se ha creado la cuenta o tenant de Infinity Portal en la región de Europa. De esta forma, la residencia de datos e infraestructura de nube se aloja en centros de datos en Europa.
13. Para ello, es necesario, en el proceso de creación de la cuenta de Infinity Portal, seleccionar la región correspondiente.


**Ilustración 3. Registro de una cuenta**

14. Se mostrará un formulario donde uno de los campos es “Select storage location”. Ésta es la única opción que afecta a la localización de infraestructura/datos, y no el campo país/ciudad previo. Seleccionar la región “EU” correspondiente a Europa.

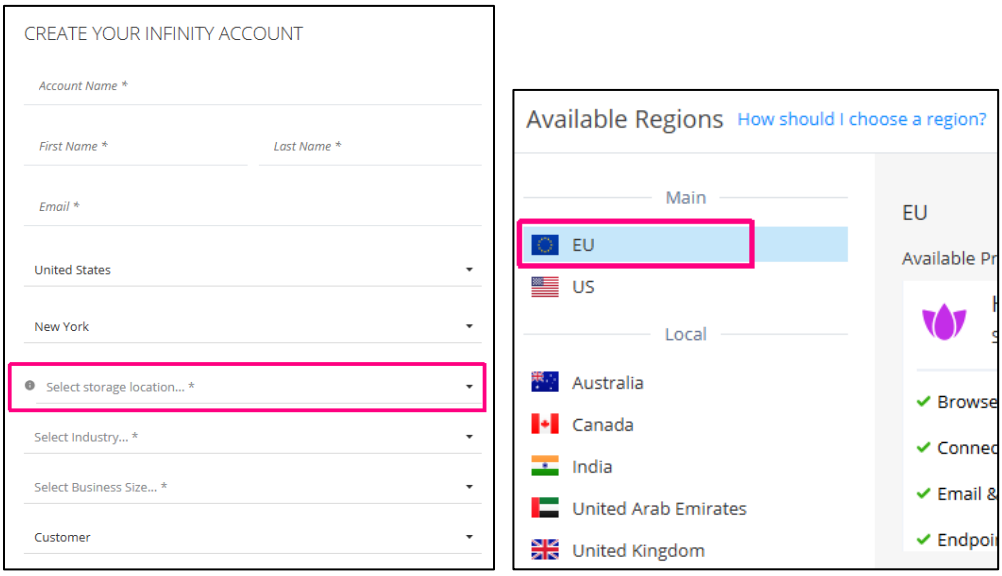



**Ilustración 4. Selección de localización**

## 4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

15. Harmony Email & Collaboration es una plataforma SaaS que no requiere de ningún componente externo a la solución para su funcionamiento, salvando por supuesto el entorno a proteger (Microsoft 365, Google Workspace, Slack, Dropbox, Citrix Sharefile). De forma adicional a la solución Harmony Email & Collaboration, Infinity Portal puede hacer uso de elementos externos como proveedores de identidades (Microsoft Entra ID, Okta, Duo, Google Workspace, otros o un servidor SAML genérico), o reenvío de de logs a un Syslog externo.

# 5 FASE DE INSTALACIÓN

16. Harmony Email & Collaboration se trata de una solución SaaS que se entrega como servicio, totalmente proporcionado por Check Point Software Technologies, sin que sea necesario el despliegue de ningún otro componente externo (salvo el entorno a proteger). No es necesario el despliegue del entorno de ninguna forma adicional al indicado en el apartado **4.4**.

# 6 FASE DE CONFIGURACIÓN

## 6.1 MODO DE OPERACIÓN SEGURO

17. No es necesario ningún despliegue particular, más allá del indicado en el apartado 4.4 para su uso seguro. Sí es necesario llevar a cabo una serie de configuraciones sencillas para adecuar el nivel de protección. Estas configuraciones no implican ningún "fine-tuning", sino una activación de las capacidades mínimas de prevención. A continuación, se detallan aquellas configuraciones necesarias según se indica en el Security Target de la cualificación.

### 6.1.1 EMAIL THREAT PREVENTION (INCLUYENDO MALWARE Y PHISHING)

18. Se debe modificar la política por defecto, de forma que no sea "Detect" sino "Prevent (inline)". Para ello, modificar la política predefinida o bien crear una nueva y aplicarla a los usuarios y/o grupos correspondientes. En la siguiente imagen se muestra un ejemplo para Microsoft 365.


**Ilustración 5. Modificación de la política de "Email Threat Prevention" a "Prevent (inline)"**

19. Las siguientes opciones no son necesarias para una configuración segura acorde a esta cualificación, pero pueden ser particularmente interesantes para según qué entorno (especialmente los correos internos).

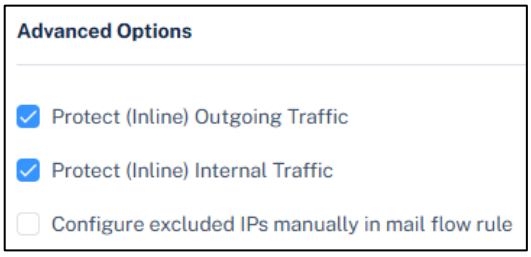



**Ilustración 6. Configuraciones adicionales (opcional)**

### 6.1.2 CLICK-TIME PROTECTION

20. Esta protección reescribe cada URL en los correos entrantes, de forma que si alguien pulsa en el enlace, éste se escaneará en este momento además del escáner que se hizo en el momento de recibir el correo. Esta protección es especialmente interesante para protegerse ante URLs cuyo contenido cambia a propósito para evadir soluciones de seguridad, o ante URLs maliciosas (por ejemplo, de phishing) de día cero. Para ello, si no la hubiera ya creada, es necesario crear y editar una política de "Click-Time Protection", de la siguiente forma:

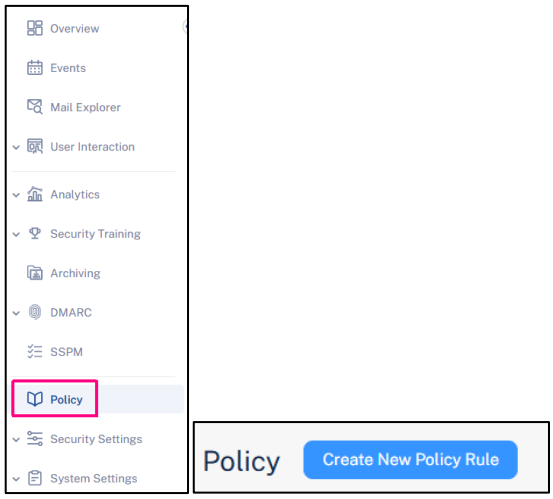



**Ilustración 7. Creación de política "Click-Time Protection**

21. En la siguiente imagen, se indica un ejemplo para Microsoft 365.

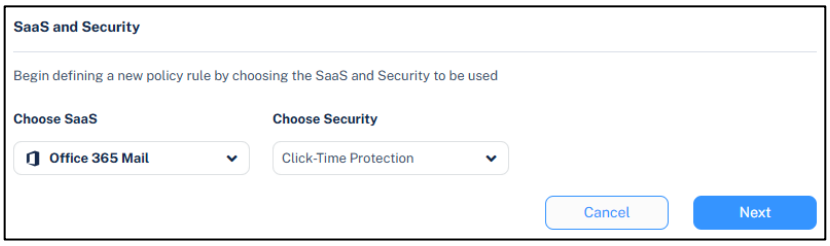



**Ilustración 8. Ejemplo de "Click-Time Protection" para Microsoft 365.**

### 6.1.3 DATA LOSS PREVENTION

22. Mediante la funcionalidad de Data Loss Prevention (DLP), Harmony Email & Collaboration puede detectar y prevenir la fuga de información que coincida con alguno de los tipos de datos y sensibilidad configurados. DLP, típicamente, es una capacidad que aplica a los correos salientes, por lo que es menester tener en cuenta que para evitar problemas en los servidores de correo de destino, es necesario configurar los registros SPF acorde con "**include:spfa.cpmails.com".**


**Ilustración 9 Configuracion para evitar el fallo en las comprobaciones SPF de correos salientes**

23. De igual forma a como se ha hecho con la política de Threat Prevention de correo electrónico, es necesario crear (si no existe previamente) una política y configurarla en modo "Prevent (inline)".

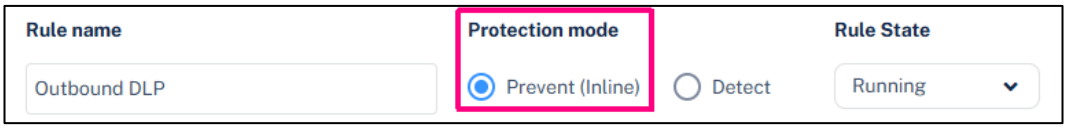



**Ilustración 10. Política "Outbound DLP"**

## 6.2 AUTENTICACIÓN

24. Harmony Email & Collaboration utiliza la infraestructura de Infinity Portal para las labores de autenticación de usuarios. Existen varias opciones disponibles.

    - Usuarios locales en el tenant.
    - Usuarios de un Proveedor de Identidades externo.

25. Asimismo, los Proveedores de Identidades pueden ser alguno de:

    - Microsoft ADFS
    - Microsoft Entra ID
    - Okta
    - OneLogin
    - Ping o Ping Federate
    - Google Workspace
    - DUO
    - RADIUS
    - Generic SAML Server

26. En caso de utilizar usuarios locales, en lugar de delegar la autenticación a un proveedor de identidades externo, éstas se configurarán en la propia cuenta. Además, es posible habilitar doble factor de autenticación, siendo una opción muy recomendable, aunque no requerida para esta cualificación.

### 6.2.1 UTILIZANDO USUARIOS LOCALES

27. En caso de no utilizar un Proveedor de identidades, se crearan usuarios locales ejecutando los siguientes pasos:

    a) En el Infinity Portal: Navega a > Usuarios y haz clic en "Nuevo" en la barra de herramientas.

    b) En el campo "Nombre", ingresa un nombre para el usuario.

    c) En el campo "Correo electrónico", ingresa la dirección de correo electrónico del nuevo usuario.

    d) En el campo "Teléfono", ingresa el número de teléfono del usuario.

    - Selecciona una región de la lista.
    - Ingresa el número de teléfono.

    e) En el campo "Grupos de usuario", selecciona los Grupos de usuario para el nuevo usuario de la lista. Puedes seleccionar múltiples Grupos de usuario para cada usuario.

    f) En el campo "Roles globales", selecciona los roles para el nuevo usuario de la lista. Puedes seleccionar múltiples roles para cada usuario..

g) Selecciona los roles de servicio específicos para asignar al usuario.

h) Haz clic en "Agregar" para guardar o en "Cancelar" para salir sin guardar al nuevo usuario.

i) El usuario aparecerá con el estado "Pendiente" en la lista completa de usuarios.

28. Cuando el usuario reciba la invitación por correo electrónico y haga clic en el enlace para aceptar la invitación, el Portal Infinity verificará si se trata de un usuario nuevo o existente.

    a) Para usuarios nuevos, el Portal Infinity abrirá la pantalla de activación y solicitará que configuren una nueva contraseña. La política de contraseñas se mostrará en la misma página.

    b) El usuario ingresa la contraseña, la confirma, selecciona "Acepto los términos de servicio del Portal Infinity" y la política de privacidad, y hace clic en "Activar".

    c) El Portal Infinity activa al usuario.

    d) Para usuarios existentes, el Portal Infinity aprueba al usuario y muestra un mensaje de aprobación.

    e) El Portal Infinity agrega al usuario a la cuenta y cambia su estado de "Pendiente" a "Activo".

    f) El usuario hace clic en "Volver para iniciar sesión" e ingresa al Portal Infinity. Los nuevos usuarios deben ingresar su correo electrónico y contraseña.

29. Cuando el usuario inicie sesión en el Portal Infinity, la cuenta aparecerá en el menú desplegable de la barra de herramientas superior.

## 6.3 ADMINISTRACIÓN DEL PRODUCTO

### 6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

30. La administración de Harmony Email & Collaboration se hace en todo caso a través de HTTPS, accediendo al portal https://portal.checkpoint.com. Ésta es una comunicación cifrada utilizando TLS 1.2 ó TLS 1.3.

31. En ningún caso, la solución es accesible a través de CLI, si bien pueden hacerse determinadas labores de gestión mediante API a través de HTTPS.

32. No es posible acceder a la gestión de otra forma que no sean las arriba mencionadas.

### 6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

33. En el portal de gestión de Harmony Email & Collaboration es posible configurar diferentes roles de administración o acceso, con diferentes niveles de autorización (RBAC). A continuación se detallan los diferentes niveles de acceso disponibles específicos para Harmony Email & Collaboration:

34. La documentación actualizada se encuentra en https://sc1.checkpoint.com/documents/Harmony_Email_and_Collaboration/Topics-Harmony-Email-Collaboration-Admin-Guide/Getting-Started/Managing-Users.htm?tocpath=Getting%20Started%7CManaging%20Users%252C%20Roles%20and%20their%20Permissions%7C_____1#Roles_and_Permissions

a) Read-Only: este rol de usuario tiene permisos de lectura para ver la información que se muestra en la interfaz de TOE, pero no se encarga de la configuración de dominios protegidos, políticas, configuraciones o administración diaria de incidentes e informes.

b) Help Desk: este rol de usuario se encarga de la administración de tickets de los usuarios. Su trabajo es investigar eventos e informes de los usuarios y responder según la política de la empresa. Un caso de uso típico es la administración de solicitudes de los usuarios para liberar correos electrónicos de la cuarentena.

c) Admin: los administradores del sistema pueden ver toda la información del sistema y realizar cualquier acción en el sistema. Esto incluye los permisos del usuario de la mesa de ayuda y la aprobación para configurar la política de seguridad y conectar/desconectar dominios protegidos y cuentas de la aplicación conectada (por ejemplo, Microsoft 365).

d) Disable receiving weekly reports: como el administrador pero sin informes semanales.

e) View sensitive data only if threats are found: como el administrador con el permiso específico “ver datos confidenciales solo si se encuentran amenazas”.

f) Receive alerts by default: como el administrador con el permiso específico “recibir alertas de forma predeterminada”.

g) View all sensitive data: como el administrador con permiso específico para “ver todos los datos confidenciales”.

h) View policy: acceso de solo lectura a las páginas de gestión de la política de seguridad.

i) View and edit policy: acceso de lectura, creación y edición de políticas, en las páginas de gestión de la política de seguridad.

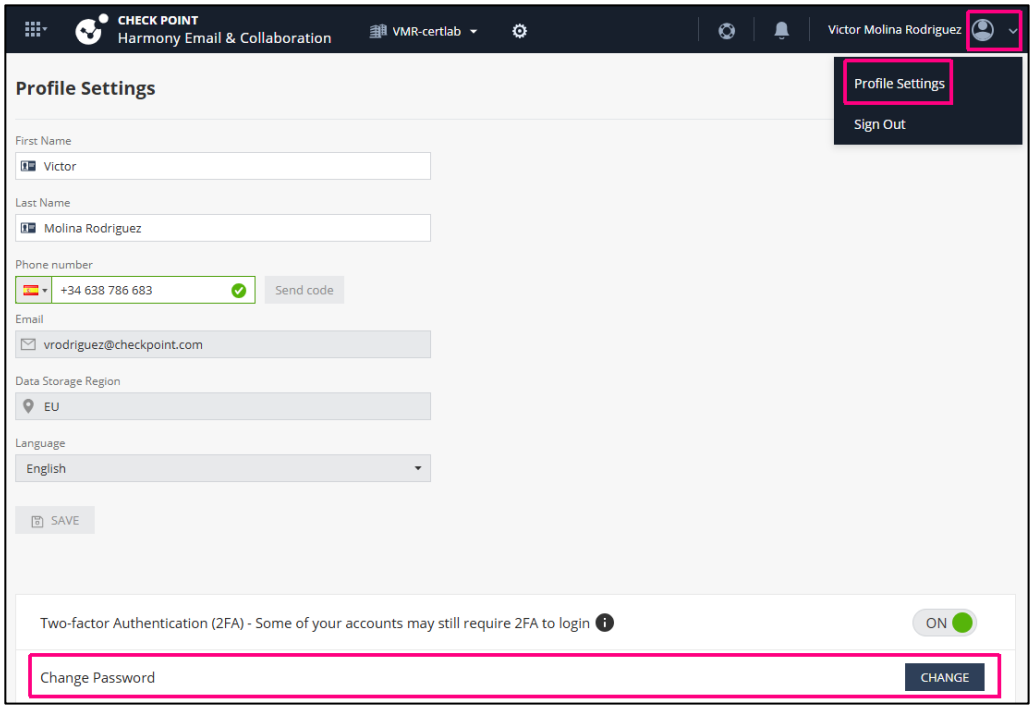
35. Para una configuración segura acorde a los parámetros de las guías STIC del CCN, es necesario cambiar el tiempo máximo de inactividad de la sesión a 5 minutos, en el siguiente menú:

```
Configuración > Identity & Access > Sessions
```


**Ilustración 11. Cambio de tiempo máximo de inactividad**

36. El sistema establece una política predefinida de seguridad de contraseñas, siendo segura por defecto, cambiando los parámetros indicados en los párrafos 33 y 34.

37. Cada usuario puede cambiar su propia contraseña a través de la plataforma, en caso de utilizarse “usuarios locales” y no de un proveedor externo (como Entra ID o Google Workspace). Para ello, puede dirigirse a “Profile Settings > Change password”.




38. Es muy recomendable configurar un doble factor de autenticación. Por defecto, el sistema pedirá que se configure de forma obligatoria al usuario en el primer establecimiento de contraseña. Para ello, pueden utilizarse diferentes aplicaciones como Microsoft Authenticator o Google Authenticator. En caso de ser necesario cambiar esta configuración, se puede hacer a nivel de usuario en el mismo apartado que el descrito en el párrafo 31.

## 6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

39. Harmony Email & Collaboration es una solución SaaS (Software as a Service) cuya infraestructura se gestiona y mantiene íntegramente por Check Point Software Technologies. El acceso a la gestión de la solución se realiza mediante el acceso por HTTPS puerto 443, a https://portal.checkpoint.com, eligiendo el servicio correspondiente.

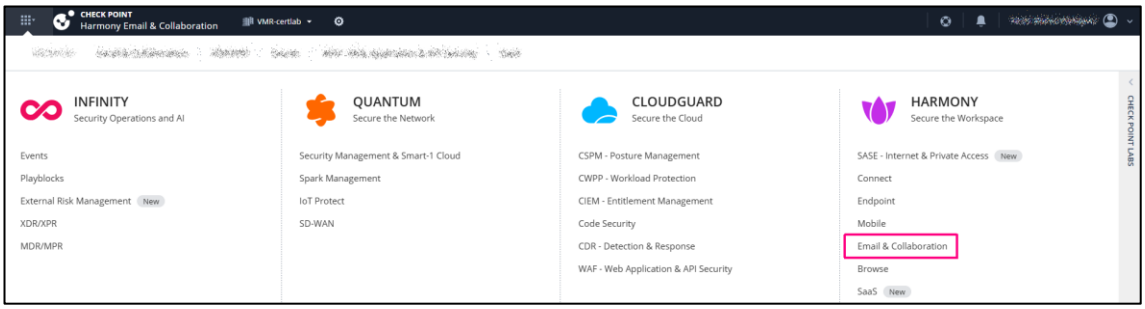
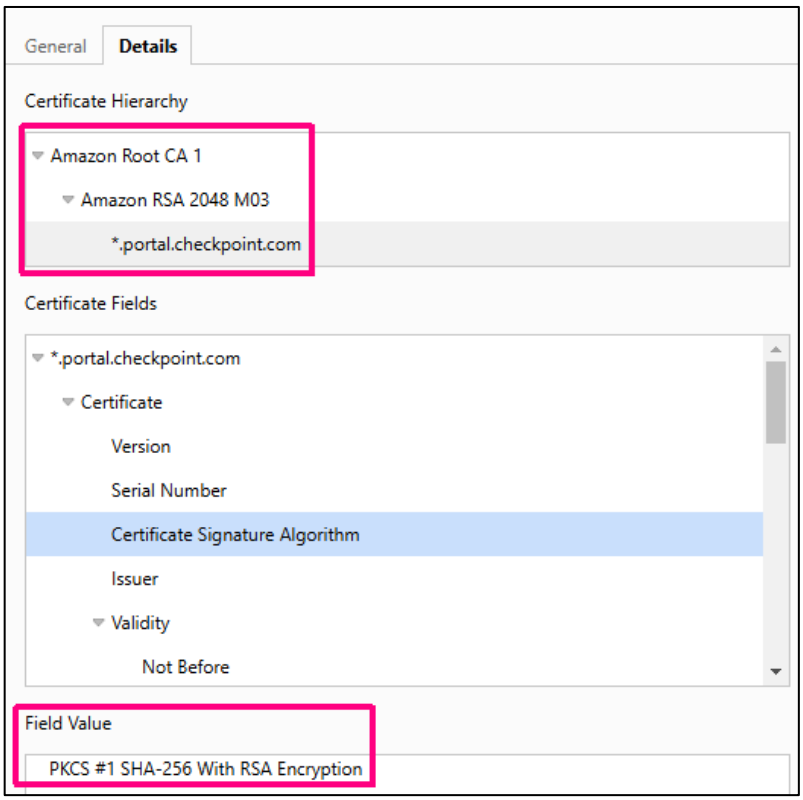



**Ilustración 12. Acceso a la función "Email & Colaboration" dentro del portal**

## 6.5 GESTIÓN DE CERTIFICADOS

40. Harmony Email & Collaboration se presenta en formato SaaS, cuya infraestructura se gestiona íntegramente por Check Point Software Technologies, incluyendo los certificados del portal de gestión https://portal.checkpoint.com.




## 6.6 SERVIDORES DE AUTENTICACIÓN

41. Los usuarios utilizados para gestionar, sea cual sea el rol específico utilizado de los indicados en el párrafo 33, pueden ser internos o externos. Para los usuarios internos, la infraestructura utilizada para la autenticación se gestiona íntegramente por Check Point sin que el administrador necesite hacer nada al respecto más allá de las operaciones de cambio de contraseña o configuración de doble factor de autenticación. En caso de utilizar autenticación externa, los servidores de autenticación serían los propios del servicio integrado, pudiendo ser cualquiera de los indicados en el párrafo 25:

- Microsoft ADFS
- Microsoft Entra ID
- Okta
- OneLogin
- Ping o Ping Federate
- Google Workspace
- DUO
- RADIUS
- Generic SAML Server

## 6.7 SINCRONIZACIÓN

42. Harmony Email & Collaboration es una solución SaaS (Software as a Service) cuya infraestructura se gestiona y mantiene íntegramente por Check Point Software Technologies. La sincronización horaria así como otros elementos necesarios para el correcto funcionamiento y auditoría de los sistemas no es necesario, y no es posible, configurarla por el administrador.

## 6.8 ACTUALIZACIONES

43. Harmony Email & Collaboration es una solución SaaS (Software as a Service) cuya infraestructura se gestiona y mantiene íntegramente por Check Point Software Technologies. Las actualizaciones de los sistemas que componen la arquitectura de la solución se gestionan íntegramente por Check Point, sin que el administrador tenga que llevar a cabo ninguna acción.

## 6.9 AUTO-CHEQUEOS

44. Harmony Email & Collaboration es una solución SaaS (Software as a Service) cuya infraestructura se gestiona y mantiene íntegramente por Check Point Software Technologies. Las comprobaciones de estado y mantenimiento de los diferentes componentes de la infraestructura se realiza por Check Point sin que el administrador tenga que realizar ninguna acción.

## 6.10 ALTA DISPONIBILIDAD

45. Harmony Email & Collaboration es una solución SaaS (Software as a Service) cuya infraestructura se gestiona y mantiene íntegramente por Check Point Software Technologies. La arquitectura está basada en componentes de nube escalables, de forma que tanto el aumento de demanda como la alta disponibilidad, ya sea por imprevistos o por operaciones de mantenimiento, se aseguran íntegramente por Check Point sin que el administrador tenga que realizar ninguna acción.
46. El estado del sistema, así como histórico, puede consultarse en https://status.checkpoint.com

## 6.11 AUDITORÍA

### 6.11.1 REGISTRO DE EVENTOS

47. En la siguiente página pueden consultarse la información y formato de registros de auditoría que recoge la solución.

    https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Content/Topics-Infinity-Portal/Audits.htm?tocpath=Account%20Settings%7C_____5#Audits

    - Severity: niveles de severidad de la acción realizada: Aviso, Información, Advertencia, Crítico
    - User: quién realiza la acción.
    - Time: la hora de creación de la auditoría, en formato DD/MM/AA, HH/MM/SS

- Service: el módulo del portal portal.checkpoint.com donde se ha realizado la acción registrada.
- Categoría: qué tipo de entidad ha realizado la acción.
- Tipo: qué acción se ha realizado.

### 6.11.2 ALMACENAMIENTO LOCAL

48. Harmony Email & Collaboration es una solución SaaS (Software as a Service) cuya infraestructura se gestiona y mantiene íntegramente por Check Point Software Technologies. El almacenamiento se gestiona por Check Point sin que el administrador tenga que llevar a cabo ninguna acción, salvo la elección de la región de residencia de datos, en el momento de la creación de la cuenta, como se indica en el párrafo 14.

### 6.11.3 ALMACENAMIENTO REMOTO

49. No se realiza ningún almacenamiento remoto en Harmony Email & Collaboration, si bien es posible enviar los logs a un servidor de logs externo, como un SIEM. Este reenvío de logs se realiza y configura desde la propia infraestructura de Infinity Portal.

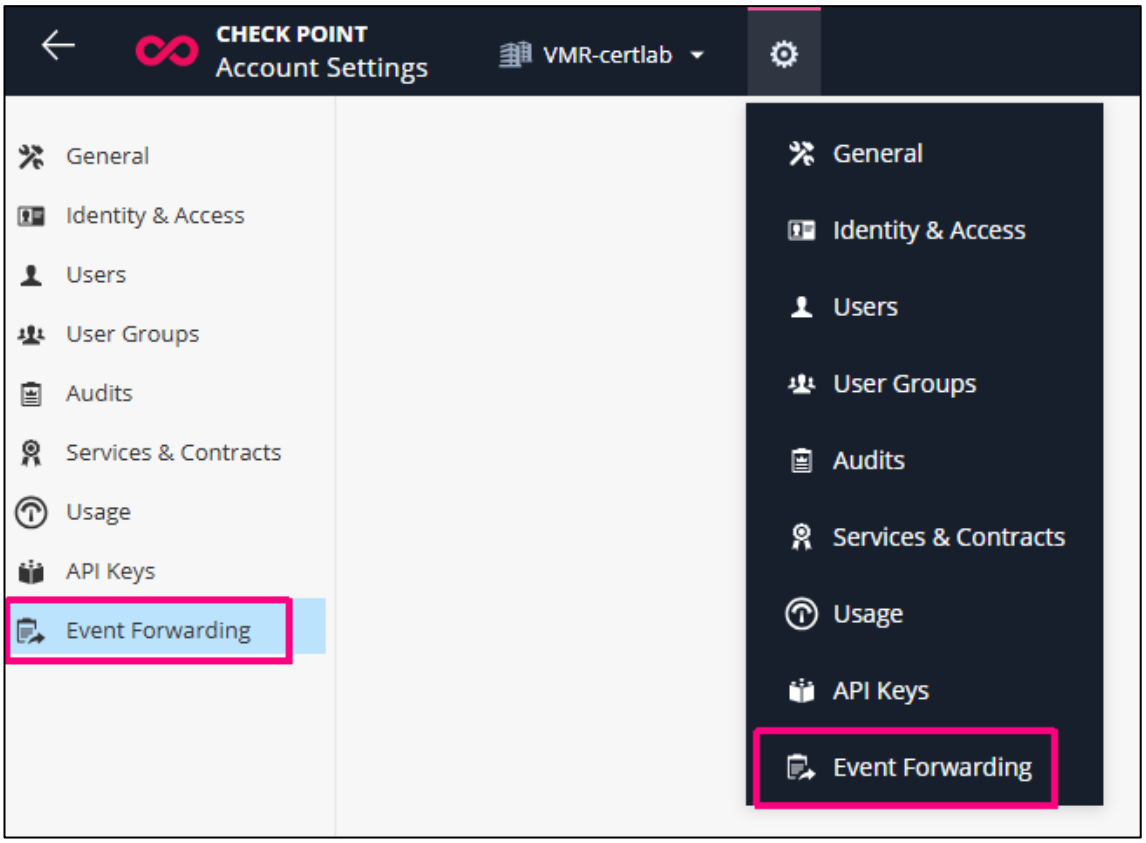



**Ilustración 13. Envío de logs a un servidor externo**

50. Para realizar una configuración del almacenamiento remoto de auditoría seguir las instrucciones del siguiente enlace:

https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Content/Topics-Infinity-Portal/Event-Forwarding.htm

## 6.12 BACKUP

51. Harmony Email & Collaboration es una solución SaaS (Software as a Service) cuya infraestructura se gestiona y mantiene íntegramente por Check Point Software Technologies. Los backups necesarios para asegurar la continuidad y potencial restauración del servicio se gestionan por Check Point, sin que el administrador tenga que realizar ninguna acción.

52. Los parámetros de retención de logs, alertas y correos electrónicos pueden personalizarse en la sección “Security Settings > Customization”, según se aprecia en la siguiente imagen:

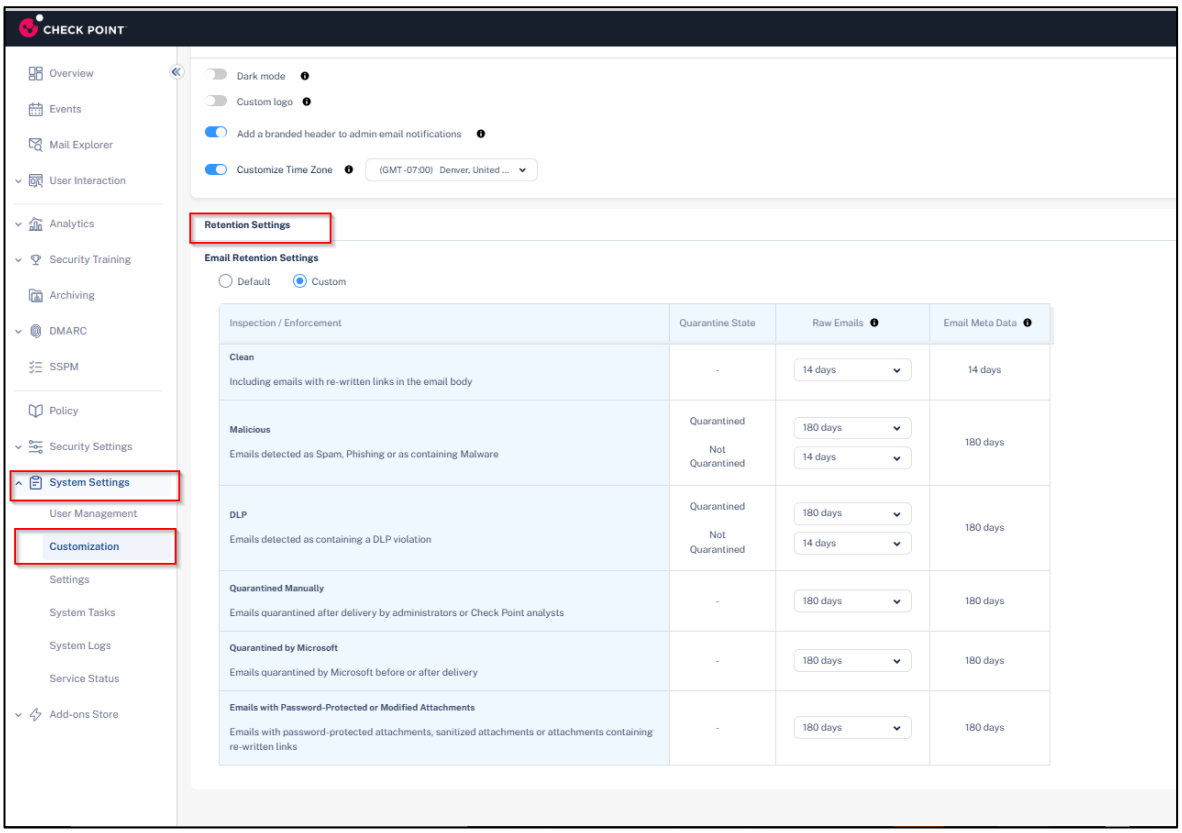
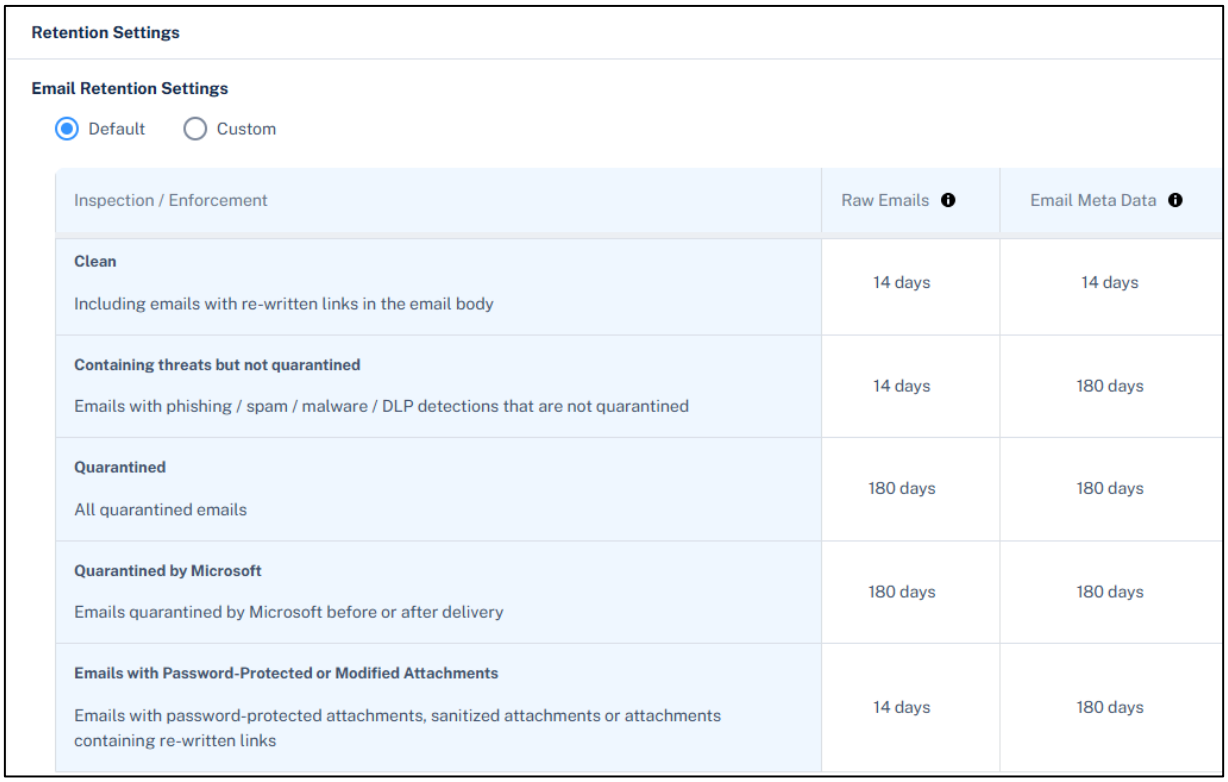



**Ilustración 14. parámetros de retención**

53. En caso de seleccionar los parámetros predefinidos (opción “custom”) estos serían los siguientes:



**Retention Settings**

**Email Retention Settings**

Default  Custom

| Inspection / Enforcement | Raw Emails | Email Meta Data |
|---|---|---|
| **Clean**<br>Including emails with re-written links in the email body | 14 days | 14 days |
| **Containing threats but not quarantined**<br>Emails with phishing / spam / malware / DLP detections that are not quarantined | 14 days | 180 days |
| **Quarantined**<br>All quarantined emails | 180 days | 180 days |
| **Quarantined by Microsoft**<br>Emails quarantined by Microsoft before or after delivery | 180 days | 180 days |
| **Emails with Password-Protected or Modified Attachments**<br>Emails with password-protected attachments, sanitized attachments or attachments containing re-written links | 14 days | 180 days |

**Ilustración 15. parámetros predefinidos**

# 7 REFERENCIAS

[GAEC] Guía de Administración de Harmony Email & Collaboration

https://sc1.checkpoint.com/documents/Harmony_Email_and_Collaboration/Topics-Harmony-Email-Collaboration-Admin-Guide/Introduction.htm

[GAIP] Guía de Administración de Infinity Portal

https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Content/Topics-Infinity-Portal/Introduction-to-Infinity-Portal.htm

[STATUS] Página de estado de servicios nube de Check Point Software Technologies

https://status.checkpoint.com

# 8 ABREVIATURAS

| | |
|---|---|
| API | Application Programming Interface |
| CCN | Centro Criptológico Nacional |
| CLI | Command-Line Interface |
| CPSTIC | Catálogo de Productos y Servicios TIC |
| DLP | Data Loss Prevention |
| DMARC | Domain-based Message Authentication, Reporting & Conformance |
| HTTPS | HyperText Transfer Protocol Secure |
| MFA | Multi-Factor Authentication |
| PES | Procedimiento de Empleo Seguro |
| RBAC | Role-Based Access Control |
| SaaS | Software as a Service |
| SIEM | Security Information and Event Management |
| SPF | Sender Policy Framework |
| STIC | Seguridad de las Tecnologías de la Información y la Comunicación |
| TLS | Transport Layer Security |

PUBLICACIONES DE DEFENSA

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