centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1520

Procedimiento de Empleo Seguro
Galleon XSR/G1

Enero 2026

Edita:

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
2026.01.14 15:38:01 +01'00'

Fecha de Edición: Enero de 2026

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. Galleon XSR/G1 es un dispositivo de almacenamiento con interfaz Gigabit y 10GbE en una carcasa extremadamente pequeña. Está diseñado para soportar las condiciones ambientales más severas sin comprometer la funcionalidad y el rendimiento.
2. El diseño optimizado en términos de tamaño, peso y alimentación lo hace ideal para su uso en pequeños sistemas aéreos y terrestres no tripulados, así como en otras aplicaciones con restricciones de espacio y energía.
3. Puede ser equipado con hasta 40TB de almacenamiento con memoria NAND tipo celdas multinivel (MLC) de Grado Industrial o hasta 20TB de almacenamiento con memoria NAND de celda de un solo nivel (SLC) de Grado Militar. Al ser los módulos de datos extraíbles, permiten tiempos de ciclo muy cortos entre misiones y el transporte fácil de datos entre el vehículo o aeronave y la estación de mando o laboratorio donde se analizan o distribuyen los datos.

2 OBJETO Y ALCANCE

4. En la presente guía se indica el procedimiento de empleo seguro para la familia de productos Galleon XSR/G1 (servidor, NAS y grabador) y que ejecutan la versión 8.4 del sistema operativo Red Hat Enterprise Linux.

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a tener en cuenta antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se indican las recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto para lograr una configuración segura.

d) Apartado 7. En este apartado se recogen las referencias utilizadas en la presente guía de empleo seguro.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

5. Comprobar la documentación de envío para corroborar que fue enviado por el proveedor seleccionado ya sea mediante la verificación del código de envío/paquete como por algún medio de información de la empresa de transporte, por ejemplo, teléfono, fax o un servicio online de rastreo de paquetes.
6. En el momento de la recepción del producto, éste debe ser examinado para comprobar que no ha sido manipulado durante el proceso de envío y corresponde con el modelo Galleon XSR o G1.
7. En caso de identificarse alguna irregularidad durante la inspección, se deberá poner inmediatamente en conocimiento del proveedor para notificar y solucionar los problemas identificados.
8. Comprobar que el contenido del paquete contiene:
    a) Unidad principal.
    b) Cable de alimentación y señal (se deben pedir por separado).
    c) CD-ROM que contiene la documentación y el software.

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. El producto debe instalarse en una ubicación físicamente segura donde solo el personal técnico disponga de acceso y autorización para la instalación, configuración y mantenimiento del producto.

4.3 CONSIDERACIONES PREVIAS

10. Aunque el XSR/G1 es un dispositivo de bajo consumo, la refrigeración debe considerarse encarecidamente al instalar la unidad. El equipo está diseñado para permitir la refrigeración por conducción, por convección, o una combinación de ambas.
11. Para la refrigeración por conducción, el XSR/G1 debe montarse sobre una placa fría que garantice que la superficie de montaje del producto se mantiene por debajo de su temperatura máxima de funcionamiento.
12. Para la refrigeración por convección, la temperatura de funcionamiento del XSR/G1 depende de la temperatura ambiente y del caudal de aire disponible.
13. Se debe solicitar al proveedor que se suministre el disco de sistema con la protección contra escritura controlada por hardware. De esta manera el disco de sistema estará protegido contra escritura otorgando al producto de una integridad del disco de arranque.

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

14. Para la administración del producto de manera local se requiere la instalación de un puesto de gestión por consola.

15. Dicho puesto de trabajo se refiere a cualquier estación de trabajo que permita una conexión local con cable cruzado entre el producto y la estación de trabajo o una estación que se componga de una pantalla y un teclado que se conecten directamente al producto.

5 FASE DE INSTALACIÓN

16. Para la correcta instalación del equipo se deben seguir los pasos descritos en la sección 2 de la guía de instalación, incluida en la documentación suministrada con el producto.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

17. El sistema operativo del producto admite los siguientes protocolos de red: CIFS, NFS, FTP, TFTP, iSCSI, SSH, TLS y SNMP. Estos vienen por defecto activados y deben ser desactivados por un administrador mediante el uso de comandos estándar disponibles para RedHat 8.4.
18. Los administradores sólo deben acceder a la unidad y realizar actividades de gestión localmente y no de forma remota. Para la gestión local, el administrador puede utilizar un teclado, monitor y ratón conectado directamente mediante un sistema KVM o un cable cruzado que proporcione una conexión directa y local entre el producto y el computador del administrador para acceder al sistema operativo Red Hat.
19. En dicha configuración por defecto, SSH y SNMP están habilitados para la administración y monitorización remotas, SSH y TLS están habilitados para la autenticación, y CIFS y NFS están habilitados tras una autenticación correcta para el acceso remoto a archivos.
20. Para un modo de operación segura, los protocolos de administración remota y autenticación SSH, TLS y SNMP se deben deshabilitar, como *root*, mediante:

```
systemctl disable ssh
systemctl disable gec-key-server
systemctl disable snmpd
```

6.2 AUTENTICACIÓN

21. El producto gestiona credenciales locales, mediante usuario y contraseña. Dichas credenciales se almacenan en el producto.
22. Para la creación y gestión de usuarios locales, ver apartado 6.3.2 CONFIGURACIÓN DE ADMINISTRADORES.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

23. Aunque el producto permite ser administrado tanto de forma local como remota, no se recomienda la administración remota, salvo que sea estrictamente necesario. En el modo de operación seguro, la administración remota está deshabilitada al seguir los pasos de descritos en la sección 6.1 MODO DE OPERACIÓN SEGURO para deshabilitar dicho acceso remoto.
24. El acceso, por tanto, se realizará mediante el acceso directo al producto o accediendo localmente con cable cruzado entre el producto y el computador del administrador para acceder al sistema operativo Red Hat.
25. En el caso de que sea estrictamente necesaria la administración remota, se recomienda encarecidamente que el acceso a la red se limite a una red privada segregada o uso de VPN en todo momento.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

26. El producto se entrega con una cuenta de usuario por defecto (“galleon)” y una cuenta de usuario administrativo (root). Ambas cuentas se pueden utilizar para iniciar sesión en el sistema utilizando “galleon” como contraseña.

Contraseña Root:	*“galleon”*
Usuario:	*“galleon”*
Contraseña:	*“galleon”*

27. Por tanto, la primera vez que se introducen las credenciales del root se deben ejecutar los siguientes comandos para aplicar una configuración de la política segura de contraseñas:

- Insertar la siguiente línea en los ficheros `/etc/authselect/custom/password-policy/system-auth` y `/etc/authselect/custom/password-policy/password-auth` (después de la línea `pam_pwquality.so`):

```
password    requisite     pam_pwhistory.so remember=5
use_authtok
```

- Insertar o añadir la siguiente opción en la linea de pam_pwquality.so bajo la sección password en los archivos `/etc/authselect/custom/password-policy/system-auth` and `/etc/authselect/custom/password-policy/password-auth` files

```
enforce_for_root
```

- Modificar las opciones correspondientes en el archivo /etc/security/pwquality.conf:

```
minlen = 12
dcredit = -1
ucredit = -1
lcredit = -1
ocredit = 1
minclass = 3
maxrepeat = 2
```

- Configurar el archivo `/etc/login.defs` para que contenga:

```
PASS_MAX_DAYS 60
PASS_MIN_DAYS 10
```

- Modificar las opciones correspondientes en el archivo /etc/pam.d/password-auth:

```
deny=3
unlock_time=300
```

- Añadir la siguiente línea al archivo "`/etc/tmux.conf`":

```
set -g lock-after-time 300
```

28. Posteriormente a esta configuración se deberán modificar las credenciales por defecto mediante los comandos independientes para cada usuario:

```
sudo passwd root
sudo passwd galleon
```

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

29. Se deben deshabilitar las interfaces físicas que no se utilicen y los servicios inseguros descritos en la sección 6.1 MODO DE OPERACIÓN SEGURO.

30. Para comprobar que ninguno de estos servicios está habilitado, se puede ejecutar el siguiente comando que listará los servicios disponibles:

```
systemctl list-unit-files
```

6.5 OPERACIÓN SOBRE EL DISCO EXTRAÍBLE (RDM)

6.5.1 ADMINISTRADORES

31. Para el manejo del disco extraíble cifrado, ya sea uno nuevo o uno que se desee reformatear, se debe inicialmente ejecutar el comando:

```
rdm-initialize
```

32. Esto creará un sistema RAID a partir del RDM y posteriormente solicitará al administrador que ingrese una frase de contraseña (*passphrase*) para cifrar la partición RAID. A continuación, se creará el sistema de archivos en esta partición cifrada.

33. La frase de contraseña debe ser segura y tener una alta entropía para proteger los datos cifrados debiendo tener, al menos, 16 caracteres de longitud y generándose aleatoriamente a partir de una fuente de alta entropía a partir de un conjunto de posibles caracteres que incluyen letras mayúsculas, minúsculas, dígitos y caracteres especiales.

34. Este proceso será necesario cuando se realice un borrado criptográfico de la capa de cifrado de SW. En este caso, el RAID se mantendrá y el script `rdm-initialize` se encargará automáticamente de la gestión de estos cambios.

6.5.1.1 AUTENTICACIÓN: DESBLOQUEO DEL RDM

35. Para desbloquear un RDM cifrado existente y montar el sistema de archivos cifrado, se debe ejecutar:

```
rdm-mount
```

36. Esto pedirá al usuario que introduzca la contraseña que se utilizó para cifrar el RDM. Si se introduce correctamente, el RDM será desbloqueado y montado.

37. Si la contraseña se introduce incorrectamente 3 veces, no se permitirán más intentos de autenticación durante los siguientes 60 segundos.

6.5.1.2 DE-AUTENTICACIÓN: BLOQUEO DEL RDM.

38. Para bloquear un RDM encriptado y preparar el RDM para su extracción del sistema, el administrador debe ejecutar:

```
rdm-unmount
```

39. Esto detendrá los servicios que utilizan el RDM, intentará desmontar el sistema de ficheros, bloqueará la partición cifrada y detendrá el RAID. Una vez hecho esto, ya no será posible acceder a los datos del RDM si no es introduciendo de nuevo la contraseña para desbloquear la partición cifrada.

6.5.2 OPERADORES

40. Para el manejo del disco extraíble del producto, el operador debe acceder localmente a su sesión, mediante teclado y monitor conectados, ya que los accesos remotos están deshabilitados.

41. Una vez iniciada correctamente la sesión, se le solicitará inmediatamente al operador la frase de contraseña que desbloqueará y montará el disco RDM, y finalizará la sesión de inicio de sesión del operador.

42. Si la frase de contraseña se introduce incorrectamente 3 veces, no se permitirán más intentos de autenticación durante los siguientes 60 segundos.

43. Para el correcto bloqueo y preparación para su extracción del disco extraíble cifrado (RDM), se debe usar la instrucción

```
rdm-unmount
```

44. Dicha instrucción detendrá los servicios que usan el RDM, intentará desmontar el sistema de archivos, bloqueará la partición cifrada y detendrá el array RAID. Una vez ejecutado satisfactoriamente el proceso ya no será posible acceder a los datos en el RDM sin introducir nuevamente la frase de contraseña para desbloquear la partición cifrada.

45. Solo el administrador o un usuario delegado puede bloquear el RDM.

6.6 SERVIDORES DE AUTENTICACIÓN

46. Para una configuración segura del producto no se debe utilizar la autenticación a través de servidores externos, debiendo realizarse únicamente mediante la base de datos local de usuarios del sistema operativo.

6.7 SINCRONIZACIÓN

47. Se recomienda que el componente esté sincronizado con el resto de sistemas de la organización para permitir una alta fiabilidad en las actividades de auditoría forense.

48. La sincronización horaria del producto se debe hacer por medio de un servidor NTP externo, configurando el demonio que se encarga de la sincronización. Esta configuración se realizará mediante el acceso al dispositivo por CLI como usuario administrador y editar el archivo `/etc/chrony.conf`, indicando en el parámetro *server* la dirección del servidor NTP:

```
server <dirección IP del servidor NTP> iburst
```

49. A continuación, guardamos dicho archivo de configuración, salimos del editor y se reinicia el demonio mediante la instrucción:

```
systemctl restart chronyd.service
```

6.8 ACTUALIZACIONES

50. El fabricante Galleon notificará directamente a los clientes cuando estén disponibles los paquetes de actualización de software aplicables al producto.

51. Para instalar un paquete de actualización de software proporcionado por Galleon, se debe:

    - Conectarse al sistema a través puerto GbE 0 con la dirección IP predeterminada 192.168.100.101.
    - Copiar el archivo de actualización recibido desde fuera del componente:

```
scp gec-xsr-sw-update-1.0.tar galleon@192.168.100.101:/tmp
```

    - Iniciar sesión en el sistema como *root*.
    - Instalar la actualización:

```
gec-install-signed-update /tmp/gec-xsr-sw-update-1.0.tar
```

52. La actualización será validada automáticamente por la utilidad *gec-install-signed-update* preinstalada y no continuará si la firma digital incrustada en la actualización no puede ser verificada.

53. Nota: al tener desactivado el protocolo SSH, en este proceso concreto y de manera puntual se podría volver a activar brevemente para transferir el archivo de actualización al sistema, pero se recomienda utilizar un método alternativo para copiar el archivo en el sistema (p.ej. conexión local / CLI).

6.9 AUTO-CHEQUEOS

54. El producto tiene implementada una colección de los llamados chequeos automáticos integrados (BIT) que están clasificados dependiendo del momento en el que son ejecutados y su disparador.

55. Durante el proceso de arranque se ejecutarán los llamados S-BIT (*start-up BIT*), que analizarán el software, hardware y memoria de manera que se abortará el arranque en caso de que no sean satisfactorios.

56. Durante la operación habitual del producto, se ejecutarán periódicamente los llamados C-BIT (*Continuous BITs*) mientras el sistema esté activo. Y los llamados I-BIT (*Initiated BITs*) son aquellos que se ejecutarán bajo petición de un agente externo, ya sea un operador o una aplicación externa que los invoque.

6.10 AUDITORÍA

6.10.1 REGISTRO DE EVENTOS

57. Al tener el producto el sistema operativo Red Hat Enterprise Linux, toda la gestión del registro de eventos recae sobre el propio sistema operativo, registrando éste todos los

eventos relativos a las actividades de administración y gestión del dispositivo y las actividades del propio sistema.

58. Para una descripción detallada de la gestión de los registros, se debe consultar la documentación oficial del sistema operativo [REF1]

6.10.2 ALMACENAMIENTO LOCAL O REMOTO

59. El producto permite la configuración del almacenamiento de los registros de manera local o de manera remota, ambas basadas en el protocolo syslog integrado.

60. La aplicación Rsyslog, en combinación con el servicio *systemd-journald*, proporciona el soporte necesario para realizar el registro local y/o remoto en Red Hat Enterprise Linux.

61. Para la correcta configuración en ambos casos, se debe consultar la documentación oficial al respecto del sistema operativo [REF2REF1]

6.11 BACKUP

62. Se recomienda realizar copias de seguridad periódicas del sistema operativo del producto para poder recuperar y restaurar el sistema en caso de fallo u otra necesidad (p.ej. migración)

63. Para realizar la copia de seguridad o restaurar el sistema utilizando una copia de seguridad existente, Red Hat Enterprise Linux proporciona la utilidad *Relax-and-Recover* (ReaR).

64. El detalle de configuración de la función *ReaR* se puede consultar en la guía Red Hat Enterprise Linux [REF2]

65. Se recomienda siempre almacenar las copias de seguridad en una ubicación externa para mayor seguridad.

7 REFERENCIAS

[REF1] Red Hat Enterprise Linux 8. Configuring logging.
https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html-single/configuring_basic_system_settings/index#configuring-logging_configuring-basic-system-settings

[REF2] Red Hat Enterprise Linux 8. Setting up Rear
https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/assembly_recovering-and-restoring-a-system_configuring-basic-system-settings#proc_setting-up-rear_assembly_recovering-and-restoring-a-system

8 ABREVIATURAS

BIT	*Built-In Test*
C-BIT	*Continuous Built-In Test*
CIFS	*Common Internet File System*
CLI	*Command Line Interface*
CRL	*Certificate Revocation List*
ENS	*Esquema Nacional de Seguridad*
FTP	*File Transfer Protocol*
GbE	*Gigabit Ethernet*
I-BIT	*Initiated Built-In Test*
iSCSI	*Internet Small Computer System Interface*
MLC	*Multi-Level Cell*
NAS	*Network-Attached Storage*
NAND	*Not AND*
NFS	*Network File System*
NTP	*Network Time Protocol*
OCSP	*Online Certificate Status Protocol*
RAID	*Redundant Array of Independent Disks*
RDM	*Removable Data Module*
ReaR	*Relax-and-Recover*
S-BIT	*Start-Up Built-In Test*
SLC	*Single-Level Cell*
SNMP	*Simple Network Monitoring Protocol*
SSH	*Secure Shell*
TFTP	*Trivial File Transfer Protocol*
TLS	*Transport Layer Security*
XSR	*Extended Storage Recorder*