centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1509

Procedimiento de empleo seguro
Guardedbox



Junio 2023

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

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
2023.07.20 11:51:03 +02'00'

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2023

NIPO: 083-23-155-1.
Fecha de Edición: junio 2023.

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 4
1.1 FUNCIONALIDADES Y CAPACIDADES 5
1.2 COMPONENTES PRINCIPALES DE GUARDEDBOX 6
1.3 PERFILES DE INSTALACIÓN, ADMINISTRACIÓN Y UTILIZACIÓN 6
2. OBJETO Y ALCANCE 7
3. ORGANIZACIÓN DEL DOCUMENTO 8
4. FASE DE DESPLIEGUE E INSTALACIÓN 9
4.1 ENTREGA SEGURA DEL PRODUCTO 9
4.2 ENTORNO DE INSTALACIÓN SEGURO 9
4.3 REGISTRO Y LICENCIAS 9
4.4 CONSIDERACIONES PREVIAS 9
4.4.1 REQUISITOS HARDWARE 10
4.4.2 SISTEMA OPERATIVO 10
4.4.3 ENTORNO DE EJECUCIÓN DOCKER 11
4.4.4 SERVICIO DE CORREO ELECTRÓNICO 12
4.4.5 SERVICIO DE DNS 12
4.4.6 COMPONENTES DE GUARDEDBOX 12
4.5 COMPROBACIÓN DE LA AUTENTICIDAD E INTEGRIDAD DEL SOFTWARE 13
4.6 INSTALACIÓN 14
5. FASE DE CONFIGURACIÓN 16
5.1 AUTENTICACIÓN 16
5.2 ADMINISTRACIÓN DEL PRODUCTO 18
5.2.1 ADMINISTRACIÓN LOCAL Y REMOTA 18
5.2.2 CONFIGURACIÓN DE ADMINISTRADORES 18
5.2.3 POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN 19
5.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 22
5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS 22
5.5 GESTIÓN DE CERTIFICADOS 23
5.6 SERVIDORES DE AUTENTICACIÓN 25
5.7 SINCRONIZACIÓN HORARIA 25
5.8 ACTUALIZACIONES 26
5.9 AUTO-CHEQUEOS 26
5.10 SNMP 27

5.11 ALTA DISPONIBILIDAD 27
5.12 AUDITORÍA 27
5.12.1 REGISTRO DE EVENTOS 28
5.12.2 ALMACENAMIENTO LOCAL 29
5.12.3 ALMACENAMIENTO REMOTO 30
5.13 BACKUP 31
5.14 SERVICIOS DE SEGURIDAD 31
5.15 CONEXIÓN A LA BASE DE DATOS 32
5.16 CONEXIÓN AL SERVIDOR DE CORREO ELECTRÓNICO 34
5.17 CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX 35
5.18 CONFIGURACIÓN DEL USUARIO ADMINISTRADOR DE GUARDEDBOX 38
6. FASE DE OPERACIÓN 40
7. UTILIZACIÓN SEGURA DE GUARDEDBOX 41
7.1 VERIFICACIÓN DEL SOFTWARE DE GUARDEDBOX EN EL LADO CLIENTE 41
8. CHECKLIST 43
9. REFERENCIAS 46
10. ANEXO: LISTADO DE FICHEROS DE CONFIGURACIÓN 47
11. ABREVIATURAS 48

1. INTRODUCCIÓN

1. **GuardedBox®** es una solución de gestión de secretos con cifrado extremo a extremo (E2EE) cuyo propósito es proporcionar un entorno de compartición y almacenamiento seguro de secretos, y que permite a una organización controlar y auditar el intercambio de secretos, tanto interno como externo.
2. El término "secreto" se refiere a cualquier información considerada de carácter sensible o privado cuya confidencialidad debe ser preservada y cuyo acceso por parte de terceros debe controlarse y limitarse según las políticas definidas por su propietario (individuo u organización). Algunos ejemplos de secreto son:
   a) Contraseñas.
   b) Certificados digitales.
   c) Ficheros con información privada (informes, facturas, listados de empleados, clientes o proveedores, contratos, nóminas, expedientes, DNI escaneado, escrituras notariales, autorizaciones firmadas, formularios cumplimentado, etc.).
   d) Informes de auditoría.
   e) Resultados de informes o pruebas médicas.
   f) El enlace web (o URL) de un repositorio de información.
   g) El código de acceso a un edificio.
   h) El localizador de un viaje o una estancia en un alojamiento.
   i) Las instrucciones para completar un procedimiento de emergencia…
   j) … o cualquier información que no deba conocerse de forma no controlada.

1.1 FUNCIONALIDADES Y CAPACIDADES

3. Las capacidades de GuardedBox para la gestión de secretos permiten:

   a) **Almacenar secretos** individuales o de grupo: todos los secretos de los usuarios se guardan en la base de datos ***cifrados (extremo a extremo)***, de forma que ningún otro usuario no autorizado, ni tampoco el servidor, pueden acceder a sus contenidos.

   b) **Compartir secretos** con otros usuarios: el propietario de un secreto o de un grupo (o los miembros de un grupo) puede elegir compartir determinados secretos con otros usuarios. Los contenidos siempre seguirán ***cifrados (extremo a extremo)*** y solo accesibles para quienes hayan obtenido el permiso necesario.

   c) Mantener el **control** y la **gestión** sobre los **secretos** que se almacenan, se comparten o se reciben. GuardedBox ofrece funcionalidades orientadas a que el usuario tenga control sobre la información que comparte y se le comparte dentro de la solución, gracias a:

      - Un sistema que muestra el estado de compartición actual y pasado de los secretos individuales y de grupo con otros usuarios.
      - Un sistema avanzado de notificaciones, mediante avisos por e-mail e indicadores visuales, que informa a los usuarios de las actividades que tienen lugar en torno a sus secretos.
        - Dentro de las actividades más habituales se incluyen la creación, modificación y eliminación de secretos, la compartición de secretos con usuarios internos o externos a GuardedBox, la creación de grupos, cambios en la membresía de un grupo o en sus propiedades, eventos relacionados con la gestión de cuentas de usuario (registro, invitaciones, borrado, cambios de contraseña, etc.), eventos de seguridad (detección de actividades sospechosas), etc.
      - Un sistema de metadatos, que informa de quién y cuándo se ha efectuado la última modificación sobre un secreto y/o sus propiedades.
      - Funcionalidades de filtrado para localizar rápidamente los secretos y grupos.
      - Mecanismos de comprobación de la identidad y las claves públicas del resto de usuarios.
      - Campos de anotaciones para proporcionar información relevante para la gestión de diferentes elementos, como ficheros, grupos, etc.

   d) **Gestionar** las preferencias de **la cuenta de usuario**, incluyendo el tipo de licencia, información de la sesión actual y del último inicio de sesión, la comprobación y renovación de las claves criptográficas, el segundo factor de autentificación (2FA) y los dispositivos de confianza, modificación de la contraseña, la recepción de notificaciones de actividad vía e-mail, las licencias (propias y asignadas), eliminar completamente la cuenta de usuario, etc.

   e) **Administrar las cuentas de los usuarios**, por parte del usuario administrador en entornos empresariales, incluyendo la gestión y monitorización del estado de las

cuentas de usuario, su desactivación y reactivación inmediatas, establecimiento de una fecha de caducidad de la cuenta, cambio del tipo de cuenta mediante la (re)asignación de licencias, o la eliminación de la cuenta de usuario.

f) Un sistema de **auditoría** con registros de actividad que permite al usuario administrador en entornos empresariales disponer de información detallada sobre el ciclo de vida de los secretos, grupos, compartición, gestión de cuentas de usuario y, en general, de todas las actividades asociadas al entorno de GuardedBox.

1.2 COMPONENTES PRINCIPALES DE GUARDEDBOX

4. GuardedBox es una aplicación web que se compone de tres elementos principales:

   a) **Back-end** (servidor): corresponde al software servidor de la aplicación desarrollado en Java, responsable de la lógica de negocio, de servir el front-end (o componente cliente) y de la interacción con la capa de persistencia (base de datos).

   b) **Front-end** (cliente): corresponde al software cliente de la aplicación desarrollado en código HTML, CSS y JavaScript, encargado de la mayoría de tareas criptográficas, con el que interactúan directamente los usuarios (tanto los usuarios administradores como los usuarios finales de GuardedBox) y que ejecuta en su navegador web.

   c) **Base de datos** (persistencia): la capa de persistencia utiliza una base de datos SQL para el almacenamiento de todos los datos de los usuarios.

1.3 PERFILES DE INSTALACIÓN, ADMINISTRACIÓN Y UTILIZACIÓN

5. En el entorno en el que ejecutará GuardedBox se identifican los siguientes perfiles o tipos de usuarios, referenciados a lo largo del presente procedimiento de empleo seguro:

   a) **Administrador del servidor, sistema, entorno, plataforma o despliegue**, asociado al entorno de ejecución Docker sobre el que ejecutará GuardedBox, encargado del **despliegue** de GuardedBox y de todas las tareas de instalación, configuración, administración y operación o mantenimiento del sistema operativo, del entorno de ejecución, y del propio servidor, sistema o plataforma.

   b) **Usuario administrador de GuardedBox**: usuario de GuardedBox encargado de la gestión (del resto) de usuarios de GuardedBox y del sistema de auditoría de GuardedBox.

   c) **Usuario final de** GuardedBox: hace uso de GuardedBox para proteger y compartir sus secretos.

2. OBJETO Y ALCANCE

6. El presente documento describe el procedimiento de empleo seguro de GuardedBox, y constituye la referencia oficial de la documentación de seguridad que recoge las consideraciones necesarias para instalar, configurar, administrar, operar o mantener, y utilizar GuardedBox de forma segura, según una configuración evaluada y certificada.
7. La información aquí recogida permite a los administradores y usuarios garantizar el principio de máxima seguridad y mínima exposición, abarcando consideraciones de seguridad tanto a nivel general como específico, e incluye referencias a otra documentación complementaria en aquellos apartados en los que se requiere aportar detalles adicionales.
8. Las recomendaciones realizadas a lo largo de este procedimiento de empleo seguro son de aplicación para el uso seguro de otras versiones de la solución; sin embargo, la versión evaluada y certificada es la **versión 8.4.0 de GuardedBox**.

3. ORGANIZACIÓN DEL DOCUMENTO

9. El presente documento se estructura en los siguientes apartados:

   a) **Apartado 4**. En este apartado se recogen aspectos y recomendaciones a considerar **antes de proceder a la instalación** de la solución, y también a tener en cuenta durante la **fase de despliegue e instalación** de la solución.

   b) **Apartado 5**. En este apartado se recogen las recomendaciones para la **fase de configuración** de la solución, para lograr una configuración segura.

   c) **Apartado 6**. En este apartado se recogen las tareas recomendadas para la **fase de operación o mantenimiento** de la solución.

   d) **Apartado 7**. En este apartado se incluyen las **recomendaciones de seguridad para la utilización de GuardedBox** por parte de los usuarios finales y de los usuarios administradores de GuardedBox.

   e) **Apartado 8**. En este apartado se incluye la ***checklist*** (o **lista de comprobación**) con las principales tareas a realizar, y el estado de cada una de ellas, por parte del administrador del entorno encargado del despliegue de GuardedBox.

   f) **Apartado 9.** Este apartado contiene la documentación complementaria a la que se ha hecho **referencia** a lo largo del presente documento.

   g) **Apartado 10.** Este anexo contiene el listado con los ficheros de configuración y propiedades de la solución.

   h) **Apartado 11.** Este apartado contiene las **abreviaturas** utilizadas a lo largo del presente documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. Para preparar el entorno asociado a un nuevo despliegue de GuardedBox, la organización deberá proporcionar un servidor con el entorno de ejecución Docker, con las características, requisitos y especificaciones detalladas en el apartado "4.4 CONSIDERACIONES PREVIAS", tanto a nivel físico, como de hardware, sistema operativo y entorno de ejecución Docker.
11. GuardedBox no tiene asociado ningún repositorio para la descarga o distribución del software, ni automático ni manual, por parte de DinoSec. Para obtener la versión actual de GuardedBox se requiere contactar con DinoSec, que llevará a cabo, en colaboración con la organización, el proceso de despliegue y proporcionará la versión actual de las imágenes de los dos contenedores Docker que conforman GuardedBox, junto a sus hashes SHA256, y a los ficheros de configuración y de propiedades, personalizados para un despliegue concreto (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX").
12. Para garantizar que los componentes que se van a desplegar no han sido manipulados y corresponden a la versión oficial de GuardedBox, es necesario verificar la autenticidad e integridad del software comparando los hashes SHA256 de las imágenes de los dos contenedores Docker con los hashes declarados oficialmente por DinoSec, tal como se detalla en el apartado "4.5. COMPROBACIÓN DE LA AUTENTICIDAD E INTEGRIDAD DEL SOFTWARE".

4.2 ENTORNO DE INSTALACIÓN SEGURO

13. El entorno (o plataforma) sobre el que ejecute GuardedBox estará protegido físicamente por su entorno operacional, y no estará sujeto a ataques físicos que puedan comprometer su seguridad o interferir en su correcta operación, lo que incluye una localización segura. El acceso debe estar restringido al personal autorizado para su administración, operación o mantenimiento, y gestión.

4.3 REGISTRO Y LICENCIAS

14. La licencia del despliegue de GuardedBox determinará el número de usuarios Premium disponibles en la solución, así como las particularidades y limitaciones (en número, tamaño, etc.) para el almacenamiento de secretos en GuardedBox, en función del acuerdo establecido entre la organización y DinoSec.

4.4 CONSIDERACIONES PREVIAS

15. Los siguientes apartados describen los elementos que se requieren para el despliegue de GuardedBox, incluyendo todos aquellos aspectos que deben ser tenidos en cuenta de forma previa a iniciar la instalación y configuración de la solución de forma segura.

16. Aunque GuardedBox es una aplicación web Java que puede ejecutar dentro de un servidor de aplicaciones Java estándar (ej. Tomcat), la configuración evaluada y certificada corresponde a la basada en un despliegue con microservicios mediante contenedores que ejecutan en un entorno Docker.

17. Por tanto, la fase de despliegue e instalación (descrita en más detalle en los siguientes subapartados y en el apartado "4.6. INSTALACIÓN") se limita a desplegar las imágenes de los dos contenedores Docker que se proporcionan como parte de la solución, junto a la configuración específica de cada despliegue de GuardedBox (descrita en el apartado "5. FASE DE CONFIGURACIÓN").

18. Los administradores del servidor con el entorno de ejecución Docker, encargados del despliegue de GuardedBox, son miembros de plena confianza y velan por los mejores intereses en materia de seguridad de la organización, estarán debidamente capacitados y carecerán de cualquier intención maliciosa o conflicto de intereses al administrar y operar el sistema.

4.4.1 REQUISITOS HARDWARE

19. Los requisitos hardware mínimos para ejecutar la componente servidora de GuardedBox son:

    a) 2 CPUs: Una CPU para cada contenedor, es decir, 1 CPU para el contenedor con el back-end de la aplicación y 1 CPU para el contenedor de la base de datos.

    b) 1 GB de memoria RAM por cada contenedor o CPU.

    c) Suficiente espacio de almacenamiento para acomodar los datos de usuario en la base de datos, en función del uso que se hará de la solución (número de usuarios, número de secretos individuales y de grupo por usuario, número de grupos, y número y tamaño de los ficheros que se almacenen). Se recomienda comenzar con un mínimo de 20 GB de espacio de almacenamiento. El tamaño máximo de un secreto se puede calcular para la versión actual de GuardedBox teniendo en cuenta los siguientes factores:

        - Número máximo de propiedades por secreto: 20.
        - Tamaño máximo de una propiedad de tipo texto: 4.000 caracteres en formato Unicode.
        - Tamaño máximo de una propiedad de tipo fichero: 30 MB.

Nota: se debe tener en cuenta que estos valores máximos definidos por defecto pueden modificarse para cada despliegue o instancia de GuardedBox.

20. En caso de entornos con un elevado número de usuarios y mucha actividad, se recomienda ampliar los requisitos mínimos hardware detallados previamente.

4.4.2 SISTEMA OPERATIVO

21. GuardedBox puede desplegarse en cualquier sistema operativo soportado por el entorno de ejecución Docker, denominado Docker Engine [**REF1**] (ej. Linux, Windows, macOS).

22. Se recomienda emplear un servidor dedicado para ejecutar GuardedBox, minimizando los componentes software instalados en el mismo.
23. El sistema operativo del servidor con el entorno de ejecución Docker se configurará de forma segura, quedando fuera del presente procedimiento de empleo seguro los detalles para su securización (se recomienda consultar la [**REF2**] para obtener las guías CCN-STIC de seguridad actualizadas del sistema operativo empleado).
24. Los administradores del entorno o plataforma llevarán a cabo las actualizaciones de seguridad correspondientes al sistema operativo. Toda persona con capacidad de realizar tareas de administración tiene control total sobre el sistema y podría, por accidente o de forma deliberada, socavar la seguridad del sistema. Por tanto, el administrador de la plataforma debe ser una persona formada en gestión de sistemas operativos, con buen conocimiento de los principios de seguridad y concienciado con la seguridad de la información gestionada por la organización.
25. Los administradores de la plataforma deberán integrar el servidor de GuardedBox en su entorno de Tecnologías de la Información (TI) para las tareas de backup, gestión, monitorización del servicio, entorno de logs, soporte y mantenimiento, etc.
26. Aunque la versión actual de GuardedBox incluye funciones de auditoría para identificar qué usuarios han llevado a cabo cada acción relativa al uso de la solución, y que puedan responder ante ellas, un administrador podría acceder a la base de datos o al servidor donde esta reside, y podría eliminar las tablas de auditoría, o todos los contenidos del servidor o de la base de datos. Por tanto, la confianza en el administrador es un elemento clave para la correcta operación de la solución.
27. Se requiere la existencia de un usuario con privilegios de administración a nivel de sistema operativo en el servidor con el entorno de ejecución Docker, para la correcta instalación y configuración de GuardedBox (ver apartado "5.2.1. ADMINISTRACIÓN LOCAL Y REMOTA").

4.4.3 ENTORNO DE EJECUCIÓN DOCKER

28. El entorno de ejecución Docker (o *Docker Engine*) se configurará de forma segura, quedando fuera del presente procedimiento de empleo seguro los detalles para su securización (se recomienda consultar la [**REF5**] para obtener la guía CCN-STIC de seguridad en contenedores).
29. El entorno de ejecución Docker del servidor debe estar preparado para (re)iniciar los contenedores de GuardedBox en el arranque del sistema, haciendo que la solución ejecute automáticamente y maximizando así su disponibilidad ante reinicios del servidor.
30. Se recomienda hacer uso de la última versión disponible de *Docker Engine* en todo momento.
31. Los administradores de la plataforma llevarán a cabo las actualizaciones de seguridad correspondientes al entorno de ejecución Docker siguiendo las prácticas de seguridad aprobadas por la organización.

4.4.4 SERVICIO DE CORREO ELECTRÓNICO

32. GuardedBox requiere de acceso al servicio de correo electrónico para poder enviar los enlaces asociados al proceso de registro, los códigos de acceso de un solo uso que se emplean como segundo factor de autentificación (2FA), diferentes notificaciones de seguridad, así como notificaciones vinculadas a las actividades de los usuarios en la solución.
33. GuardedBox puede utilizar cualquier servicio de correo electrónico con SMTP, recomendándose el uso de SMTPS (habitualmente en el puerto 587/tcp o, antiguamente, 465/tcp), es decir, SMTP sobre TLS, pudiendo hacer uso de STARTTLS.
34. Los detalles de configuración de la cuenta de usuario en el servidor de correo electrónico están disponibles en el apartado "5.16. CONEXIÓN AL SERVIDOR DE CORREO ELECTRÓNICO".
35. La configuración detallada del servicio de correo electrónico queda fuera del alcance del presente procedimiento de empleo seguro.

4.4.5 SERVICIO DE DNS

36. Si el acceso a GuardedBox se realiza a través de un nombre en el servicio DNS o *hostname* (ej. www.guardedbox.com), opción recomendada desde el punto de vista de seguridad para su integración con HTTPS y el certificado digital asociado (en lugar de mediante la dirección IP directamente), se procederá a dar de alta el nombre en el servicio DNS de la organización.

NOTA: para poder obtener el certificado digital para HTTPS es un requisito habitual disponer del registro en el servicio de DNS previamente.

37. Se recomienda hacer uso de DNSSEC en el servicio DNS de la organización, con el objetivo de proporcionar autenticidad e integridad sobre los registros DNS.
38. Complementariamente, se recomienda que los navegadores web o equipos de los usuarios finales de GuardedBox hagan uso de DoH o DoT con el objetivo de proporcionar confidencialidad sobre el uso del servicio DNS por parte de los clientes.

4.4.6 COMPONENTES DE GUARDEDBOX

39. Tal como se detalla en el apartado "1.2. COMPONENTES PRINCIPALES DE GUARDEDBOX" GuardedBox está formado por tres componentes principales que, como se indica a continuación, han sido diseñados, desarrollados e implementados para ejecutar de manera segura:

    a) **Back-end** (servidor): GuardedBox se proporciona como solución principalmente mediante el contenedor Docker de back-end. Dicho contenedor ya tiene aplicadas las recomendaciones y mejores prácticas de seguridad para reducir su exposición frente a potenciales ataques e implementar el principio de mínimos privilegios.

    b) **Front-end** (cliente): al tratarse de una aplicación web, GuardedBox proporciona una componente cliente (front-end) que ejecuta en el navegador web de los usuarios. En

las conexiones al servicio web de la solución, el back-end proporciona el código correspondiente al front-end, de forma que no es necesario instalar ningún elemento en los dispositivos cliente de los usuarios.

c) Tal como se describe en el apartado "5.9. AUTO-CHEQUEOS", el front-end de GuardedBox comprueba que dispone de la última versión de la solución y, en caso contrario, insta al usuario a hacer uso siempre de la última versión disponible.

d) GuardedBox soporta cualquier navegador web moderno, tanto en equipos tradicionales como en dispositivos móviles. La organización es responsable de mantener los navegadores web de los usuarios convenientemente actualizados a la última versión disponible y configurados de forma segura.

e) **Base de datos** (persistencia): GuardedBox utiliza una base de datos relacional MySQL, que se proporciona como parte de la solución dentro del contenedor Docker de base de datos asociado a la capa de persistencia. Dicho contenedor ya tiene aplicadas las recomendaciones y mejores prácticas de seguridad para reducir su exposición frente a potenciales ataques e implementar el principio de mínimos privilegios.

f) Los detalles de configuración de las cuentas de usuario en la base de datos están disponibles en el apartado "5.15. CONEXIÓN A LA BASE DE DATOS".

4.5 COMPROBACIÓN DE LA AUTENTICIDAD E INTEGRIDAD DEL SOFTWARE

40. La solución de GuardedBox se proporciona mediante dos imágenes de contenedores Docker, uno asociado al back-end (que también contiene el front-end) y otro asociado a la base de datos con la capa de persistencia, denominados "guardedbox" y "guardedbox-mysql" respectivamente.

41. Las imágenes de los contenedores para la última versión de GuardedBox, proporcionadas por DinoSec, vendrán acompañadas de los hashes SHA256 de ambas imágenes Docker.

42. Antes de proceder a su instalación, se debe comprobar la autenticidad e integridad del software, comparando los hashes SHA256 de las imágenes de los dos contenedores Docker a desplegar, con los proporcionados por DinoSec.

43. Para la **versión 8.4.0 de GuardedBox** los hashes SHA256 son los siguientes:

Hashes SHA256 de las imágenes de los dos contenedores Docker: versión 8.4.0 de GuardedBox
Contenedor del back-end (y front-end): **guardedbox-8.4.0.tar**
3802bf256716e1ebbaccdaa483e71568609a7eb1b353b0a7d1cb54f231965f4e
Contenedor de la BD: **guardedbox-mysql-1.0.1.tar**
313790d708c28ddb2029f6fce8c722305c646b47ee4775ca8e90b65367e6efd3

4.6 INSTALACIÓN

44. La fase de instalación se limita a desplegar los dos contenedores Docker cuyas imágenes se proporcionan como parte de la solución, junto a los ficheros de configuración y de propiedades (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX").

45. Los requisitos para la instalación se han descrito en todos los subapartados previos dentro del apartado "4.4 CONSIDERACIONES PREVIAS".

46. Una vez completados todos los pasos asociados a la configuración inicial de GuardedBox (ver y completar el apartado "5. FASE DE CONFIGURACIÓN"), será necesario transferir (si no se ha hecho antes), los dos ficheros ".tar" con las imágenes de los dos contenedores Docker de GuardedBox a un directorio común (ej. "/srv/guardedbox"), dentro del directorio "./containers", separados por subdirectorios ("./app" y "./db"), junto a los ficheros de propiedades dentro del directorio "./secrets" y al fichero de configuración principal "docker-compose.yml":

```
/srv/guardedbox:
        docker-compose.yml
        ./containers:
                ./app/guardedbox-8.4.0.tar
                ./db/guardedbox-mysql-1.0.1.tar
        ./secrets:
                <Ficheros de propiedades de GuardedBox>
        ./volumes/db/data:
                <Ficheros de la base de datos de GuardedBox>
```

Figura 1 – Estructura de directorios de GuardedBox en el servidor

47. Se debe crear adicionalmente el directorio "./volumes/db/data", con permisos para "nobody:nogroup", empleado para el almacenamiento de la base de datos.

48. Una vez disponibles en el servidor con el entorno de ejecución Docker las dos imágenes de los contenedores, y los ficheros de configuración y de propiedades de GuardedBox, y habiéndose creado el directorio para el volumen Docker que será empleado por la capa de persistencia para la base de datos, y tras cargar en Docker las dos imágenes de los contenedores ("docker load"), basta con proceder a arrancar GuardedBox mediante Docker Compose [**REF7**] (una herramienta para la definición y ejecución de aplicaciones Docker compuestas por múltiples contenedores), mediante el siguiente comando desde el directorio en el que se encuentra el fichero "docker-compose.yml":

```
docker compose up -d
```

Nota: se debe recordar que el responsable del despliegue de GuardedBox en la organización no llevará a cabo las fases de despliegue e instalación, ni la fase de configuración, de manera independiente, sino en colaboración con DinoSec, que se encargará de parametrizar la instancia concreta de GuardedBox según los requisitos de la organización.

49. Por tanto, GuardedBox se inicia y detiene ejecutando o parando los contenedores Docker asociados, mediante los siguientes comandos de Docker Compose:

```
docker compose up -d
docker compose down
```

50. Mediante el siguiente comando es posible monitorizar los logs de GuardedBox:

```
docker compose logs -f
```

51. Una vez GuardedBox ha arrancado correctamente, se puede empezar a hacer uso de la solución mediante un navegador web, accediendo al nombre asignado para GuardedBox en el servicio DNS (ej. www.guardedbox.com) por la organización (ver apartado "4.4.5. SERVICIO DE DNS"), obteniéndose acceso a la página web principal de login de GuardedBox:

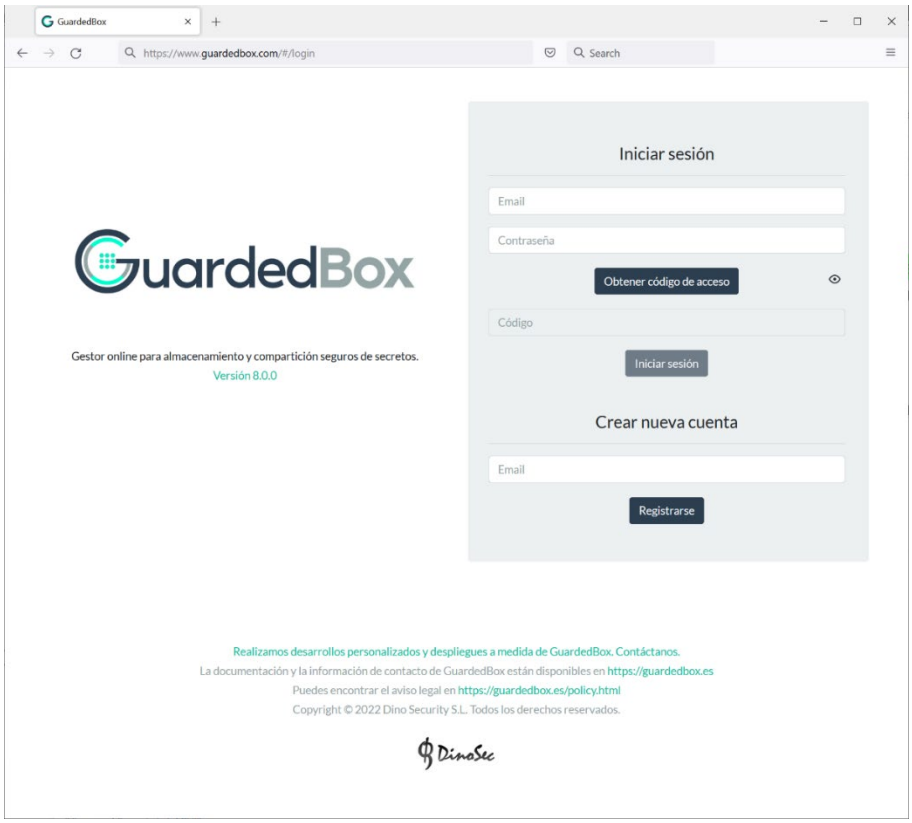


Figura 2 - Página web principal de login de GuardedBox

5. FASE DE CONFIGURACIÓN

5.1 AUTENTICACIÓN

52. El acceso al interfaz web de GuardedBox se realiza mediante un navegador web empleando HTTPS, HTTP sobre TLS 1.2 o 1.3 (ver apartado "5.4. CONFIGURACIÓN DE PROTOCOLOS SEGUROS"), haciendo uso de un certificado digital válido (ver apartado "5.5. GESTIÓN DE CERTIFICADOS").

53. GuardedBox lleva a cabo la autentificación de los usuarios a través de su interfaz web, independientemente del rol del usuario (usuario final o administrador), mediante un mecanismo de verificación avanzado en el que el servidor (o back-end) no requiere almacenar ninguna representación de la contraseña (ej. hash), tal como ocurre en la mayoría de servicios, evitando así ataques de diccionario, fuerza bruta o tablas arcoiris (*rainbow tables*) en caso de compromiso del servidor.

54. El usuario se debe haber registrado previamente en GuardedBox, demostrando durante el proceso de registro que es el propietario de la cuenta de correo electrónico (e-mail) asociada a la cuenta de usuario de GuardedBox.

55. El proceso de autentificación de GuardedBox se basa en un mecanismo de desafío y respuesta (*challenge/response*[1]) en el que el usuario, de manera simplificada, tras introducir sus credenciales (usuario y contraseña), deriva una clave criptográfica de login para el proceso de autentificación.

56. En cada intento de autentificación por parte del usuario, el back-end remite al front-end un desafío (o *challenge*) único, que es firmado mediante la clave privada de login, para generar una respuesta (correspondiente a la firma del desafío) que es remitida al servidor.

57. El servidor verifica la firma de dicha respuesta para ese desafío y ese usuario concretos, empleando su clave pública de login, que fue almacenada durante el proceso de registro de la cuenta del usuario en GuardedBox.

58. Si la firma es correcta, el usuario es válido, ya que dispone de la clave privada de login correcta derivada a partir de su contraseña, por tanto, dispone de la contraseña correcta; en caso contrario, el proceso de autentificación falla.

59. Adicionalmente a la verificación de las credenciales del usuario (usuario y contraseña), GuardedBox requiere llevar a cabo la verificación de un segundo factor de autentificación (2FA), ya sea mediante códigos de acceso o empleando un dispositivo (o navegador web) de confianza, previamente registrado por el usuario.

60. Estas capacidades asociadas al 2FA, así como la posibilidad de cambiar la contraseña y/o de renovar las claves criptográficas en cualquier momento, incluso sin cambiar la contraseña, están disponibles para el usuario a través de las preferencias de la sección de gestión de la cuenta de usuario.

[1] Similar a ASSCRAM (Asymmetrically Signed Salted Challenge Response Authentication Mechanism).

61. GuardedBox implementa diferentes mecanismos defensivos avanzados en el proceso de autentificación para evitar ataques de enumeración (pre-autenticación), y proteger así las credenciales y el valor del 2FA de los usuarios, incluyendo la generación de notificaciones de seguridad por e-mail para alertar al usuario de actividades sospechosas.

62. De manera similar, GuardedBox implementa mecanismos defensivos adicionales en el proceso de autentificación y de registro para evitar ataques de fuerza bruta, introduciendo tiempos de espera y gestionando escenarios de realización de múltiples intentos fallidos de autenticación, ya sea por credenciales o por 2FA, o de registro, ya sea directamente o por invitación.

Nota: los valores, número de intentos, temporizadores, etc., de todos estos mecanismos de seguridad avanzados, así como los parámetros de los códigos de acceso del 2FA, son configurables (opcionalmente) a través del fichero de propiedades del back-end de GuardedBox (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX"), concretamente a través del conjunto de propiedades "security-parameters.".*

Nota: opcionalmente, como mecanismo de autentificación adicional, GuardedBox soporta el uso de autentificación HTTP básica (Basic Authentication), que es protegida mediante los mecanismos de conexión a través de HTTPS (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX").

63. La política asociada a la longitud y complejidad de las contraseñas admitidas por GuardedBox para todos los roles de usuario se detalla en el apartado "5.2.3. POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN".

Nota: la potencial integración con servidores de autenticación externos, complementando el proceso de autentificación de GuardedBox, se detalla en el apartado "5.6. SERVIDORES DE AUTENTICACIÓN".

64. Adicionalmente, GuardedBox permite el uso de *API tokens* únicos como mecanismo de autentificación para el acceso a *endpoints* específicos de la API. Estos *endpoints* de la API de GuardedBox permiten (opcionalmente) su integración con otros componentes externos y servicios corporativos, por ejemplo, un módulo que permite establecer la lista concreta de usuarios de dominio habilitados y deshabilitados en GuardedBox a nivel empresarial, y que puede ser actualizada dinámicamente en cualquier momento.

65. Una representación de estos *API tokens* es almacenada en la BD de GuardedBox, restringiendo el acceso al *endpoint* concreto y al rol asociado a cada token, empleando para ello un hash HMAC SHA256 mediante una clave criptográfica propia del back-end.

66. Las credenciales de autentificación empleadas por GuardedBox para su interacción con otros componentes propios, como el certificado digital utilizado para HTTPS o su conexión con la base de datos, o con otros componentes externos, como el servidor de correo electrónico para el envío de notificaciones, se gestionan a través de las propiedades de GuardedBox (ver apartado "5.17. CONFIGURACIÓN DE LAS

PROPIEDADES DE GUARDEDBOX"), y son almacenadas como secretos de Docker[2] y protegidas por parte del sistema operativo del servidor en el que ejecuta GuardedBox.

5.2 ADMINISTRACIÓN DEL PRODUCTO

5.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

67. Administración del servidor de GuardedBox:
68. Las fases de despliegue, instalación y configuración de GuardedBox se completan localmente mediante un terminal empleando la consola del servidor, transfiriendo los ficheros necesarios también de manera local, por parte del administrador del servidor, sistema, entorno o plataforma.
69. Las tareas de administración, operación y mantenimiento de GuardedBox a nivel de sistema operativo del servidor se llevan a cabo localmente. El acceso a la consola del servidor se puede proporcionar de manera presencial (*on-site*) o mediante una conexión remota a través de una VPN.
70. En caso presencial, el acceso debe estar restringido al personal autorizado.
71. En caso de disponibilidad de una conexión remota mediante VPN, se habilitará el acceso hacia el servidor en el que ejecuta GuardedBox únicamente al personal autorizado, y se proporcionarán los elementos necesarios para el control de acceso sobre el mismo (segundo factor de autentificación, por ejemplo, mediante tokens físicos, credenciales de usuario, etc.).
72. La configuración de la VPN en el entorno de la organización queda fuera del alcance del presente procedimiento de empleo seguro.
73. Aunque se requiere disponer de un usuario con privilegios de administración a nivel de sistema operativo en el servidor con el entorno de ejecución Docker durante el proceso de despliegue, instalación y configuración inicial (ver apartado "4.4.2. SISTEMA OPERATIVO"), posteriormente, todos los ficheros y directorios de GuardedBox están asociados a un usuario no privilegiado de sistema operativo (ej. usuario "guardedbox").
74. Administración de GuardedBox (interfaz web):
75. Las tareas de administración para la gestión de las cuentas de usuario y del sistema de auditoría se realizan a través de la propia interfaz web de GuardedBox, accediendo con un usuario administrador de GuardedBox.

5.2.2 CONFIGURACIÓN DE ADMINISTRADORES

76. GuardedBox dispone de dos roles para las cuentas de usuario: **usuario administrador** y **usuario final** de GuardedBox, tal como se describe en el apartado "7. UTILIZACIÓN SEGURA DE GUARDEDBOX".

[2] Los secretos son montados mediante Docker Compose, ya que no se hace uso de Docker Swarm para gestionar un *swarm* o clúster de Docker Engines; en entornos de alta disponibilidad se recomienda el uso de Kubernetes (ver apartado "5.11. ALTA DISPONIBILIDAD").

77. Por defecto, todos los usuarios que se registran en GuardedBox disponen del rol de usuario final.

78. Para configurar inicialmente el rol de administrador para un usuario (ej. "administrador@guardedbox.com"), este debe registrarse en primer lugar en GuardedBox:

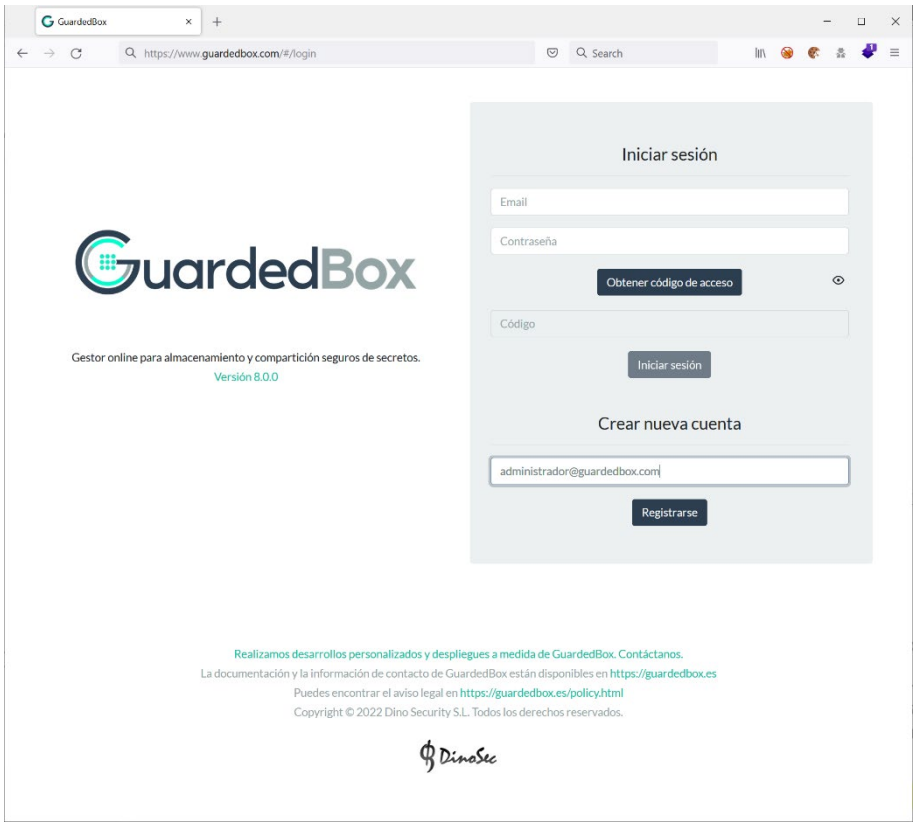


Figura 3 – Registro inicial del usuario administrador de GuardedBox

79. Una vez completado el registro, el administrador del despliegue debe de acceder manualmente a la base de datos y otorgar el rol de administrador a dicho usuario (ver apartado "5.18. CONFIGURACIÓN DEL USUARIO ADMINISTRADOR DE GUARDEDBOX").

80. Se recomienda llevar a cabo esta tarea como paso inicial durante la fase de despliegue e instalación (ver apartado "4 FASE DE DESPLIEGUE E INSTALACIÓN ") y, concretamente, como uno de los pasos finales de la fase de configuración inicial de este apartado "5. FASE DE CONFIGURACIÓN".

5.2.3 POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN

81. Tanto para los roles de usuario administrador como de usuario final, GuardedBox permite definir la política asociada a la longitud y complejidad de las contraseñas admitidas por GuardedBox a través del fichero de propiedades del front-end (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX"), concretamente mediante las siguientes propiedades:

```
"registration": {
    ...
```

```
        "passwordMinLength": 16,
        "passwordMinStrength": 80
    },
```

82. Por defecto GuardedBox impone un mínimo de 16 caracteres de longitud para las contraseñas de los usuarios, con una fortaleza mínima del 80% en base a un medidor propio de verificación de la fortaleza de las contraseñas, que tiene en cuenta la incorrecta generación de contraseñas en escenarios reales (incluso aún combinando caracteres de diferentes tipos), y que adicionalmente tiene en cuenta el uso de múltiples juegos de caracteres, incluyendo caracteres en minúscula y mayúscula, números y caracteres especiales o símbolos (más y menos comunes), de manera correcta (ej. no siguiendo secuencias de teclas en el teclado físico).

83. GuardedBox proporciona capacidades a los usuarios para la renovación de sus contraseñas a lo largo del tiempo, promoviendo el uso de frases de paso (*passphrases*) y centrando esfuerzos en motivar a los usuarios a la selección de contraseñas realmente robustas en escenarios, y frente a ataques, reales.

Nota: GuardedBox permite a los usuarios renovar las claves criptográficas asociadas a su cuenta en cualquier momento, incluso sin cambiar su contraseña.

84. Complementariamente, GuardedBox proporciona tanto un generador como un medidor de la robustez de las contraseñas propios, tanto para los secretos que gestiona (con propiedades de tipo contraseña), como (en el caso del medidor) para la propia contraseña empleada por la cuenta del usuario:

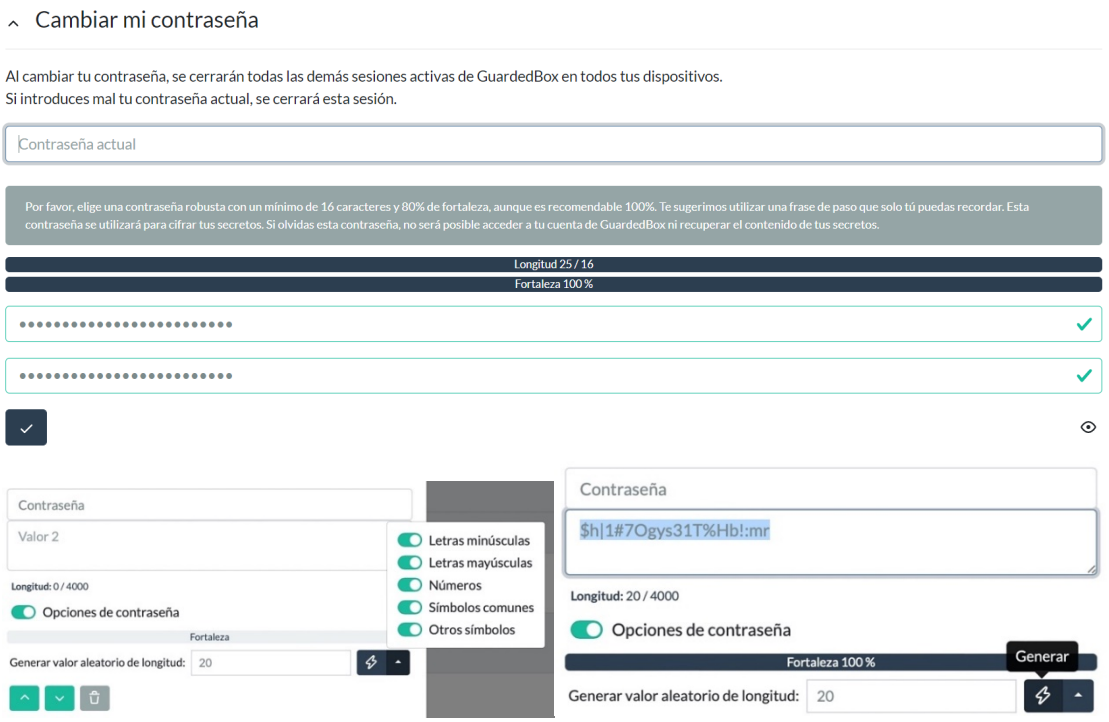


Figura 4 – Generador y medidor de la robustez de las contraseñas de GuardedBox: cuenta de usuario y secretos con contraseñas

85. GuardedBox permite definir la duración máxima de una sesión sin actividad (*timeout* de inactividad) a través del fichero de propiedades del back-end (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX"), así como la duración máxima de una sesión con actividad (*timeout* de autenticación), concretamente mediante las siguientes propiedades (el valor de la duración de una sesión sin actividad se traslada desde la propiedad del back-end al front-end):

```
back-end:
server.servlet.session.timeout = 5400
server.servlet.session.max-timeout = 86400
```

```
front-end:
    "session": {
        "timeout": 5400
    },
```

86. El valor por defecto de GuardedBox para la duración máxima de una sesión sin actividad es de una hora y media o 90 minutos (5.400 segundos). Si una sesión abierta ha estado inactiva todo ese tiempo, se cerrará automáticamente.

87. El valor por defecto de GuardedBox para la duración máxima de una sesión con actividad es de un día o 24 horas (86.400 segundos). Debido a que la comprobación de sesiones inactivas se realiza una vez al día, en el peor escenario, una sesión podría estar activa un máximo de 48 horas y 15 minutos. Una sesión que ha estado activa todo ese tiempo, será cerrada automáticamente, y el usuario deberá volver a autenticarse para abrir una nueva sesión.

88. Sin embargo, una vez la sesión ha sido cerrada, el usuario puede seguir trabajando con GuardedBox localmente en su navegador web sin sesión, si así lo desea. Este tipo de acceso únicamente permite consultar datos asociados a la cuenta de usuario y a sus secretos (individuales y de grupo, propios y recibido), pero no permite llevar a cabo ninguna edición o modificación de ningún elemento. En cualquier momento el usuario puede cerrar su sesión manualmente.

89. GuardedBox no impone ninguna restricción respecto al número de sesiones simultáneas que puede establecer un usuario, con rol de usuario final o de usuario administrador (o al número de usuarios administradores que pueden acceder simultáneamente), empleando diferentes pestañas del mismo o de distintos navegadores web, permitiendo por diseño este escenario de uso.

90. GuardedBox permite definir los mensaje de aviso y consentimiento en el inicio de sesión (*login banner*), y los términos y condiciones y política de privacidad durante el proceso de registro, a través de los ficheros de propiedades de idioma del front-end (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX"), concretamente mediante las propiedades "footer*" de los siguientes ficheros para los diferentes idiomas disponibles:

```
front-lang-[es|en]-2.json
```

5.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

91. Las comunicaciones (entrantes y salientes) requeridas por el servicio de GuardedBox, y que deben ser configuradas en los sistemas de red encargados del filtrado de tráfico en el entorno, son:

    a) Entrantes: (hacia GuardedBox)

        - Servicio web: HTTP (80/tcp) y HTTPS (443/tcp).

Nota: estas comunicaciones permiten el uso estándar de GuardedBox por parte de los usuarios finales, así como el acceso a endpoints específicos de la API de GuardedBox por parte de servicios corporativos en el caso de integraciones específicas (opcional), o por parte de la autoridad certificadora (CA) encargada de la renovación del certificado digital para HTTPS (opcional, según el modelo de renovaciones automáticas empleado por la CA).

    b) Salientes: (desde GuardedBox)

        - Servidor de correo electrónico: SMTPS (587/tcp o 465/tcp), o SMTP (25/tcp)[3] (ver siguiente apartado "5.4. CONFIGURACIÓN DE PROTOCOLOS SEGUROS").

92. Los puertos correspondientes a las comunicaciones web (entrantes) desde los equipos de los usuarios de la solución (tanto internos como externos) y a las comunicaciones de e-mail (salientes) hacia el servidor de correo electrónico, se deberán abrir en los cortafuegos correspondientes, tanto en el servidor con el entorno de ejecución Docker o servidor de aplicación, como en el resto de elementos perimetrales y equipos encargados de las redes de comunicaciones del entorno.

5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

93. GuardedBox únicamente hace uso de protocolos de comunicación seguros (ver apartado anterior).

94. Para recibir los establecimientos de las conexiones web por parte de los usuarios finales, GuardedBox hace uso de HTTP y HTTPS. Todo el tráfico HTTP (80/tcp) recibido es automáticamente redireccionado a HTTPS (443/tcp).

95. A nivel del protocolo HTTP, GuardedBox soporta las versiones HTTP/1.1 y HTTP/2. A través del fichero de propiedades del back-end (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX") es posible habilitar o deshabilitar HTTP/2 (en caso de estar deshabilitado se hará uso de HTTP/1.1), concretamente a través de la propiedad:

```
server.http2.enabled = true
```

Nota: GuardedBox dispone de propiedades de configuración avanzadas para, por ejemplo, poder seleccionar el conjunto de cabeceras HTTP de seguridad a emplear en el protocolo HTTPS para las comunicaciones web.

[3] Se desaconseja el uso de SMTP sin TLS, y utilizar únicamente SMTPS con STARTTLS.

96. A nivel del protocolo TLS, GuardedBox soporta las versiones TLS 1.2 y 1.3, únicas versiones recomendadas por las buenas prácticas de seguridad actualmente. A través del fichero de propiedades del back-end (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX") es posible habilitar o deshabilitar las versiones de TLS disponibles, concretamente a través de la propiedad:

```
server.ssl.enabled-protocols = TLSv1.3+TLSv1.2
```

Nota: GuardedBox dispone de propiedades de configuración avanzadas para, por ejemplo, poder seleccionar el conjunto concreto de suites de cifrado (cipher suites) a emplear en el protocolo TLS para las comunicaciones HTTPS. Por defecto GuardedBox está configurado para hacer uso de algoritmos y funciones criptográficas admitidos según la guía CCN-STIC 807 [REF6].

Asimismo, GuardedBox proporciona soporte para OCP Stapling, de cara a que el navegador web del usuario pueda validar de manera óptima el estado de revocación del certificado digital de GuardedBox.

97. Para generar las notificaciones de seguridad y actividad por e-mail, GuardedBox hace uso en su conexión con el servidor de correo electrónico de SMTPS (587/tcp), SMTP sobre TLS.

98. Se recomienda habilitar en GuardedBox la utilización de mecanismos de autenticación y del protocolo STARTTLS, permitiendo obligar a su uso, en su comunicación con el servidor de correo electrónico a través del fichero de propiedades del back-end (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX"), concretamente a través de las propiedades:

```
spring.mail.properties.mail.smtp.auth = true
spring.mail.properties.mail.smtp.starttls.enable = true
spring.mail.properties.mail.smtp.starttls.required = true
```

99. Todos los protocolos seguros que utiliza la solución utilizan algoritmos y funciones criptográficas admitidos según la guía CCN-STIC 807 [**REF6**], específicamente:

    - ECDSA con curvas P-256 o superior.
    - Funciones Hash SHA-256 o superior.
    - Cifrado AES-128 o superior.
    - Elliptic Curve Diffie-Hellman P-256 o superior.

5.5 GESTIÓN DE CERTIFICADOS

100. GuardedBox hace uso de HTTPS para ofrecer la aplicación web y proporcionar autentificación, cifrado e integridad.

101. Durante el proceso de despliegue, instalación y configuración inicial de GuardedBox es necesario obtener un certificado digital X.509 válido para HTTPS para el servidor web de GuardedBox, que debe ser emitido por una autoridad certificadora (CA) de confianza, de forma que pueda ser reconocido por todos los navegadores web de los usuarios que accedan a la solución.

102. GuardedBox hace uso de la cabecera HTTP de seguridad STS, entre otros motivos, para no permitir conexiones por parte de los usuarios si la validez del certificado digital no puede ser verificada.

103. La organización es responsable de seleccionar la CA que se encargará de emitir el certificado digital, así como de generar y remitirle la solicitud de certificado (CSR), y de obtener el certificado digital que será configurado en GuardedBox, en colaboración con DinoSec, empleando las herramientas externas definidas por la organización o sugeridas por la CA elegida (por ejemplo, mediante OpenSSL o Certbot).

104. El certificado digital obtenido deberá usar algoritmos y funciones criptográficas admitidos por la guía CCN-STIC 807 [**REF6**] , específicamente (en el caso de RSA, GuardedBox recomienda emplear claves de 4096 bits de longitud):

- RSA con claves de, al menos, 3072 bits de longitud.
- ECDSA con curvas P-256 o superior.
- DSA con claves de, al menos, 3072 bits de longitud.
- Funciones Hash SHA-256 o superior.

105. El certificado digital para HTTPS emitido por la autoridad certificadora (CA) seleccionada por la organización es habitualmente proporcionado mediante dos ficheros correspondientes al certificado emitido por la CA ("cert.pem"), o preferiblemente (opción recomendada por GuardedBox) correspondiente a la cadena completa de certificación en caso de existir CAs intermedias ("fullchain.pem"), y a la clave privada asociada ("privkey.pem").

106. Una vez se dispone del certificado, es necesario convertir sus dos ficheros en un único fichero en formato PKCS#12 (por ejemplo, mediante OpenSSL), que será utilizado directamente por GuardedBox:

```
openssl pkcs12 -export -in fullchain.pem -inkey privkey.pem -name server
-out server.p12
```

107. El proceso de conversión o exportación del certificado digital en un único fichero en formato PKCS#12 solicitará definir una contraseña que protegerá la clave privada asociada al certificado dentro del fichero "server.p12".

108. El fichero con el certificado digital en formato PKCS#12 deberá ser proporcionado a GuardedBox, para que pueda hacer uso del certificado en su servidor web empleando HTTPS, referenciado a través del fichero "docker-compose.yml" como un secreto de Docker, estando disponible en la carpeta de secretos (ej. "./secrets"); ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX":

```
./secrets/server.p12
```

NOTA: el fichero "server.p12" debe tener permisos 644 en el caso de emplearse Linux/Unix como SO del servidor.

109. Se recomienda hacer uso de una contraseña robusta aleatoria de (al menos) 43 caracteres de longitud, combinando números, letras mayúsculas y minúsculas, y signos de puntuación.

110. La contraseña seleccionada deberá ser proporcionada a GuardedBox, para que pueda hacer uso del certificado digital en su servidor web empleando HTTPS, a través del fichero de propiedades del back-end (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX"), concretamente a través de la propiedad:

```
server.ssl.key-store-password = <contraseña del certificado digital>
```

111. La versión actual de GuardedBox no dispone de funcionalidad asociada a certificados digitales cliente de los usuarios finales, por lo que no requiere realizar ninguna validación y no es necesario importar ningún certificado de las CA raíz (*root CA certificate*) que han emitido dichos certificados cliente.

112. El certificado de GuardedBox se renovará siguiendo las políticas de la organización, pudiendo realizarse de forma manual o automática (ej. a través de HTTPS, DNS, etc., según las opciones proporcionadas por la CA). Igualmente, el certificado se revocará y será sustituido en caso de cualquier incidente de seguridad siguiendo las políticas de la organización.

113. La gestión del ciclo de vida del certificado digital queda fuera del alcance del presente procedimiento de empleo seguro, y debe acomodarse a los procedimientos definidos por la organización.

5.6 SERVIDORES DE AUTENTICACIÓN

114. GuardedBox puede ser integrado en entornos empresariales con mecanismos corporativos de Single Sign-On (SSO) y diversos servidores externos y/o protocolos de autenticación (Directorio Activo, RADIUS, LDAP, SAML, Kerberos, etc.), empleando protocolos seguros de conexión (como TLS o IPsec), incluso mediante desarrollos personalizados.

115. Sin embargo, en todos esos escenarios sigue siendo necesario que los usuarios tengan asociada una contraseña robusta, exclusiva e independiente a su cuenta de GuardedBox, de la que se derivarán sus claves criptográficas. La contraseña de GuardedBox complementa las credenciales del mecanismo de autentificación corporativo empleado, y puede ser considerada en estos escenarios como un segundo, o incluso un tercer, factor de autentificación.

5.7 SINCRONIZACIÓN HORARIA

116. Se recomienda que el servidor con el entorno de ejecución Docker sobre el que ejecutará GuardedBox, al igual que todos los sistemas utilizados por la organización, se encuentre sincronizado con una fuente de tiempo fiable, mediante NTP, para permitir una alta fiabilidad en los sistemas de auditoría y *logging*, y de otros metadatos de tiempo manejados por la solución.

117. La configuración de NTP, o preferiblemente de NTS, del servidor en el que ejecuta GuardedBox queda fuera del alcance del presente procedimiento de empleo seguro.

5.8 ACTUALIZACIONES

118. GuardedBox no dispone de un servicio de actualizaciones, ni automático ni manual, dentro de la propia solución. Para actualizar la versión de GuardedBox, un aspecto fundamental desde el punto de vista de seguridad, se requiere transferir las imágenes Docker actualizadas, correspondientes a los nuevos contenedores asociados a una nueva versión de GuardedBox, al servidor con el entorno de ejecución Docker.

119. Las imágenes actualizadas de los contenedores Docker para la nueva versión de GuardedBox, junto a sus hashes SHA256, serán proporcionadas por DinoSec proactivamente, y se transferirán al servidor con el entorno de ejecución Docker y desplegarán siguiendo el procedimiento definido conjuntamente entre DinoSec y la organización durante la fase de despliegue e instalación (ver apartado "4.6. INSTALACIÓN").

120. Antes de proceder a la ejecución de la nueva actualización de GuardedBox, se debe verificar la autenticidad e integridad del software comparando los hashes SHA256 de las imágenes de los dos contenedores Docker con los hashes declarados oficialmente por DinoSec, de manera similar a como se recomendaba durante el despliegue e instalación inicial de GuardedBox (ver apartado "4.5. COMPROBACIÓN DE LA AUTENTICIDAD E INTEGRIDAD DEL SOFTWARE").

121. Dado que cualquier actualización de seguridad y/o nueva versión de GuardedBox modificará el/los hash/es del/los componente/s afectado/s, siempre es necesario obtener previamente los hashes SHA256, que serán proporcionados por DinoSec junto a las nuevas imágenes de los contenedores Docker, y verificarlos.

122. En caso de identificarse cualquier discrepancia en los hashes, comunicar con DinoSec, indicando el número de versión de GuardedBox y los datos de contacto del responsable en la organización.

123. Una vez verificada la integridad de las imágenes de los dos nuevos contenedores Docker, y tras transferirlas al servidor con el entorno de ejecución Docker, se deben cargar en Docker ("docker load"), y basta con proceder a arrancar GuardedBox mediante Docker Compose (ver apartado "4.6. INSTALACIÓN"), para disponer en ejecución de la nueva versión de GuardedBox.

5.9 AUTO-CHEQUEOS

124. GuardedBox verifica que el navegador web del usuario dispone de la última versión del front-end asociada a la última versión de la solución disponible en el back-end. En caso de discrepancia, GuardedBox notifica al usuario y le insta a cerrar la sesión actual y a abrir una nueva, que automáticamente hará uso de la última versión de GuardedBox disponible en el entorno.

125. GuardedBox realiza múltiples verificaciones sobre la integridad y coherencia de los datos disponibles para el usuario, y de los datos que el usuario remite desde el front-end al back-end, implementando múltiples capas de sincronización para acomodar escenarios en los que un mismo usuario dispone de diferentes sesiones activas y está modificando datos entre ellas que afectan a los mismos secretos, así como escenarios de compartición entre usuarios a través de grupos, donde múltiples usuarios pueden estar trabajando y editando los mismos secretos.

126. Adicionalmente, y de manera interna, GuardedBox realiza múltiples verificaciones durante su funcionamiento y operación sobre la integridad criptográfica de los datos almacenados, para validar que la información intercambiada entre usuarios es realmente compartida entre usuarios que pueden hacerlo, es decir, que están actualmente compartiendo un secreto individual, y/o que son miembros de un mismo grupo.

127. Por otro lado, los usuarios pueden verificar en todo momento la integridad del software desde su navegador web, tal como se indica en el apartado "7.1. VERIFICACIÓN DEL SOFTWARE DE GUARDEDBOX EN EL LADO CLIENTE".

5.10 SNMP

128. La solución no requiere hacer uso de SNMP para su gestión.

5.11 ALTA DISPONIBILIDAD

129. GuardedBox está preparado para ejecutar tanto en un entorno *standalone* (es decir, en un único servidor), como en un entorno de alta disponibilidad con redundancia basado en Kubernetes y contenedores Docker [**REF5**]. La configuración del entorno Kubernetes, en caso de ser requerido, queda fuera del presente procedimiento de empleo seguro.

5.12 AUDITORÍA

130. GuardedBox dispone de dos mecanismos principales de *logging*, auditoría y registro del funcionamiento y de las actividades asociadas a la solución:

a) **Sistema de *logging* de GuardedBox**: genera registros de actividad sobre las actividades de la aplicación web desde un punto de vista técnico, los accesos HTTPS por parte de los clientes, posibles errores o excepciones, etc., a través de la consola de GuardedBox en el entorno de ejecución Docker.

b) **Sistema de auditoría de GuardedBox**: permite registrar y consultar todos los eventos que genera la actividad de los usuarios dentro de la solución (detallados en el siguiente apartado "5.12.1. REGISTRO DE EVENTOS"). Los detalles y capacidades de este sistema de auditoría se detallan en el "Manual de administrador de GuardedBox" [**REF4**].

131. El formato de salida del sistema de *logging* de GuardedBox puede ser configurado a través de las propiedades de GuardedBox (ver apartado "5.17. CONFIGURACIÓN DE LAS

PROPIEDADES DE GUARDEDBOX"), y concretamente de las propiedades "logging.*" y de sus ficheros asociados: "logback-access.xml" y "logback-root.xml".

132. En el caso de requerirse personalizaciones específicas del sistema de *logging* para un despliegue concreto de GuardedBox, DinoSec colaborará con la organización para adecuar este sistema en su instancia concreta de la solución.

133. El sistema de auditoría de GuardedBox se habilita a través del fichero de propiedades del back-end (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX"), concretamente a través de la propiedad:

```
audit-events.logging-enabled = true
```

134. La versión actual de GuardedBox incorpora un sistema de *blockchain* basado en firmas criptográficas encadenadas para asegurar la integridad y autenticidad de los registros asociados a los eventos de auditoría almacenados en base de datos.

5.12.1 REGISTRO DE EVENTOS

135. El objetivo del sistema de auditoría de GuardedBox en entornos empresariales es dejar registro de las acciones y actividades que se llevan a cabo desde el front-end por parte de todos los usuarios durante su uso normal de la solución.

136. Los detalles de donde se almacenan los registros del sistema de auditoría de GuardedBox se proporcionan en el apartado "5.12.2. ALMACENAMIENTO LOCAL".

137. GuardedBox registra todos los eventos asociados a las actividades de los usuarios y vinculados a las interacciones entre el front-end y el back-end de la solución. Por ejemplo:

a) Login y logout de usuarios.

b) Cambio de contraseña (o renovación de claves, sin cambio de contraseña) de los usuarios.

c) Eventos específicos de la funcionalidad de GuardedBox, por ejemplo, asociados a la cuenta de usuario, y a la creación y compartición de secretos:

- Modificación del rol de un usuario.
- Activación/desactivación de una cuenta.
- Modificación de las propiedades de un secreto individual o de grupo.
- Compartición de un nuevo secreto individual o de grupo.
- Eliminación de un secreto de grupo.
- Adición de un usuario a un grupo.
- Eliminación de un usuario de un grupo.
- Modificación de las propiedades de un grupo.
- Envío de una invitación para registro en GuardedBox.
- Compleción de un registro por parte de un usuario al que se ha enviado un enlace de invitación.

- Se produce un intento de inicio de sesión con credenciales correctas y un código de acceso incorrecto.
- Se intenta crear una cuenta para una dirección de e-mail que ya está registrada.
- Etc.

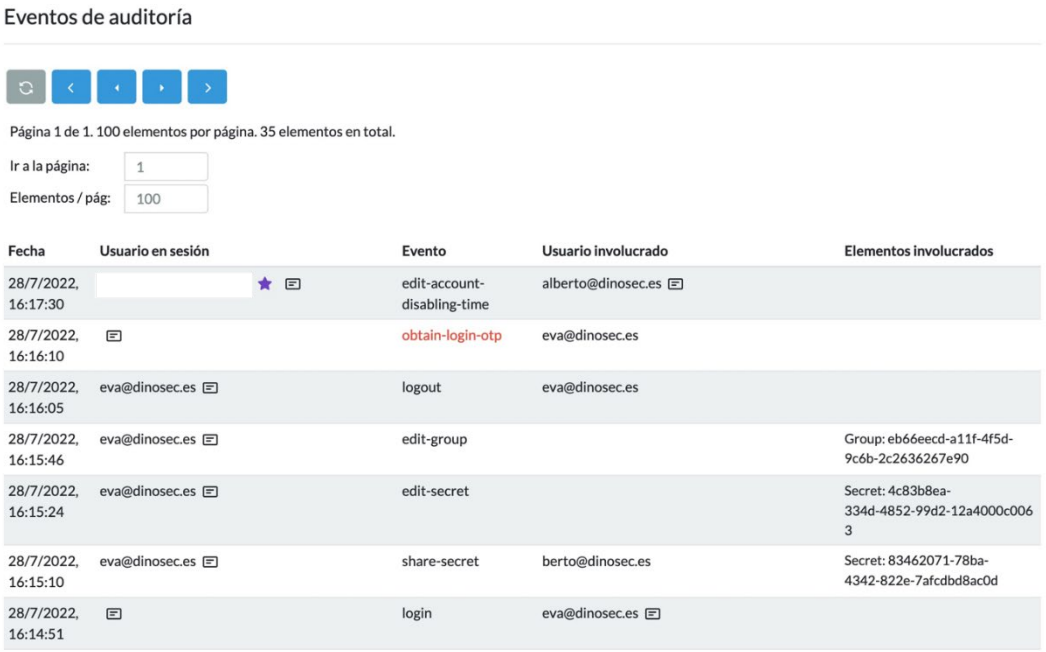


Figura 5 – Tabla de "Eventos de auditoría" de GuardedBox

138. La tabla del interfaz gráfico de usuario de GuardedBox para el sistema de auditoría incluye para cada registro la fecha y hora del evento, el usuario en sesión que generó la actividad, el tipo de evento (correspondiente al mensaje específico del evento), el resultado del evento (según su color), y otros usuarios y elementos involucrados en la acción del usuario en sesión (en caso de aplicar), junto a detalles adicionales de bajo nivel de estos últimos en función de su naturaleza. Los detalles de todos estos campos están disponibles en el "Manual de administrador de GuardedBox" [**REF4**].

139. El sistema de auditoría de GuardedBox conserva la orientación de cifrado extremo a extremo (EE2E) de los datos de usuario en la solución, por lo que ninguna información vinculada al contenido de los secretos se almacena en claro por parte del sistema de auditoría.

140. Adicionalmente, algunas funcionalidades que producen notificaciones por e-mail hacia los usuarios, de nuevo, sin incluir contenidos relevantes conservando la orientación E2EE, también quedan registradas en el servidor de correo electrónico.

5.12.2 ALMACENAMIENTO LOCAL

141. El sistema de *logging* de GuardedBox permite procesar y redirigir todos los registros y logs proporcionados a través de la consola de GuardedBox en el entorno de ejecución Docker, mediane la salida estándar, a un fichero local.

142. La redirección de la salida estándar de GuardedBox a través del entorno de ejecución Docker hacia un fichero local se realizará siguiendo los procedimientos de gestión de logs definidos por la organización.

143. El sistema de auditoría de GuardedBox almacena localmente todos los eventos y registros en un tabla de base de datos de GuardedBox ("audit_event"), para su posterior consulta por parte de las funcionalidades disponibles en el interfaz web de GuardedBox para el usuario administrador de GuardedBox a través de la vista "Eventos de auditoría" (ver detalles en el "Manual de administrador de GuardedBox" [**REF4**]):

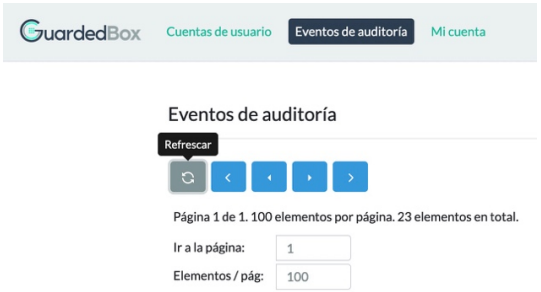


Figura 6 – Vista de "Eventos de auditoría" para el usuario administrador de GuardedBox

144. Alternativamente, los eventos y registros del sistema de auditoría de GuardedBox podrían ser consultados directamente a través de la base de datos de GuardedBox si se dispone de acceso a, o de una copia de, la misma.

145. La vista "Eventos de auditoría" solo permite su consulta por parte de los usuarios autorizados, correspondientes a los usuarios administradores de GuardedBox, y no permite a ningún usuario modificar o eliminar los registros de auditoría.

146. Los registros del sistema de auditoría de GuardedBox solo pueden ser eliminados accediendo a la tabla asociada en la base de datos por parte del administrador del despliegue de la solución.

147. Ambos sistemas, *logging* y auditoría de GuardedBox, se configuran según las indicaciones del apartado "5.12. AUDITORÍA".

148. El administrador del despliegue de GuardedBox debe monitorizar los recursos de almacenamiento disponibles en el servidor en el que ejecuta GuardedBox, empleando los mecanismos de monitorización y gestión definidos por la organización, con el objetivo de identificar si se está alcanzando el límite máximo de almacenamiento, de cara a que esta situación no interfiera sobre la correcta salvaguarda de los registros de auditoría y logs generados por la solución.

5.12.3 ALMACENAMIENTO REMOTO

149. El sistema de *logging* de GuardedBox permite procesar y redirigir todos los registros proporcionados a través de la consola de GuardedBox en el entorno de ejecución

Docker, mediane la salida estándar a un fichero local (como se ha indicado previamente), o a un sistema remoto, por ejemplo, a un servidor de Syslog.

150. Se recomienda hacer uso de Syslog (o Syslog-ng) sobre TLS en el servicio *logging* remoto y centralizado de la organización, con el objetivo de proporcionar confidencialidad, autenticidad e integridad sobre los registros de log.

151. La configuración de Syslog en el entorno de la organización queda fuera del alcance del presente procedimiento de empleo seguro.

5.13 BACKUP

152. GuardedBox únicamente requiere que se haga backup de la base de datos MySQL asociada a la capa de persistencia de la aplicación.

153. Adicionalmente, como parte de las actividades de backup del servidor en el que ejecuta GuardedBox, se recomienda hacer backup de los ficheros de configuración y de despliegue de la instancia concreta de GuardedBox (ver estructura completa de directorios y ficheros en el apartado "4.6. INSTALACIÓN").

154. Los mecanismos de backup empleados en el entorno del despliegue de GuardedBox, tanto para bases de datos como para ficheros, quedan fuera del alcance del presente procedimiento de empleo seguro, y deben llevarse a cabo siguiendo los procedimientos de backup definidos por la organización.

5.14 SERVICIOS DE SEGURIDAD

155. Tal como se ha descrito en la introducción del presente documento (ver apartado "1. INTRODUCCIÓN"), GuardedBox es una solución de gestión de secretos con cifrado extremo a extremo (E2EE), por lo que su propósito fundamental es proporcionar capacidades y servicios de seguridad avanzados para el intercambio de compartición y el almacenamiento seguro de información confidencial en tiempo real, tanto dentro como fuera de la organización.

156. Para ello GuardedBox ofrece múltiples capacidades focalizadas en el cifrado de la información compartida entre usuarios, y funcionalidades adicionales para permitir a los usuarios realizar una correcta gestión de los secretos, disponiendo de control sobre ellos en todo momento, y de poder ser notificados sobre potenciales escenarios de ataque en los que sus secretos podrían ser comprometidos, por ejemplo, si no son compartidos con los destinatarios correctos o si se producen eventos de compartición no esperados.

157. Las principales opciones de configuración asociadas a los mecanismos de seguridad más avanzados de GuardedBox, ya que por defecto toda la gestión de secretos se lleva a cabo de manera segura por diseño de la solución, están disponibles en la vista de la cuenta del usuario ("Mi cuenta") y en la vista de gestión de contactos ("Mis contactos").

158. Desde "Mi cuenta" es posible gestionar las preferencias de la cuenta del usuario (ver apartado "1.1. FUNCIONALIDADES Y CAPACIDADES") y, entre otros, verificar los detalles de la cuenta del usuario y de sus últimas sesiones, realizar la gestión de la contraseña y claves criptográficas, y del 2FA y los dispositivos de confianza, así como gestionar las

notificaciones de actividad vía e-mail, muchas de ellas asociadas a eventos de seguridad relevantes o a potenciales actividades sospechosas.

159. Desde "Mis contactos" es posible gestionar la lista de contactos del usuario, una lista propia, privada y protegida, junto al estado de confianza en la clave pública de cada uno de los contactos con los que se comparten secretos (tanto individualmente como a través de grupos, y tanto enviados como recibidos), un aspecto crucial en las tareas asociadas a la correcta verificación de la identidad de los usuarios (o extremos) cuando se hace uso de mecanismos de cifrado extremo a extremo (EE2E).

160. Todos los detalles de configuración, así como las recomendaciones de utilización, tanto de la vista para gestionar las preferencias de la cuenta del usuario en GuardedBox, como de la vista para gestionar la lista de contactos del usuario, están disponibles en el "Manual de usuario de GuardedBox" [**REF3**].

161. Todas las funcionalidades asociadas a la criptografía de la solución para la gestión de secretos utilizan por defecto algoritmos y funciones criptográficas admitidos según la guía CCN-STIC 807 [**REF6**], según se ha indicado ya en apartados anteriores, específicamente:

- ECDSA con curvas P-256 o superior.
- Funciones Hash SHA-256 o superior.
- Cifrado AES-128 o superior.
- Elliptic Curve Diffie-Hellman P-256 o superior.

5.15 CONEXIÓN A LA BASE DE DATOS

162. En resumen, las tareas de configuración inicial para la conexión a la base de datos (BD) incluyen:

a) La configuración del usuario "root" de MySQL en la BD para tareas de administración de bajo nivel.

b) La creación del esquema de la BD con las tablas necesarias para GuardedBox.

c) La creación del usuario de aplicación (ej. "guardedbox") para el acceso a la BD, únicamente con los permisos necesarios.

d) La creación de usuarios complementarios de gestión, edición y consulta (ej. "manager", "editor" y "monitor", respectivamente) en la BD para tareas de gestión, cada uno de ellos únicamente con los permisos necesarios.

163. Inicialmente, al ejecutar por primera vez el contenedor Docker de la BD durante la fase de despliegue e instalación, se creará el usuario administrador de la BD (usuario "root" en MySQL, existente por defecto), cuyas credenciales serán modificadas por unas suficientemente robustas y que estarán convenientemente protegidas. Estas credenciales serán diferentes a cualquier otra utilizada en otros componentes del mismo o de otros entornos.

164. Se recomienda hacer uso de una contraseña robusta aleatoria de (al menos) 43 caracteres de longitud, combinando números, letras mayúsculas y minúsculas, y signos de puntuación.

165. El usuario administrador de la BD será utilizado exclusivamente para llevar a cabo la configuración inicial, y para tareas de gestión y administración de la base de datos de bajo nivel (en caso de ser necesarias), pero no será utilizado por parte de GuardedBox en su conexión a la BD, ni debería ser utilizado para las tareas de gestión de la BD por parte del administrador del despliegue.

166. El usuario de aplicación (ej. "guardedbox") para el acceso a la BD por parte de GuardedBox hará uso del tipo de autentificación Standard.

167. A lo largo del presente apartado se recomienda hacer uso de una contraseña robusta aleatoria de (al menos) 43 caracteres de longitud, combinando números, letras mayúsculas y minúsculas, y signos de puntuación para todos los usuarios de BD. Se debe tener en cuenta que en algunos casos las contraseñas de los usuarios de gestión, edición y consulta de BD serán utilizadas por personal técnico y pueden requerir ser usables y legibles por humanos, en lugar de aleatorias, aun manteniendo su robustez. Sin embargo, la contraseña del usuario de aplicación para el acceso a la BD por parte de GuardedBox únicamente será utilizada por la aplicación, por lo que no debe ser legible, debe ser completamente aleatoria, incrementando así su robustez.

168. El usuario de aplicación para el acceso a la BD hará uso del tipo de autentificación nativa de MySQL, identificada como "mysql_native_password"[4].

169. Todos los usuarios de gestión y administración de la BD harán uso del tipo de autentificación de MySQL conocido como "Caching SHA-2 Pluggable Authentication", basado en hashes SHA256 (e identificado como "caching_sha2_password")[5].

170. Todos los usuarios de BD dispondrán de sus cuentas sin especificar una limitación en el host desde el que se puede establecer la conexión con la BD ("%"), ya que durante la ejecución de GuardedBox la BD nunca estará expuesta hacia el exterior, fuera del entorno de ejecución Docker.

171. La creación del esquema de la BD necesario para GuardedBox se llevará a cabo por parte de DinoSec durante la fase de despliegue e instalación, y la fase de configuración inicial, en colaboración con la organización, ya que la estructura de la BD puede cambiar en función de la versión de GuardedBox.

172. Se debe crear un usuario de aplicación (ej. "guardedbox") para el acceso a la BD por parte de GuardedBox, cuyas credenciales serán suficientemente robustas y estarán convenientemente protegidas. Estas credenciales serán diferentes a cualquier otra utilizada en otros componentes del mismo o de otros entornos.

173. El usuario de aplicación para el acceso a la base de datos será utilizado exclusivamente por parte de GuardedBox para llevar a cabo todas las interacciones con la capa de

[4] https://dev.mysql.com/doc/refman/8.0/en/native-pluggable-authentication.html
[5] https://dev.mysql.com/doc/refman/8.0/en/caching-sha2-pluggable-authentication.html

persistencia y consultar, almacenar y modificar los datos de los usuarios gestionados por la solución.

174. Se recomienda hacer uso de una contraseña aleatoria de (al menos) 43 caracteres de longitud, combinando números, letras mayúsculas y minúsculas, y signos de puntuación.

175. El usuario y la contraseña seleccionados deberán ser proporcionados a GuardedBox, para que pueda interactuar con la BD, a través del fichero de propiedades del back-end (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX"), concretamente, a través de las propiedades:

```
spring.datasource.username = <usuario de acceso a la BD>
spring.datasource.password = <contraseña de acceso a la BD>
```

176. Los permisos o privilegios a nivel del esquema de BD de GuardedBox del usuario empleado por la aplicación (es decir, para el acceso a la BD por parte de GuardedBox), incluyen SELECT, INSERT (UPDATE y DELETE), y LOCK TABLES.

177. Para todos los siguientes usuarios de BD se recomienda hacer uso de una contraseña aleatoria de (al menos) 43 caracteres de longitud, combinando números, letras mayúsculas y minúsculas, y signos de puntuación.

178. Se debe crear un usuario de gestión (ej. "manager") de BD, cuyas credenciales serán suficientemente robustas y estarán convenientemente protegidas. Estas credenciales serán diferentes a cualquier otra utilizada en otros componentes del mismo o de otros entornos.

179. Se debe crear un usuario de edición (ej. "editor") de BD, cuyas credenciales serán suficientemente robustas y estarán convenientemente protegidas. Estas credenciales serán diferentes a cualquier otra utilizada en otros componentes del mismo o de otros entornos.

180. Se debe crear un usuario de consulta (ej. "monitor") de BD, cuyas credenciales serán suficientemente robustas y estarán convenientemente protegidas. Estas credenciales serán diferentes a cualquier otra utilizada en otros componentes del mismo o de otros entornos.

181. Los permisos o privilegios, únicamente a nivel del esquema de BD de GuardedBox, de cada uno de estos usuarios son:

a) manager: Todos los privilegios.

b) editor: SELECT, INSERT (UPDATE y DELETE), y LOCK TABLES.

c) monitor: SELECT.

5.16 CONEXIÓN AL SERVIDOR DE CORREO ELECTRÓNICO

182. Se debe crear una cuenta de e-mail en el servicio de correo electrónico de la organización para su uso específico por parte de GuardedBox, cuyas credenciales serán suficientemente robustas y estarán convenientemente protegidas. Estas credenciales

serán diferentes a cualquier otra utilizada en otros componentes del mismo o de otros entornos.

183. El usuario de correo electrónico de GuardedBox será utilizado exclusivamente por parte de GuardedBox para llevar a cabo todas las interacciones con el servidor de correo electrónico y enviar e-mails a los usuarios que hacen uso de la solución.

184. Se recomienda hacer uso de una contraseña aleatoria de (al menos) 43 caracteres de longitud, combinando números, letras mayúsculas y minúsculas, y signos de puntuación.

185. El usuario y la contraseña seleccionados deberán ser proporcionados a GuardedBox, para que pueda interactuar con el servidor de correo electrónico mediante SMTPS, a través del fichero de propiedades del back-end (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX"), concretamente a través de las propiedades:

```
spring.mail.username = <usuario de acceso al servidor de e-mail>
spring.mail.password = <contraseña de acceso al servidor de e-mail>
```

5.17 CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX

186. GuardedBox permite, a través de sus ficheros de propiedades y de configuración, llevar a cabo la configuración detallada de los ajustes de la solución y poder así personalizar múltiples aspectos de su despliegue para cada instancia concreta:

a) El fichero de propiedades principal del back-end se denomina "**application.properties**".

b) El fichero de propiedades principal del front-end se denomina "**front-properties.json**".

c) Adicionalmente, se dispone de un **conjunto de ficheros de propiedades complementario** con los detalles del formato de los logs generados a través de la consola de GuardedBox en el entorno de ejecución Docker ("logback-access.xml" y "logback-root.xml"), con los logos personalizables ("custom-logo-[1|2].png"), y con los mensajes o literales empleados por la solución para los diferentes idiomas soportados, por ejemplo, español ("es") e inglés ("en"), tanto para el back-end ("back-lang-[es|en]-[1|2].properties"), como para el front-end ("front-lang-[es|en]-[1|2].json").

d) Por último, también forma parte de las propiedades de la solución el fichero con el certificado digital para HTTPS en formato PKCS#12: "**server.p12**" (ver apartado "5.6. GESTIÓN DE CERTIFICADOS").

187. A modo de **resumen**, para llevar a cabo el despliegue de GuardedBox, es necesario por tanto modificar las siguientes propiedades de los ficheros de configuración del back-end y del front-end (también referenciadas en otros apartados a lo largo del presente documento):

a) application.properties

- Nombre en el servicio DNS o *hostname* (ej. www.guardedbox.com) que será empleado en cada despliegue concreto para que GuardedBox ofrezca su

servicio (ver apartado "4.4.5. SERVICIO DE DNS"), asociado también al certificado digital para HTTPS (ver apartado "5.5. GESTIÓN DE CERTIFICADOS"):

- Propiedad:
  - server.external-url (ej. https://www.guardedbox.com).

- Adicionalmente es necesario reflejar el mismo nombre en el servicio DNS asociado a la instancia de GuardedBox en la configuración del dominio vinculado a la cookie empleada para la identificación de los dispositivos de confianza:
  - Propiedad:
    - trusted-devices.cookie-domain (ej. www.guardedbox.com).

- Contraseña que protege el certificado digital para HTTPS del fichero "server.p12" (ver apartado "5.5. GESTIÓN DE CERTIFICADOS"):
  - Propiedad:
    - server.ssl.key-store-password.

- Conexión de GuardedBox con la base de datos (ver apartado "5.15. CONEXIÓN A LA BASE DE DATOS"):
  - Propiedades:
    - spring.datasource.url: string de conexión a la BD.
    - spring.datasource.username: usuario de acceso a la BD.
    - spring.datasource.password: contraseña de acceso a la BD.

- Conexión de GuardedBox con el servidor de correo (ver apartado "5.16. CONEXIÓN AL SERVIDOR DE CORREO ELECTRÓNICO" y apartado "5.4. CONFIGURACIÓN DE PROTOCOLOS SEGUROS"):
  - Propiedades de conexión:
    - spring.mail.host: servidor de correo electrónico (*hostname*).
    - spring.mail.port: puerto asociado al servicio SMTPS.
    - spring.mail.username: usuario de acceso al servidor de e-mail.
    - spring.mail.password: contraseña de acceso al servidor de e-mail.
  - Propiedades de seguridad: soportando y obligando a la utilización de mecanismos de autenticación y del protocolo STARTTLS.
    - spring.mail.properties.mail.smtp.auth.
    - spring.mail.properties.mail.smtp.starttls.enable.
    - spring.mail.properties.mail.smtp.starttls.required.

- Temporizadores de duración de las sesiones de usuario (ver apartado "5.2.3. POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN"):
  - Propiedades:
    - server.servlet.session.timeout: duración máxima de una sesión sin actividad (en segundos).
    - server.servlet.session.max-timeout: duración máxima de una sesión con actividad (en segundos).

- Habilitar el sistema de auditoría de GuardedBox (ver apartado "5.12. AUDITORÍA"):
  - Propiedad:
    - audit-events.logging-enabled.
- Clave criptográfica utilizada por la blockchain del sistema de auditoría de GuardedBox para la generación de hashes HMAC (ver apartado "5.12. AUDITORÍA"):
  - Propiedad:
    - audit-events.signature-key.
- Claves criptográficas utilizadas por diversos mecanismos defensivos de GuardedBox (todos ellos referenciados en el apartado "5.1. AUTENTICACIÓN"), utilizadas para la generación de hashes HMAC (ver apartado "5.17. CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX"):
  - En cada despliegue se recomienda configurar estas claves con valores aleatorios de 256 bits en formato Base64.
  - Propiedades:
    - accounts.login-salt-from-unregistered-email-key: clave empleada en mecanismos defensivos de protección del proceso de autentificación.
    - api-tokens.token-database-representation-key: clave empleada en la representación de los *API tokens* en BD.
    - trusted-devices.email-representation-key: clave empleada en la representación del nombre de la cookie utilizada para la identificación de los dispositivos de confianza.

Nota: GuardedBox dispone de propiedades de configuración avanzadas en el back-end (opcionales) para, por ejemplo, poder habilitar adicionalmente el uso de autentificación HTTP básica (Basic Authentication), gestionar parámetros que permiten definir desde donde y quienes pueden llevar a cabo el proceso de registro (permiten restringir si se muestra la sección de registro para nuevos usuarios en la página web principal de login, concretamente desde redes o rangos de direcciones IP concretos o para usuarios de dominios concretos), configurar el formato de los logs generados a través de la consola de la solución (complementario al sistema de auditoría), configurar numerosos mecanismos, algoritmos y parámetros criptográficos, parámetros con los valores, número de intentos, temporizadores, etc., de múltiples mecanismos de seguridad defensivos avanzados, configurar la planificación para la ejecución de tareas programadas (que ejecutan de fondo) mediante un sistema de cron parametrizable, definir el tipo de licencia asociado a las nuevas cuentas de usuario que son registradas y su duración, propiedades de las cookies empleadas para la identificación de los dispositivos de confianza, y todas las referencias a los ficheros de literales de los idiomas y logos personalizados previamente referenciados.

b) front-properties.json

- Política de longitud y complejidad de las contraseñas de GuardedBox (ver apartado "5.2.3. POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN"):
  - Propiedad: (categoría "registration")

        - passwordMinLength: longitud mínima de la contraseña.
        - passwordMinStrength: complejidad mínima de la contraseña.
    - Duración máxima de una sesión sin actividad (ver apartado "5.2.3. POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN"):
        - Propiedad: (categoría "session")
            - timeout: duración máxima de una sesión sin actividad (en segundos), valor proporcionado realmente por el back-end.

Nota: GuardedBox dispone de propiedades de configuración avanzadas en el front-end (opcionales) para, por ejemplo, configurar numerosos mecanismos, algoritmos y parámetros criptográficos, etc.

188. Se recomienda no modificar el resto de propiedades del back-end y del front-end de GuardedBox, ya que por defecto disponen de valores considerados seguros y que son estándar para todas las instancias de GuardedBox, es decir, no requieren ser modificados entre diferentes despliegues de GuardedBox.

189. En el caso de requerirse personalizaciones específicas para un despliegue concreto de GuardedBox, DinoSec colaborará con la organización para adecuar su instancia concreta de la solución.

190. Adicionalmente a todos los ficheros previos específicos que forman parte de las propiedades de GuardedBox, se dispone del fichero de configuración principal "**docker-compose.yml**" con la configuración general de Docker para GuardedBox [**REF7**], las referencias a los dos contenedores Docker (denominados "guardedbox" y "guardedbox-mysql") y las referencias a todos los ficheros de propiedades y configuración, que es empleado para la ejecución de la solución (ver apartado "4.6. INSTALACIÓN").

191. El listado con los ficheros que son utilizados para la configuración de la solución por parte de DinoSec, para cada instancia de GuardedBox en cada despliegue concreto, se incluyen en el anexo "10. ANEXO: LISTADO DE FICHEROS DE CONFIGURACIÓN".

5.18 CONFIGURACIÓN DEL USUARIO ADMINISTRADOR DE GUARDEDBOX

192. Una vez el futuro usuario administrador de GuardedBox se ha registrado como un usuario final en la solución, tal como se detalla en el apartado "5.2.2. CONFIGURACIÓN DE ADMINISTRADORES", el administrador del despliegue accederá manualmente a la base de datos (BD) con el usuario "editor", con permisos de edición en la BD, y le otorgará el rol de administrador a dicho usuario en la tabla "account_" y columna "role", cambiando el valor a "account_admin", en lugar del valor por defecto "account_premium" para un usuario final.

193. Una vez realizado el cambio, si el usuario administrador accede de nuevo a GuardedBox, verá que es identificado con el rol de administrador ("Administrador" arriba a la derecha, en color morado) en lugar de como un usuario final ("Premium" arriba a la derecha, en color verde):

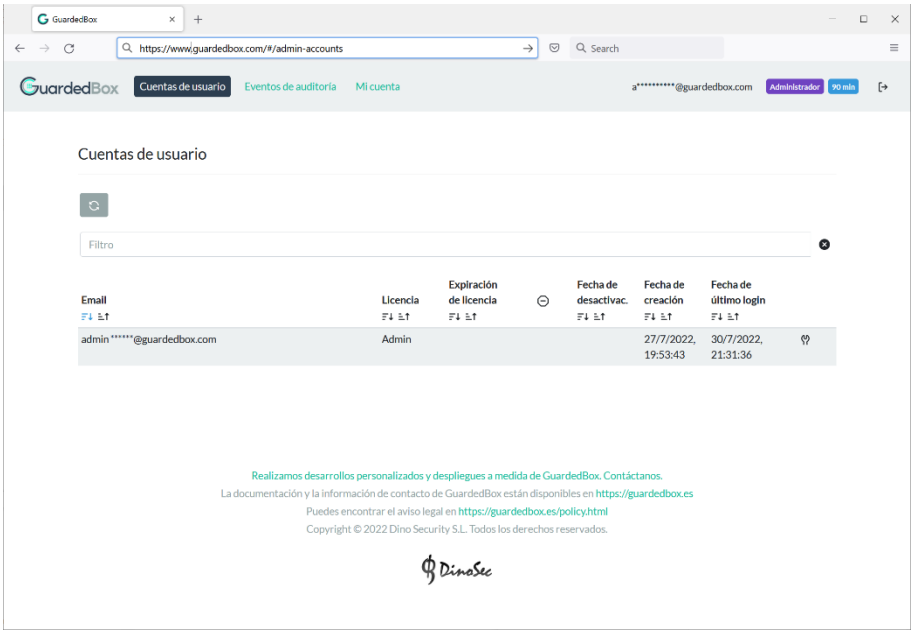


Figura 7 – Acceso inicial del usuario administrador de GuardedBox

194. La configuración de usuarios administradores de GuardedBox en la BD se llevará a cabo por parte de DinoSec, tanto durante la fase de despliegue e instalación, y la fase de configuración inicial, como posteriormente (en caso de ser necesario), en colaboración con la organización.

195. En este punto se pueden considerar completadas las fases de despliegue e instalación, y la fase de configuración inicial de GuardedBox, y se puede proceder a su utilización, operación y mantenimiento.

6. FASE DE OPERACIÓN

196. Durante la fase de operación y mantenimiento de la solución se recomienda disponer de (al menos) las siguientes revisiones periódicas y procedimientos operativos:

a) La solución debe estar instalada y mantenida en un entorno físico seguro. Esto incluye un edificio seguro con control de acceso o un entorno controlado por el administrador.

b) Comprobaciones periódicas del software del producto para comprobar que no se han introducido elementos no autorizados.

c) Mantenimiento y revisión periódica de los registros de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.

d) La información de auditoria se guardará en las condiciones y por el periodo establecido en la normativa de seguridad.

e) Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

f) Gestionar correctamente los certificados digitales utilizados, actualizándolos cuando sea necesario, por ejemplo, al expirar.

g) Realizar copias de seguridad periódicamente, así como configurar el envío periódico de copias a un servidor externo.

h) El entorno debe contar con las últimas actualizaciones de seguridad para protegerlo de amenazas y vulnerabilidades conocidas, y con objeto de mantener una configuración segura.

i) DinoSec informará a los responsables de la operación y mantenimiento del entorno de cualquier vulnerabilidad que afecte a GuardedBox y/o a cualquiera de sus dependencias o componentes, y proporcionará una nueva versión de GuardedBox mediante nuevos contenedores Docker con las imágenes actualizadas que corrijan dichas vulnerabilidades.

7. UTILIZACIÓN SEGURA DE GUARDEDBOX

197. El propósito de utilizar GuardedBox es proteger la confidencialidad de la información propia de la organización, tanto en su almacenamiento como en su compartición. Por ello, al margen de la configuración segura de la solución, se debe trasladar a todos los usuarios las buenas prácticas y recomendaciones de seguridad que se describen en el presente apartado.

198. GuardedBox define dos roles para las cuentas de usuario:

a) **Usuario administrador**: este rol es el responsable de gestionar las cuentas del resto de usuarios de GuardedBox, así como del sistema de auditoría, por ejemplo, para consultar sus registros o *logs*. Las cuentas de e-mail vinculadas a este rol no deben utilizarse para ningún otro propósito, ni deben enviar correos manualmente, evitando que exista conocimiento sobre su existencia, tanto interna como externamente. Este rol también permite configurar los ajustes de la cuenta de usuario del administrador.

b) **Usuario final**: este rol puede hacer un uso estándar de GuardedBox y, por ejemplo, crear, editar, compartir y recibir secretos tanto individuales como de grupo, o configurar los ajustes de la cuenta de usuario.

199. Existen recomendaciones de utilización segura de GuardedBox comunes a ambos roles, además de ciertas recomendaciones específicas para cada rol. Todas ellas, junto a los mecanismos detallados para aplicar estas recomendaciones, se describen en los correspondientes apartados del "Manual de usuario de GuardedBox" [**REF3**] y del "Manual de administrador de GuardedBox" [**REF4**]. Concretamente:

a) Usuario administrador [**REF4**]: apartado "Utilización segura por parte del usuario administrador de GuardedBox".

b) Usuario final [**REF3**]: apartado "Buenas prácticas para la correcta gestión de secretos".

200. Se recomienda proporcionar a los usuarios finales, y administradores, de GuardedBox de la organización nociones básicas de cifrado extremo a extremo (E2EE) y, en particular, de los mecanismos de verificación de identidad.

7.1 VERIFICACIÓN DEL SOFTWARE DE GUARDEDBOX EN EL LADO CLIENTE

201. GuardedBox permite verificar el software asociado al front-end desde el lado cliente, es decir, empleando el navegador web del usuario. Para ello, es necesario comprobar que se está haciendo uso de la última versión disponible de la solución, como los hashes SHA512 y SHA384 asociados al standard web SRI de los dos componentes web principales del front-end en la solución (el valor "<codigo>" está compuesto por 20 caracteres hexadecimales):

k) JavaScript: /js/bundle.*<codigo>*.js

l) CSS: /css/bundle.*<codigo>*.css

202. La versión de GuardedBox se muestra en la página web de login o autentificación, y los hashes SHA512 y SHA384 (en Base64), junto al nombre de los dos componentes web principales del front-end, se pueden obtener visualizando el código fuente de dicha página web de login con un navegador web:

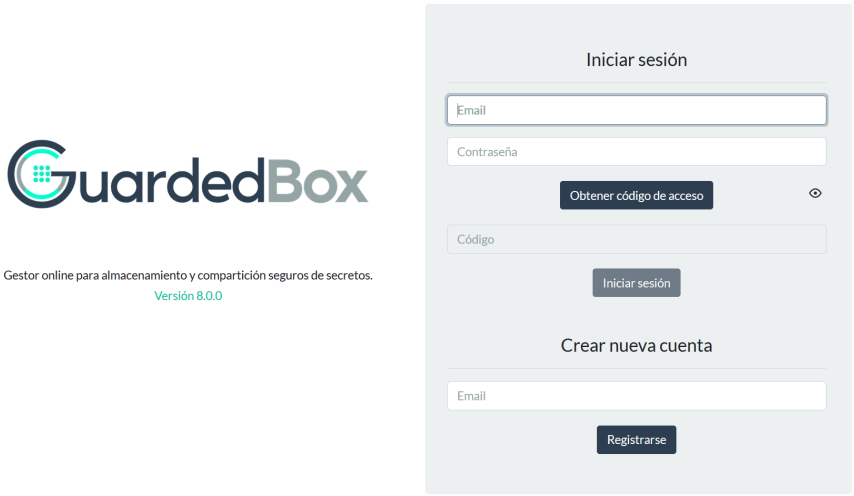


Figura 8 – Versión actual de GuardedBox en la página web principal de login

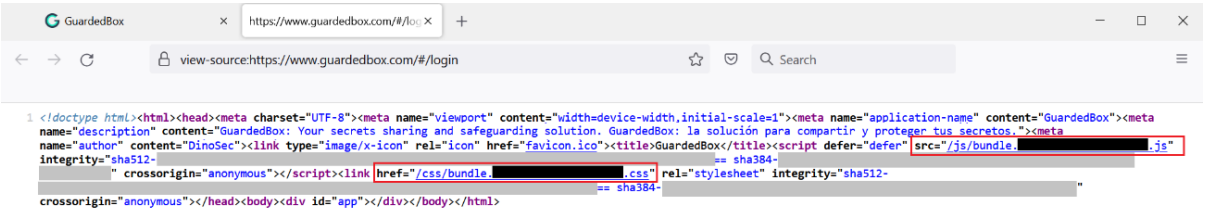


Figura 9 - Código fuente HTML de la página web principal de login de GuardedBox

203. Dado que cualquier actualización de seguridad y/o nueva versión de GuardedBox modificará los hashes (en color gris en la imagen previa) y los nombres de los dos componentes web principales del front-end (en concreto, el valor del "<codigo>"; en color negro en la imagen previa), se deben verificar sus valores y monitorizar cambios sobre los mismos para detectar si potencialmente se han obtenido elementos no autorizados en el lado del cliente.

204. En caso de identificarse cualquier discrepancia en los hashes, deberá comunicarse a DinoSec, indicando el número de versión de GuardedBox y los datos de contacto del responsable en la organización.

8. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Confirmación de las licencias	☐	☐	
Verificación de los requisitos hardware	☐	☐	
Verificación de los requisitos de SO	☐	☐	
Verificación de los requisitos del entorno de ejecución Docker	☐	☐	
Verificación de los requisitos del servicio de e-mail	☐	☐	
Verificación de los requisitos del servicio de DNS	☐	☐	
Comprobación de la autenticidad e integridad del software	☐	☐	
Instalación de GuardedBox	☐	☐	
Verificación del acceso web a GuardedBox	☐	☐	
CONFIGURACIÓN			
AUTENTICACIÓN			
Definir si se activará el acceso a *endpoints* mediante *API tokens*	☐	☐	
ADMINISTRACIÓN DEL PRODUCTO			
Verificar el acceso a la consola, y privilegios, en el servidor	☐	☐	
Configuración del usuario administrador de GuardedBox	☐	☐	
Definir la política de contraseñas	☐	☐	
Definir los parámetros de sesión	☐	☐	
Establecer el mensaje de aviso y consentimiento	☐	☐	
CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS			
Habilitar tráfico de red entrante hacia GuardedBox	☐	☐	
Habilitar tráfico de red saliente desde GuardedBox	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Configuración de las versiones del protocolo HTTP	☐	☐	
Configuración de las versiones del protocolo TLS	☐	☐	
Configuración del protocolo SMTPS	☐	☐	
GESTIÓN DE CERTIFICADOS			
Obtención del certificado digital para HTTPS de la CA	☐	☐	
Exportación del certificado digital en formato PKCS#12	☐	☐	
SERVIDORES DE AUTENTICACIÓN			
Definir si se realizará una integración en SSO	☐	☐	
SINCRONIZACIÓN HORARIA			
Configuración del protocolo NTP (o NTS) en el servidor	☐	☐	
ALTA DISPONIBILIDAD			
Definir si GuardedBox se desplegará en un entorno de HA	☐	☐	
AUDITORÍA			
Configurar el sistema de logging local	☐	☐	
Configurar el sistema de logging remoto	☐	☐	
Habilitar el sistema de auditoría	☐	☐	
BACKUP			
Configuración de los mecanismos de realización de backups	☐	☐	
CONEXIÓN A LA BASE DE DATOS			
Configuración del usuario administrador de la BD	☐	☐	
Creación del esquema de la BD	☐	☐	
Creación del usuario de aplicación para el acceso a la BD	☐	☐	
Creación de usuarios complementarios en la BD	☐	☐	
CONEXIÓN AL SERVIDOR DE CORREO ELECTRÓNICO			
Configuración de la conexión con el servidor de e-mail	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
CONFIGURACIÓN DE LAS PROPIEDADES DE GUARDEDBOX			
Configuración del fichero de propiedades del back-end	☐	☐	
Configuración del fichero de propiedades del front-end	☐	☐	
Configuración de los ficheros del sistema de *logging*	☐	☐	
Configuración de los ficheros de idiomas del back-end y front-end	☐	☐	
Configuración de los ficheros de logos personalizados	☐	☐	
OPERACIÓN			
Comprobaciones periódicas del software	☐	☐	
Mantenimiento y revisión periódica de los registros de auditoría	☐	☐	
Gestión y renovación del certificado digital para HTTPS mediante la CA	☐	☐	
Realización de copias de seguridad (backups)	☐	☐	
Actualizaciones de seguridad en el servidor	☐	☐	
Actualizaciones de la versión de GuardedBox	☐	☐	

9. REFERENCIAS

205. Documentación complementaria que se ha referenciado a lo largo del presente procedimiento de empleo seguro:

REF1 "Docker Engine". Docker.
https://docs.docker.com/engine/

REF2 "Listado de guías CCN-STIC". CCN-CERT.
https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html

REF3 "Manual de usuario de GuardedBox". Versión 1.0 (Versión 8.4.0 de GuardedBox). DinoSec.
https://www.dinosec.com/guardedbox/Manual_de_usuario_de_GuardedBox_v8.4.0.pdf

REF4 "Manual de administrador de GuardedBox". Versión 1.0 (Versión 8.4.0 de GuardedBox). DinoSec.
https://www.dinosec.com/guardedbox/Manual_de_administrador_de_GuardedBox_v8.4.0.pdf

REF5 "Guía de Seguridad de las TIC. CCN-STIC 652A. Seguridad en contenedores". CCN-CERT. Julio 2020.
https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/5189-ccn-stic-652a-seguridad-en-contenedores/file.html

REF6 "Guía de Seguridad de las TIC. CCN-STIC 807. Criptología de empleo en el Esquema Nacional de Seguridad" (ENS). CCN-CERT. Mayo 2022.
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

REF7 "Docker Compose". Docker.
https://docs.docker.com/compose/

10.ANEXO: LISTADO DE FICHEROS DE CONFIGURACIÓN

206. El presente anexo incluye un listado con los ficheros referenciados a lo largo del presente documento que son utilizados para la configuración de la solución por parte de DinoSec (en colaboración con la organización), para cada instancia de GuardedBox y en cada despliegue concreto:

a) Dos ficheros ".tar" correspondientes a las imágenes de los dos contenedores Docker de la aplicación de la solución GuardedBox y de la base de datos.

b) Fichero de configuración principal de Docker: "docker-compose.yml".

c) Fichero de configuración y de propiedades principal del back-end: "application.properties".

d) Fichero de configuración y de propiedades principal del front-end: "front-properties.json".

e) Ficheros de configuración y de propiedades complementarios de GuardedBox (para un máximo de 13 ficheros adicionales):

- Formato de salida del sistema de *logging* de GuardedBox: "logback-access.xml" y "logback-root.xml".
- Dos logos personalizables: "custom-logo-[1|2].png".
- Mensajes o literales empleados por la solución para los diferentes idiomas soportados, por ejemplo, español ("es") e inglés ("en"):
  - Back-end: "back-lang-[es|en]-[1|2].properties".
  - Front-end: "front-lang-[es|en]-[1|2].json".
- Fichero con el certificado digital para HTTPS en formato PKCS#12: "server.p12".

f) Esquema de la base de datos: "guardedbox.sql".

11. ABREVIATURAS

2FA	*Two Factor Authentication*.
BD	Base de datos.
CA	*Certificate Authority.*
CPU	*Central Processing Unit.*
CCN	Centro Criptológico Nacional.
CSR	*Certificate Signing Request.*
DNS	*Domain Name Service.*
DNSSEC	*DNS Security Extensions.*
DoH	*DNS over HTTPS.*
DoT	*DNS over TLS.*
E2EE	*End to End Encryption.*
ENS	Esquema Nacional de Seguridad.
HA	*High Availability (alta disponibilidad).*
HMAC	*Hash-based Message Authentication Code.*
HTTP	*Hyper Text Transport Protocol.*
HTTPS	*Hyper Text Transport Protocol Secure.*
NTP	*Network Time Protocol.*
NTS	*Network Time Security.*
RAM	*Random Access Memory.*
SHA	*Secure Hash Algorithm.*
SMTP	*Simple Mail Transfer Protocol.*
SMTPS	*Simple Mail Transfer Protocol Secure.*
SO	Sistema Operativo.
SQL	*Structured Query Language.*
SRI	*SubResource Integrity.*

SSO	*Single Sign-On.*
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones.
STS (o HSTS)	*Strict Transport Security (o HTTP Strict Transport Security).*
TLS	*Transport Layer Security.*
VPN	*Virtual Private Network.*[6]

[6] El uso de VPNs hace referencia a la opción asociada a disponer de un acceso remoto por parte del personal técnico hacia el entorno en el que se encuentra el servidor sobre el que ejecuta GuardedBox.

PUBLICACIONES DE DEFENSA

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