centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1705

Procedimiento de Empleo Seguro
Sandas GRC

Octubre 2025

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-26-140-6

Fecha de Edición: Octubre de 2025

centro criptológico nacional

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.05.05 13:19:34 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1 INTRODUCCIÓN

1. SandaS GRC es la plataforma para el Gobierno de la Seguridad, Gestión del Riesgo y evaluación del Cumplimiento Normativo.
2. El motor de Gestión del Riesgo integrado en SandaS GRC permite el desarrollo de un proceso de Evaluación del Riesgo conforme a las mejores prácticas internacionales (ISO 27005, ISO 31000), respecto a distintos marcos normativos (ENS, ISO 27001, LOPDGDD, NIST SP 800-82, PCI-DSS, Privacidad Internacional, Compliance Penal, Marcos de Controles ad-hoc, …) y en distintos contextos de amenazas.
3. SandaS GRC es un software comercializado por defecto en modalidad Software como Servicio (SaaS), pudiendo comercializarse desplegando instancias en las instalaciones del cliente (on-premise).
4. Sandas GRC está basada, para la estrategia de mejora continua, en las cuatro fases del Ciclo de Deming, permitiendo su alineamiento con diversas metodologías y sistemas de gestión.
5. Permite integrar en un mismo proyecto una gestión multi-organización, permitiendo la evaluación y análisis de diferentes estructuras corporativas.
6. SandaS GRC puede integrarse con PILAR, INES y otras herramientas del CCN para facilitar el cumplimiento del Esquema Nacional de Seguridad.
7. Dispone de una amplia biblioteca de marcos normativos y catálogos de activos, amenazas y controles predefinidos, que aceleran la configuración del proyecto, permitiendo además definir, cargar y crear marcos propios o normas de seguridad ad-hoc.

2 OBJETO Y ALCANCE

8. Esta guía es de aplicación para la versión 6.20 de la plataforma SandaS GRC, alojada en el proveedor de servicios en la nube de Amazon Web Services (AWS) en región europea.
9. Se trata de una plataforma a la que se accede mediante un portal de seguridad, que gestiona el acceso de los usuarios al servicio.
10. El objetivo de este documento es servir como una guía para realizar el alta, una configuración inicial y la operación segura del producto Sandas GRC v.6.20.
11. 3.El servicio Sandas GRC en su versión 6.20 ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTA en la familia “Análisis y Gestión de Riesgos”.

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar en el alta del producto.

b) Apartado 5. En este apartado se recogen las recomendaciones para tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

c) Apartado 6. En este apartado se recogen las tareas recomendadas para la fase de operación y el mantenimiento del producto.

4 ALTA EN LA PLATAFORMA

4.1 REGISTRO Y LICENCIAS

12. El acceso a SandaS GRC se realiza a través del portal de seguridad https://cybersecurity.telefonica.com/gravity/login [REF1], que proporciona la autenticación y autorización a partir de las credenciales introducidas y validadas. Una vez el usuario se ha logado en el Portal podrá acceder al servicio de SandaS GRC.
13. El usuario deberá contar con una cuenta autorizada para acceder a SandaS GRC. El proceso de inscripción de SandaS GRC en muy similar a cualquier otro servicio digital. Si es la primera vez que accede a SandaS GRC, debe previamente realizar el proceso de registro. La gestión del alta de usuario se realiza por los administradores del portal de seguridad donde se ubica Sandas GRC.
14. En el momento en el que se formaliza la suscripción a SandaS GRC, el usuario recibe un correo electrónico con instrucciones para proceder al registro en el Portal de autenticación.
15. Una vez dado de alta el usuario, el administrador se pone en contacto con el usuario para informarle del alta y de que le llegará un correo con un enlace específico. Debe considerarse que el usuario dispone de un plazo de 72 horas para proceder al registro desde el momento que recibe este correo electrónico. Tras ese período el enlace expira y debe solicitarse uno nuevo a los administradores a través del buzón soporte-sandasgrc@govertis.com [REF2].

4.2 CONSIDERACIONES PREVIAS

16. El entorno de producción Sandas GRC se implementa en un Centro de Proceso de Datos alojado en una región europea de Amazon Web Services (AWS), y para su funcionamiento se despliega como mínimo utilizando la siguiente infraestructura, la cual es proporcionada por el fabricante al ser un servicio SaaS.

4.2.1 INSTANCIAS DE INTERFAZ DE USUARIO

17. Se despliega un mínimo de 2 instancias para alojar las máquinas front-end proporcionando redundancia y garantizar su resiliencia dentro de los parámetros de servicio.
18. Estas máquinas deben tener como mínimo las siguientes características:
    - Ubuntu 18.04.2 LTS como sistema operativo o posterior.
    - Arquitectura x86_64.
    - CPU de 4 núcleos.
    - Memoria RAM de 16GB.
    - Red: 10 Gigabit.
    - Disco SSD 64GB.
    - Disco HDD 100GB.
19. Por otro lado, deben tener instalado los siguientes servicios:
    - Servidor web/proxy inverso: NGINX o posterior.
    - Servidor de aplicaciones: Apache Tomcat 8 o posterior.

- Oracle Java JRE 1.8 o posterior.

4.2.2 INSTANCIAS DEL SISTEMA DE ARCHIVOS

20. Son necesarias para almacenar los documentos cargados por los usuarios.
21. Disponen de una capacidad mínima de 100GB, ampliable en función de las necesidades de los clientes, la contratación de espacio adicional o la demanda del servicio.

4.2.3 BALANCEADORES DE CARGA ELÁSTICOS

22. Equilibradores de alta disponibilidad.
23. Este balanceador se encarga de balancear la carga entre las dos máquinas para aumentar la tolerancia a fallos, evitar sobrecarga de recursos en una instancia y minimizar el tiempo de respuesta.
24. En el supuesto de que una de las instancias este inoperativa, la otra continuaría funcionando sin interrupción.

4.2.4 ALMACENAMIENTO DE BASES DE DATOS RELACIONALES

25. Instancia de base de datos.
    - Motor: PostgreSQL 10.6 o superior.
    - Tamaño de almacenamiento: 150 GB o superior.

5 FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

26. Los componentes funcionales de la Plataforma SandaS GRC están disponibles a través de una única interfaz. En la Ilustración 1, se muestra el esquema general de la Plataforma Sandas GRC. El usuario accede a través del portal de autenticación de manera unificada a todos los servicios.

27. Al tratarse de un servicio en la nube, no es necesario por parte del cliente realizar ninguna configuración segura.

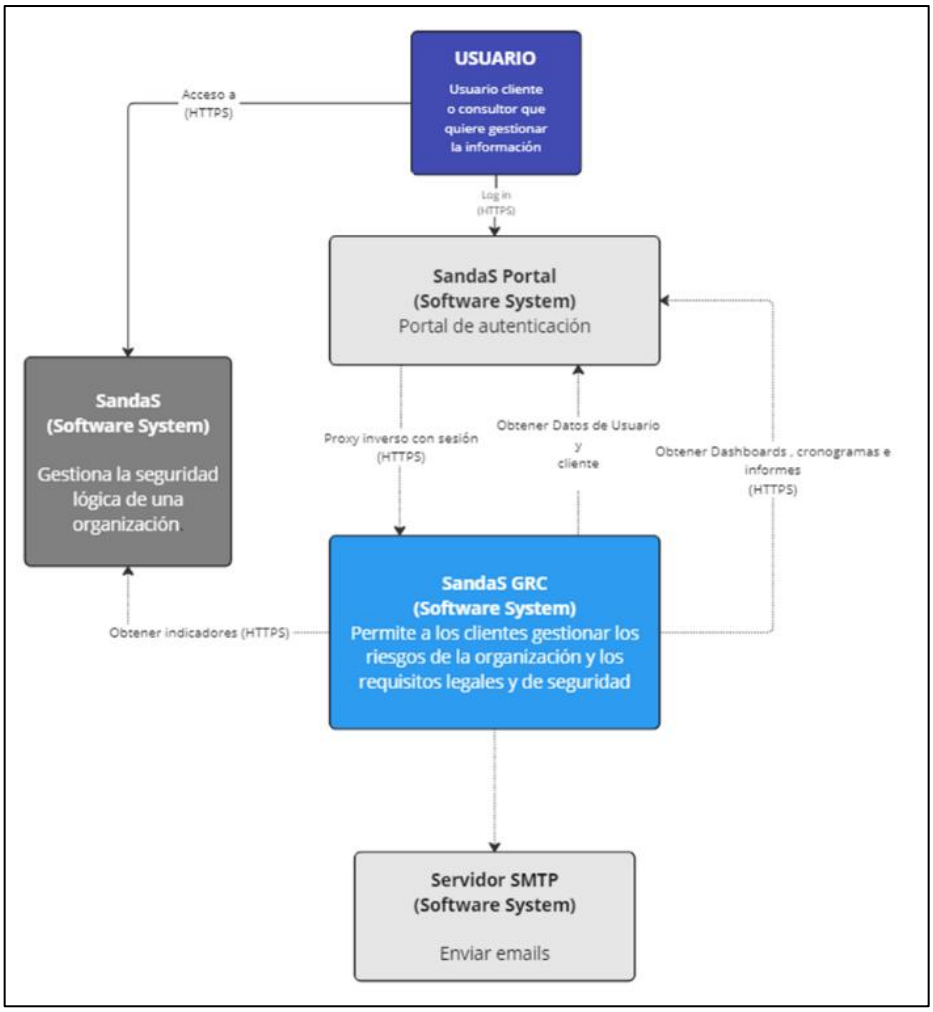

Ilustración 1. Arquitectura Sandas GRC

5.2 AUTENTICACIÓN

28. El acceso a la interfaz de SandaS GRC se realiza desde un navegador utilizando HTTPS.

29. El inicio de sesión en SandaS GRC requiere introducir el nombre de usuario y su contraseña como primer paso. Seguidamente deberá utilizar una herramienta multi-factor, que proporcionará un código de un solo uso (OTP – One-Time Password) para lograr el acceso, una vez validada la identidad del usuario mediante ese segundo factor de autenticación.

30. Si los datos introducidos son correctos se permitirá el acceso. Si estos resultaran incorrectos y se superase el máximo permitido (consultar el apartado 5.3.2 CONFIGURACIÓN DE USUARIOS) se bloquearía la cuenta.
31. La creación de usuarios e instancias se gestiona a través del Portal de Autenticación. Un usuario no puede darse de alta por sí mismo, debe realizarse por los administradores. Desde este portal también se gestiona el perfilado de permisos para el usuario o su asignación a roles predefinidos.
32. Si el usuario no accede en 3 meses queda bloqueado su acceso.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 PORTAL DE SEGURIDAD

33. Al tratarse de un servicio en la nube, la administración del producto se realiza a través del portal de seguridad, al que se accede de forma remota utilizando el protocolo seguro HTTPS, con TLSV1.2 o superior para crear un canal cifrado.
34. No están habilitados los protocolos TLS 1.1, TLS1.0, SSLv1 y SSLv2.

5.3.2 CONFIGURACIÓN DE USUARIOS

35. **Configuración de la política de contraseñas seguras**. La configuración de la política de contraseñas viene dado por defecto por las Directivas del portal de seguridad, por el cual se accede a SandaS GRC. Dicha configuración cumple los siguientes requisitos:
    - Longitud mínima de la contraseña: doce (12) caracteres.
    - Composición de la contraseña: la contraseña debe tener al menos una (1) minúscula, una (1) mayúscula, un (1) número y un (1) carácter del grupo (&!"#'() *+,-./:;<=>?@[]^{|}).
    - Número de contraseñas anteriores que no se permite utilizar: cinco (5).
    - Tiempo de validez hasta que expira una contraseña: noventa (90) días.
36. Adicionalmente se pueden configurar los métodos de doble configuración Authenticator y Latch.
37. **Configuración de los parámetros de sesión**. La configuración de los parámetros de sesión viene dado por las Directivas del propio portal de seguridad, por el cual se accede a SandaS GRC**.** Dicha configuración cumple los siguientes requisitos:
    - Tiempo de inactividad de las sesiones: cinco (5) minutos.
    - Número de intentos fallidos de inicio de sesión: tres (3) intentos.
38. Una vez que se ha intentado 3 veces, el usuario se bloquea y se solicita cambio de contraseña. Para ello, se envía un nuevo código de activación al correo del usuario para que pueda realizarse el cambio de contraseña. Sin este código no puede realizarse el cambio de contraseña y el usuario queda bloqueado.

5.3.3 CONFIGURACIÓN DE ADMINISTRADORES

39. El alta de un administrador solo puede realizarse por parte del equipo de Administración de SandaS GRC.

40. **Configuración de la Política segura de contraseñas**. Deberá cumplir con los siguientes requisitos mínimos:

    - Longitud mínima de la contraseña: doce (12) caracteres.
    - Composición de la contraseña: a contraseña debe tener al menos una minúscula, una mayúscula, un número y un carácter del grupo (&!"#'()*+,-./:;<=>?@[]^{|}).
    - Número de contraseñas anteriores que no se permite utilizar: cinco (5).
    - Tiempo de validez hasta que expira una contraseña: tres meses (90 días).

41. El usuario Superadministrador puede llevar a cabo las siguientes funciones:

    - Administración del producto de forma remota.

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

42. Todo el acceso al producto se realiza mediante el uso del puerto 443 (HTTPS). El resto de los puertos están cerrados.

5.5 SINCRONIZACIÓN HORARIA

43. Al tratarse de un servicio en la nube, las instancias donde está alojado el servicio se sincronizan mediante el uso de NTP.

5.6 ACTUALIZACIONES

44. El proveedor de servicios en la nube es el responsable de la actualización del software de infraestructura y se encarga de mantener sus sistemas actualizados sin la intervención del usuario.

45. El equipo de administración de SandaS GRC es responsable de actualizar el software de plataforma, incluyendo los servicios mínimos que debe tener instalados, detallados en el apartado 4.2 CONSIDERACIONES PREVIAS.

46. En SandaS GRC se realizan actualizaciones funcionales periódicas, en las que se añaden nuevas funcionalidades. Las actualizaciones pueden no afectar a todos los componentes y elementos de la plataforma.

47. Las actualizaciones son previamente comprobadas y ejecutas en un servidor de pruebas, réplica del que está en producción. Una vez comprobado que la funcionalidad es correcta y se ha validado el procedimiento de actualización, se realiza el pase a producción de los cambios incluidos.

5.7 ALTA DISPONIBILIDAD

48. El producto tiene por defecto alta disponibilidad, teniendo para ello dos instancias de interfaz y dos bases de datos replicadas, con un balanceador que permite en todo momento que se elija la instancia que atiende una petición, redirigiendo la carga hacia la instancia activa en caso de indisponibilidad, como se detalla en el apartado 4.2 CONSIDERACIONES PREVIAS.

5.8 AUDITORÍA

5.8.1 REGISTRO DE EVENTOS

49. Todos los accesos a la plataforma quedan registrados en los archivos de registro o logs.
50. Para su posterior consulta, el administrador puede acceder desde el menú "Configuración" al menú "Registro de accesos".
51. Adicionalmente, la plataforma conserva archivos log generados por el siguiente software:
    - Servidor Tomcat.
    - Servidor Apache.
    - Servidor NGINX.
    - Portal de autenticación.
52. Dichos archivos log complementan a los logs funcionales generados por SandaS GRC, que incluyen detalles de las operaciones realizadas en la plataforma por cada usuario, pudiendo ser consultados sólo por los administradores de SandaS GRC.

5.8.2 ALMACENAMIENTO

53. Al tratarse de un servicio en la nube, el almacenamiento es el proporcionado por el proveedor del servicio Cloud. Dicho almacenamiento se conserva cifrado empleando el algoritmo AES de 256 bits.
54. Los registros de acceso al sistema se almacenan en ficheros de log en las carpetas asociadas al diferente software de plataforma mencionado en el apartado previo.
55. El producto conserva los registros de auditoría en la propia base de datos. La información de auditoría se guarda en las condiciones y por el periodo establecido en la normativa de seguridad y revisión periódica de los registros.

5.9 BACKUP

56. El procedimiento de respaldo mantiene dos tecnologías (Almacenamiento en Ficheros y Base de datos) en las que generar copias de seguridad.
57. Se conservan 7 copias diarias, 5 semanales y 24 copias mensuales.

6 FASE DE OPERACIÓN

58. Durante la fase de operación los administradores de SandaS GRC disponen de diferentes procedimientos operativos para detectar y prevenir errores de funcionamiento y seguridad.

59. Para ello, se realiza de forma periódica como labores de gestión y mantenimiento:

    - Comprobaciones para asegurar que no se ha introducido ningún software no autorizado.
    - Comprobaciones de la configuración del software, para verificar que no se ha desconfigurado y que se mantienen, por tanto, las configuraciones seguras del software desplegado previamente autorizadas.
    - Monitorización del estado de los discos, RAM, procesos, CPU y otros parámetros de las instancias y el proveedor Cloud.
    - En cada cambio de versión, se actualizan los paquetes que incluyen la implementación de las mejoras funcionales y correctivas de los diferentes módulos.
    - En los procesos de actualización pueden aplicarse parches de seguridad del sistema operativo y otro software base.
    - Los registros de auditoría deben de estar protegidos de borrados y modificaciones no autorizadas. Solamente el personal de seguridad autorizado podrá acceder a ellos.

7 REFERENCAS

[REF1] Portal de seguridad
https://cybersecurity.telefonica.com/gravity/login

[REF2] Buzón de soporte técnico
soporte-sandasgrc@govertis.com

8 ABREVIATURAS

AES	Advanced Encryption Standard (Estándar de Cifrado Avanzado)
AWS	Amazon Web Services
CMBD	Configuration Management Data base (Sistema de gestión de Base de Datos)
CPSTIC	
CPD	Centro de Procesamiento de Datos
ENS	Esquema Nacional de Seguridad
GRC	Gobierno, Riesgo y Cumplimiento
HDD	Hard Disk Drive (Unidad de Disco Duro)
ISO	International Organization for Standardization
JRE	Java Runtime Environment (Entorno de Ejecución de Java)
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales
LTS	Long-Term Support (Soporte a Largo Plazo)
NGINX	(No es un acrónimo, pero es un servidor web/proxy inverso ampliamente utilizado)
NIST	National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología)
NTP	Network Time Protocol (Protocolo de Tiempo de Red)
OTP	One-Time Password
PCI-DSS	Payment Card Industry Data Security Standard (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago)
SaaS	Software as a Service (Software como Servicio)
SO	Sistema Operativo
SP	Special Publication (Publicación Especial)
SSD	Solid State Drive (Unidad de Estado Sólido)
SSH	Secure Shell
SSL	Secure Sockets Layer (Capa de Conexión Segura)
TLS	Transport Layer Security

PUBLICACIONES DE DEFENSA

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