Guía de Seguridad de las TIC
CCN-STIC 1215

Procedimiento de empleo seguro
GLORIA

Julio de 2022

MINISTERIO DE DEFENSA

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

Centro Criptológico Nacional, 2022
NIPO: 083-22-125-1

Fecha de Edición: julio de 2022

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. **GLORIA** (**G**estor de **LO**gs para **R**esponder ante **I**ncidentes y **A**menazas) es una plataforma para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos. Basada en los sistemas SIEM (*Security Information and Event Management*), va un paso más allá de las capacidades de monitorización, almacenamiento e interpretación de los datos relevantes.
2. Así, mediante técnicas de correlación compleja de varias fuentes de eventos o análisis de patrones para la identificación de anomalías, permite una orientación muy flexible hacia la vigilancia del mundo IP.
3. La plataforma permite las siguientes funcionalidades a través de distintos módulos:
    a) **Monitorización de entornos tecnológicos (IT/OT)** y recolección de eventos de seguridad desde sistemas de detección de intrusos basados en red (NIDS) y en host (HIDS), sistemas automáticos de análisis de vulnerabilidades, analizadores de tráfico y conectores que permiten obtener los registros o logs de actividad de cualquier sistema o dispositivo del mundo IP.
    b) **Inteligencia**: técnicas de correlación compleja de eventos que sirve de base para el desarrollo y parametrización de los mismos.
    c) **Gestión del servicio**: consola única de gestión de alertas e incidentes que recoge todas las incidencias o alertas automáticas generadas por el sistema de correlación.
    d) **Automatización, orquestación y reducción de tiempos de respuesta**: para la mejora de las técnicas de correlación compleja de eventos se hace especialmente necesaria la integración de las capacidades de SIEM, la notificación de incidentes y la ciberinteligencia. De esta manera permiten la reducción del trabajo manual y repetitivo de los operadores/analistas de seguridad en los procesos de detección y respuesta a incidentes.
4. **GLORIA** se ha integrado con CARMEN, REYES y LUCIA para favorecer la detección, análisis e intercambio de incidentes.

2. OBJETO Y ALCANCE

5. El presente documento tiene como objetivo detallar las configuraciones de seguridad del producto **GLORIA 5.6.0**, de forma que la protección y funcionamiento del producto se realice de acuerdo con unas garantías mínimas de seguridad.

6. Los componentes de **GLORIA** se suministran en imágenes virtuales (.ova) preparadas para su despliegue sobre un hipervisor *VMWare ESXi*. Se resalta que **se debe utilizar un hipervisor VMWare ESXi con soporte de seguridad por parte del fabricante**[1]. Siendo los recursos recomendados para las máquinas virtuales los siguientes:

Máquina virtual	Requisitos básicos			
	vCPU	RAM	HD (S.O)	HD (datos)
ARGOS	4	6 GB	60 GB	
ARGOS-LogServer	8	8 GB	20 GB	
ARGOS-LogData1	8	16 GB	20 GB	750 GB
ARGOS-LogData2	8	16 GB	20 GB	750 GB
TRITON	8	16 GB	40 GB	
EMAS	4	6 GB	60 GB	

7. Estos componentes de **GLORIA** se ejecutan sobre el **sistema Operativo CentOS 7.9** y usa el siguientes *softwares* de terceros: Servidor de aplicaciones *Apache Tomcat*, Servidor de aplicaciones *Apache*, Gestor de colas *RabbitMQ*, Gestor de Base de datos *PostgreSQL*, Gestor de Documentos *ElasticSearch* y Máquina virtual Java 1.8.

8. **GLORIA ha sido cualificado e incluido en el Catálogo de Productos y Servicios de STIC en la familia. La versión evaluada y cualificada ha sido la 5.6.**

[1] A fecha de publicación de esta guía, mayo de 2022, ESXi 6.5 o superior.

3. ORGANIZACIÓN DEL DOCUMENTO

9. El presente documento se estructura en las secciones indicadas a continuación:

   a) **Apartado 4**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.

   b) **Apartado 5**. En este apartado se recogen las recomendaciones a 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 o mantenimiento del producto.

   d) **Apartado 7**. En este apartado se recoge la lista de elementos que deben revisarse.

   e) **Apartado 8**. Referencias.

   f) **Apartado 9.** Abreviaturas.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. Para la preparación de un nuevo despliegue de **GLORIA**, se solicita a la organización la información de direccionamiento final que va a tener el despliegue en su infraestructura y se realiza la instalación de cada componente y la paquetería actualizada en la plataforma de virtualización de S2 Grupo, generando una máquina virtual por cada componente.
11. Las imágenes virtuales de los componentes de **GLORIA** se exportan a ficheros OVA y se ponen a disposición del cliente en un repositorio privado de S2 Grupo, junto a las guías de administración y operación. En el repositorio también se ubicarán los ficheros de texto que indican el hash SHA256 de cada componente y de las guías de administración y operación.
12. Para garantizar que los elementos que se van a desplegar no han sido manipulados, cada componente tiene un nombre y unos ficheros de firma asociados. Adicionalmente, se configura una fecha de caducidad del enlace en el que el cliente solo tendrá permisos de descarga y lectura.
13. Una vez publicados, se comunica al cliente vía email la siguiente información relacionada con la descarga:
    - URL de descarga.
    - Contraseña de acceso.
    - Fecha de vigencia del enlace facilitado a partir de la cuál dejará de estar disponible la descarga.
    - Hash SHA256 de cada componente y los manuales de administración y operación.
14. La organización realizara la descarga directamente del repositorio del fabricante a través de una cuenta solo con permisos de lectura.
15. Antes de realizar el despliegue de cada componente, **se debe validar que el hash de cada imagen *ova* que se va a desplegar es correcto**. Tras compararlo con el hash indicado en el fichero *GLORIA_COMPONENTE_<X.Y.Z>.sha*, si todo es correcto, continua el proceso. **También se deberá comprobar el hash de los manuales**, para asegurar que los documentos no han recibido modificaciones durante el proceso de envío.

4.2 ENTORNO DE INSTALACIÓN SEGURO

16. El producto **debe ubicarse en un CPD, que cuente con las medidas de seguridad adecuadas a la información que procesa**, y que pueda establecer las conexiones necesarias para el desarrollo de su funcionalidad. El acceso debe estar restringido al personal autorizado para su gestión.

4.3 REGISTRO Y LICENCIAS

17. Los módulos se entregan preconfigurados desde S2 Grupo al cliente que lo adquiere. Se puede verificar que el material entregado se corresponde con el material publicado mediante la comprobación de los hashes de los ficheros, que quedan registrados en la plataforma EMAS de S2 Grupo, para poder ser verificados en cualquier instante, quedando así registro de versión y paquetería.

4.4 CONSIDERACIONES PREVIAS

18. Se recomienda facilitar a S2 Grupo la información de configuración de red (IP, direccionamiento, máscara de red, puerta de enlace). De esta forma, dicha información se parametrizará en el producto durante la instalación inicial. Se generará un certificado auto firmado para la IP/DOMINIO.
19. **Este certificado deberá ser sustituido en la instalación de la organización por el instalador de S2 Grupo, por uno autorizado y reconocido por la organizació**n.

4.5 INSTALACIÓN

20. La organización se encargará del despliegue inicial de la solución a partir de las imágenes virtuales descargadas del repositorio de ficheros del fabricante (S2 Grupo).
21. Se accede a la herramienta *vmWare vSphere Web Client* para realizar las tareas administrativas de creación del virtual *switch* para la comunicación de los componentes de **GLORIA**. El procedimiento a seguir es el siguiente:
    - Acceder a la opción *Hosts and clusters.*
    - Seleccionar el ESX donde se va a realizar el despliegue de **GLORIA** y con el botón derecho del ratón sobre el ESX seleccionado, seleccionar la opción *añadir red*.
    - Seleccionar la opción *grupo de puertos de máquina virtual para switch estándar*.
    - En la siguiente opción seleccionar la *creación de un nuevo switch*.
    - No es necesario seleccionar ningún adaptador porque va a ser de uso interno para las máquinas.
    - Se debe aceptar la advertencia.
    - Asignar un nombre que resulte después identificativo para el administrador del entorno de virtualización *Internal Gloria.*
    - Finalmente se muestra un resumen y seleccionar *Finalizar.*
22. En la propia herramienta *vmWare vSphere Web Client*, el proceso descrito a continuación se debe seguir para cada una de las imágenes a importar. El orden de importación e inicialización de las máquinas virtuales debe de ser el siguiente: *emas,*

triton, argos-logdata1, argos-logdata2, argos-logserver y *argos*. Las tareas a llevar a cabo son las siguientes:

- Acceder a la opción de *Hosts and clusters.*
- Seleccionar el *cluster* donde se desea desplegar la *.ova* mostrando el menú de acciones. Seleccionar la opción de despliegue de plantilla OVF.
- Se abre un asistente. Se debe seleccionar la imagen OVA del componente de gloria que se desee importar.
- Se muestran los detalles de la OVA, marcar *Siguiente*, pudiendo indicar una descripción personalizada si se considera adecuado.
- Seleccionar el directorio que se desee dentro del *cluster* en el que se despliega la máquina.
- Seleccionar el *datastore*.
- Para el siguiente paso, hay dos (2) posibilidades:
    - Máquina de *argos*, con dos (2) interfaces de red (una accesible desde la red del cliente y otra privada para la comunicación con el resto de componentes).
    - Resto de máquinas, con solo una interfaz de red por máquina (la privada).
- En *argos* debe haber dos (2) interfaces y se debe seleccionar la red de destino de cada interfaz, la primera interfaz será de uso interno entre la *suite*. Por lo que es necesario seleccionar la red interna creada anteriormente. La segunda interfaz es la que permite el acceso a la interfaz web de gestión por lo que su red de destino será la que permita acceder a la máquina.
- En el resto máquinas solo hay una interfaz de red, por lo que se configura solo la red de destino interna, ya que *argos* será la puerta de entrada al resto de componentes de la *suite*.
- Finalmente se muestra un resumen de las características de la máquina que se importa.
- Se debe esperar a que la máquina finalice el proceso de desplegarse.
- Por último, se debe arrancar la máquina.

23. Se deben repetir estas acciones para desplegar todas las imágenes OVA facilitadas por el fabricante.
24. Al realizar el despliegue de cada uno de los componentes (*argos*, *argos-logserver*, *argos-logdata*, *triton*, *emas*, *hera*), el instalador valida que el sistema se encuentra en la versión correcta ejecutando el siguiente comando:

    $ <componente>-version

25. Adicionalmente, para los componentes *argos, tritón, emas* y *hera*, el técnico se conecta a la interfaz web y accede al menú *ayuda > acerca de*, comprobando que, tras la actualización, la ventana de la aplicación web muestra la versión correcta.

26. Para comprobar la versión del producto, se puede ejecutar el siguiente comando en el componente de argos:

    $ gloria-version

27. Una vez desplegadas las máquinas virtuales, se puede comprobar el acceso a la plataforma a través de la URL del dominio reservado para **GLORIA**. Se mostrará la interfaz de acceso a la herramienta, con los enlaces a los diferentes componentes:

Ilustración 1. Interfaz de acceso de GLORIA

5. FASE DE CONFIGURACIÓN

5.1 AUTENTICACIÓN

28. El acceso a la interfaz gráfica de GLORIA se realiza desde un navegador utilizando **HTTPS sobre TLSv1.2** y está controlado mediante el uso de una pareja de valores usuario y contraseña. Todo usuario que interactúe con el sistema debe haber sido **dado de alta previamente** por un usuario con permisos de administración.
29. El inicio de sesión en GLORIA requiere introducir el nombre de usuario y su contraseña de acceso con el fin de validar la identidad de la persona que desea autenticarse en el sistema.
30. Si estos datos son incorrectos, GLORIA notificará el motivo del rechazo e invitará al usuario a introducir los datos nuevamente; si, por el contrario, son correctos, se autorizará el acceso.
31. Estas credenciales se almacenan en la base de datos local cifradas mediante un algoritmo hash. Este algoritmo no es configurable por parte del usuario.
32. Las claves de los componentes internos que requieren autenticación (BBDD, gestor de colas…) por defecto están almacenadas en el sistema de ficheros y protegidas por el sistema operativo en el que se ejecuta GLORIA.
33. **Se recomienda utilizar el acceso por SSH con el usuario configurador del SO para la configuración del producto**. Dicho acceso se realiza también mediante usuario/contraseña. El usuario *root* (superusuario) del sistema operativo no puede acceder vía SSH directamente, lo hará escalando desde un usuario sin privilegios.
34. Las claves de SSH se generan en el momento de la instalación y son únicas para cada instalación.

5.2 ADMINISTRACIÓN DEL PRODUCTO

5.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

35. Se utilizará la interfaz web para la operación del producto y para algunas labores de configuración, como los usuario y roles. La conexión a esta interfaz se realiza mediante HTTPS sobre TLSv1.2 por defecto.
36. Es desde la interfaz web del componente *emas* dónde se gestionan los usuarios de GLORIA y sus roles. Los roles permiten/ocultan las pantallas a las que puede acceder un usuario.
37. Se utilizará la interfaz CLI accesible desde SSH para configurar parámetros como la información de red o las comunicaciones del producto. Esta conexión se realiza mediante SSHv2 por defecto. Para este acceso se dispone de los usuarios *admin* y *root* del Sistema Operativo.
38. Las restricciones de acceso remoto (SSH o HTTPS) quedan delegadas en la seguridad de redes de la organización.

39. Tan solo se puede acceder al producto remotamente mediante HTTPS o SSH. No existe otro tipo de acceso no seguro como HTTP, Telnet, etc.

5.2.2 CONFIGURACIÓN DE ADMINISTRADORES

40. La aplicación web de GLORIA, en su componente *emas*, que es el encargado de la autenticación y autorización de la herramienta, dispone de un conjunto de roles predefinidos que no es posible eliminar, pero sí es posible configurar.
41. En la base de datos de *emas* hay creado un usuario administrador por defecto a partir del cual se podrá realizar la configuración del sistema.
42. **Se debe modificar la contraseña de administrador al acceder por primera vez**, siguiendo la política de contraseñas establecida en el apartado 5.2.3 POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN. Para ello, acceder a la pantalla de cambio de contraseña en el menú *Parametrización/Contraseña*
43. En función del rol asignado al usuario, éste dispondrá de diferentes capacidades. A continuación, se describen las funciones disponibles para cada rol de la interfaz web configurados por defecto:
    - **Administrador**: Rol con permisos totales sobre EMAS y HERA.
    - **Técnico**: Rol de acceso standard. Su visibilidad depende de cómo sea configurado en *EMAS*.
    - **Solo Lectura**: Rol de acceso que no puede realizar modificaciones sobre ninguna entidad.
    - **Dirección N3 y N4**: Rol que permite la configuración de las notificaciones con un mayor nivel y gestionar los canales.
    - **Visor de identificadores**: Rol que permite visualizar los identificadores de las entidades, ocultos por defecto.
    - **Acceso Tritón**: Rol que habilita el acceso al componente *TRITON*.
    - **Acceso Argos**: Rol que habilita el acceso al componente *ARGOS*.
    - **Acceso Hera**: Rol que permite el acceso al componente *HERA*.
44. Los roles de acceso *TRITON*, acceso *ARGOS* y acceso *HERA* proporcionan acceso a cada uno de esos componentes y una vez dentro del componente, dan acceso a todas sus pantallas, por lo que no existe una gestión específica de pantallas en esos componentes. Se considera que un usuario que accede al componente accede a toda su funcionalidad sin restricción.
45. Sin embargo, en el componente *emas* sí se dispone de una gestión de visibilidad más detallada, puesto que aquí es donde se administran los usuarios. En este caso, el rol de visor de identificadores es especial y lo que ofrece no es acceso a pantallas, sino que permite visualizar el identificador de las entidades (personas, nodos ebs, proyectos...). El rol de administrador tiene por defecto todos los permisos sobre todas las pantallas del componente *emas*. El resto de roles que permiten acceso a

emas, no tienen casi ningún permiso por defecto y es un usuario Administrador el que puede asignárselos.

46. El detalle sobre la creación y modificación de usuarios y roles, se puede consultar en los apartados *Usuarios y roles* y *Gestión de personal* de la *Guía de administrador del producto* – REF1.
47. En el caso en que la autenticación esté configurada para realizarse a través de la base de datos, un usuario puede cambiar su contraseña si lo desea accediendo a la pantalla de cambio de contraseña en el menú *Parametrización/Contraseña*.
48. Se deberá introducir la contraseña actual del usuario, y la nueva contraseña, esta última por duplicado para mayor seguridad.

5.2.3 POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN

49. El producto permite definir el tiempo de inactividad de las sesiones, tras el cual será necesario reautenticarse. Este tiempo se define de forma individual para cada usuario, durante la creación de estos, utilizando el parámetro *TimeOut*. Por defecto está establecido en 30 minutos, **se debe modificar y configurar un tiempo de 5 minutos**.
50. Para generar contraseñas de los usuarios de la interfaz web y la interfaz de gestión, el producto fuerza la siguiente política de seguridad (no modificable):
    - Debe de tener entre 8 y 64 caracteres.
    - Contener una letra, un número y alguno de los símbolos !@#$%^-_.
    - La contraseña nueva y la repetición de contraseña deben ser iguales.
51. Sin embargo, **el administrador deberá exigir los siguientes requisitos en las contraseñas de los usuarios**:
    - Longitud mínima: 12 caracteres.
    - Exigir el uso de, al menos: una letra minúscula, una letra mayúscula, un número y un símbolo.
    - Cambiar las contraseñas cada 60 días. Impedir un nuevo cambio hasta pasados 10 días.
    - No reutilizar las últimas 5 contraseñas.
52. Desde la interfaz de *EMAS* se puede acceder al menú *Configuración/Configuración Global* y a su pestaña *Valores por defecto* para cambiar la configuración de bloqueo de usuarios y de caducidad de contraseña.
53. El *Bloqueo usuarios inactivos* permite establecer si se bloquean automáticamente los usuarios que no han entrado en *emas* pasado cierto tiempo:

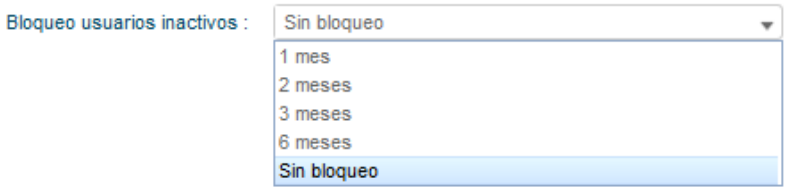

Ilustración 2. Bloqueo de usuarios

54. Si se selecciona *Sin bloqueo*, las cuentas no caducan, mientras que si se selecciona alguna de las otras opciones las cuentas caducarán pasado ese tiempo. Los usuarios no bloqueados no podrán entrar en el sistema a no ser que sean desbloqueados por el administrador en la pestaña de control de acceso de la gestión de personas.

55. El desplegable de caducidad de contraseñas permite establecer si los usuarios tienen que renovar la contraseña obligatoriamente pasado el tiempo seleccionado, en su siguiente acceso al sistema. **Se debe seleccionar un valor de dos meses**:

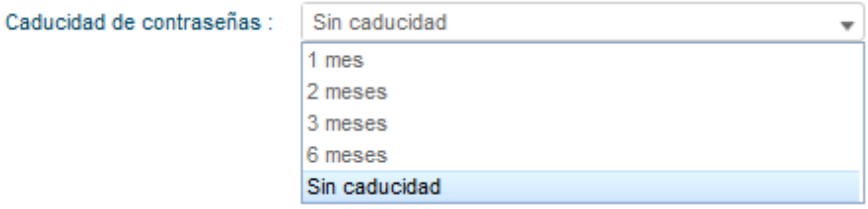

Ilustración 3. Caducidad de contraseñas

5.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

56. Los únicos puertos (y servicios) abiertos son HTTPS, SSH y, si se configura, recepción de tráfico por *syslog*. El resto de los servicios/puertos son de uso interno y no se exponen.

5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

57. El acceso a GUI mediante HTTPS está configurado con un certificado firmado por una CA autofirmada en el módulo de *argos*. **Se deberá actualizar por uno firmado por un CA válida y reconocida por el organismo, para ello se deberá informar al configurador de S2Grupo**.

58. El producto utiliza por defecto el protocolo TLS versión 1.2 o superior. La configuración de dicho protocolo corresponde al servicio web de cada componente.

59. El producto utiliza por defecto el protocolo SSHv2. La configuración de dicho protocolo corresponde al Sistema Operativo de cada componente.

5.5 GESTIÓN DE CERTIFICADOS

60. **La organización deberá proporcionar a S2Grupo el certificado digital, así como las claves de la entidad certificado raíz asociadas**, quedando este configurado en la preparación de las máquinas virtuales para la entrega inicial.

61. El configurador del sistema seguirá los siguientes pasos para su configuración:

    - Copiar el fichero de certificado a utilizar en GLORIA (el fichero denominado de ahora en adelante *gloria.crt*) a la ruta */etc/pki/tls/certs/gloria.crt* a través de SSH/SCP. El fichero de certificado no debe tener clave de apertura.
    - Copiar el fichero de clave privada del certificado a utilizar en GLORIA (el fichero denominado de ahora en adelante *gloria.key*) a la ruta */etc/pki/tls/certs/gloria.key* a través de SSH/SCP.
    - Copiar el fichero de claves públicas de la entidad certificadora y sus entidades de certificación intermedias, que firman el certificado anterior a utilizar en GLORIA (el fichero denominado de ahora en adelante *ca.crt*) a la ruta */etc/pki/tls/certs/gloria.crt* a través de SSH/SCP. El fichero de certificado no debe tener clave de apertura.
    - Editar el archivo */etc/httpd/conf.d/100-argos.conf* mediante vi;
        - Modificar la línea que comienza por *SSLCertificateFile* de forma que quede así:

          ```
          SSLCertificateFile /etc/pki/tls/certs/gloria.crt
          ```

        - Modificar la línea que comienza por *SSLCertificateKeyFile* para que quede así:

          ```
          SSLCertificateKeyFile /etc/pki/tls/private/gloria.key
          ```

        - Agregar tras la línea anterior la línea indicada a continuación:

          ```
          SSLCertificateChainFile /etc/pki/tls/certs/ca.crt
          ```

5.6 SINCRONIZACIÓN HORARIA

62. **Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados** para permitir una alta fiabilidad en los sistemas de auditoría y *logging*.

63. El producto hace uso del servicio NTP del Sistema Operativo (*CentOS 7*). Para la configuración del servicio de sincronización horaria (NTP), se deben realizar las siguientes acciones:

    - *$vi /etc/ntp.conf*
    - Añadir/modificar: *server <IP_SERVER_NTP> iburst*
    - *systemctl restart ntpd* [Arrancar servicio]

5.7 ACTUALIZACIONES

64. Un técnico de S2 Grupo es quien realiza la actualización de GLORIA, para ello obtiene la versión a instalar del sistema de registro y configuración para realizar la intervención en las instalaciones del cliente, física o remotamente.
65. La actualización es modular y una liberación de versión no tiene por qué afectar a todos los componentes y puede contener solo uno o varios componentes, teniendo cada componente su fichero de actualización independiente.
66. El paquete de actualización se denomina *GLORIA_COMPONENTE_<X.Y.Z>.tar.gz*, siendo <X.Y.Z> valores numéricos que permiten identificar de forma unívoca la versión de GLORIA que va a ser actualizada. Este fichero incluye el ejecutable *update.sh* junto con todos los elementos que se van a actualizar, ya sea paquetería o funcionalidad.
67. Antes de realizar la actualización de cada componente, el técnico de S2 Grupo **debe validar que el hash SHA-256** del paquete que va a instalar corresponde con el que se ha indicado en el gestor de eventos de S2 Grupo, comprobando de este modo que no se ha realizado ninguna modificación del paquete.
68. Tras asegurarse de que todo es correcto, realiza la actualización ejecutando el comando *update.sh*.
69. Tras ejecutar la actualización individualmente en cada uno de los componentes (*argos, argos-logserver, argos-logdata, tritón, emas, hera*), el técnico de S2 Grupo valida que el sistema se encuentra en la versión correcta ejecutando el siguiente comando:

    $ <componente>-version

70. Adicionalmente, para los componentes *argos, tritón, emas* y *hera*, el técnico se conecta a la interfaz web y accede al menú ayuda, opción *'acerca de'*, comprobando que, tras la actualización, la ventana de la aplicación web muestra la versión correcta.
71. Para comprobar la versión del producto, se puede ejecutar el siguiente comando en el componente de argos:

    $ gloria-version

5.8 SNMP

72. No se habilita el servicio SNMP en los componentes de **GLORIA**.

5.9 ALTA DISPONIBILIDAD

73. El producto dispone por defecto de alta disponibilidad en los datos mediante la réplica de la información en dos discos. No obstante, se delega en el motor de virtualización del cliente la capacidad de alta disponibilidad ante errores de apagado o sufrimiento de alguna otra avería.

5.10 AUDITORÍA

5.10.1 REGISTRO DE EVENTOS

74. Todos los accesos al producto mediante la interfaz se registran en ficheros de log para su posterior consulta.

75. GLORIA genera registros de auditoría para todos los eventos relevantes relacionados con la seguridad. Estos incluyen la fecha y la hora del evento, el tipo de evento, el sujeto que genera el registro de autoría y el resultado del evento: exitoso (valor 1) o fallido (valor 0). Se pueden consultar desde el menú *Gestión/Consulta logs seguridad.*

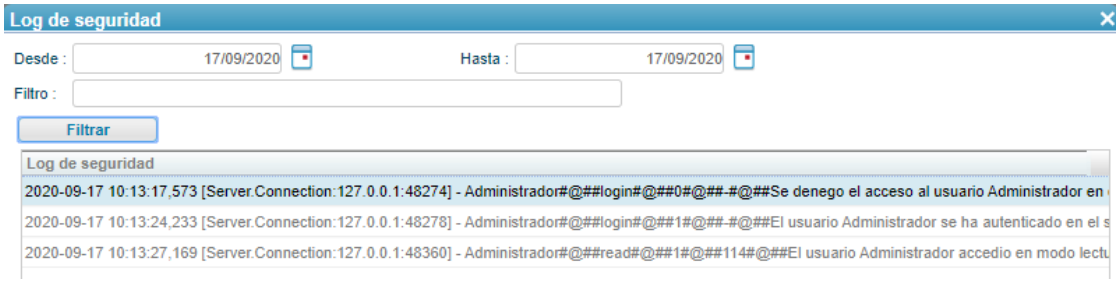

Ilustración 4. Consulta de logs de seguridad

76. Adicionalmente, en un inicio de sesión satisfactorio, se registra el identificador de sesión (entre paréntesis) y componente al que se accede:

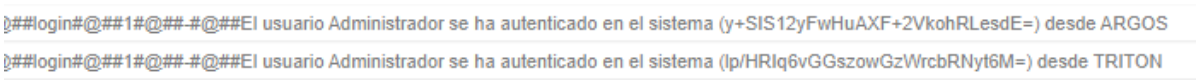

Ilustración 5. Logs de inicio de sesión

77. Y en un acceso a una alerta se registra el identificador de la misma:

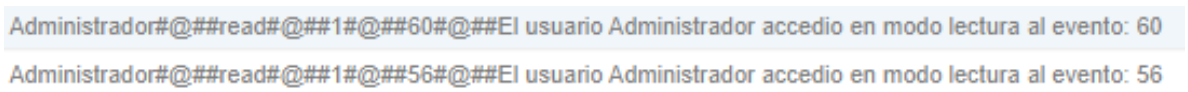

Ilustración 6. Generación de alertas

78. GLORIA registra la información de auditoría de forma legible y permitiendo únicamente su consulta a usuarios con el rol administrador. Con protección de los registros de auditoría almacenados, frente a modificaciones y eliminaciones.

5.10.2 ALMACENAMIENTO LOCAL

79. Los registros de acceso al sistema se almacenan en ficheros de log en diferentes rutas según el servicio. Estos logs rotan periódicamente para garantizar que la máquina no se quede sin espacio.

80. Por defecto, los logs de auditoría tienen un tamaño de 20 Mb y se mantienen un total de 5 logs (100Mb de log en total). Esta configuración solo puede ser modificada por un usuario configurador con acceso a la máquina (*root*), en ningún caso, por los usuarios (administradores o no) de GLORIA.

5.10.3 ALMACENAMIENTO REMOTO

81. El servidor permite enviar los registros de alerta (y sólo esos) a un servicio remoto vía correo electrónico o sms, si así se configura.
82. La configuración de estos servicios ha de realizarse por un usuario configurador de la máquina (acceso *root*). El detalle se puede consultar en el apartado *El sistema de notificaciones* de la *Guía de administrador del producto* – REF1.

5.11 BACKUP

83. No existe un método de *backup* de la máquina. Al tratarse de máquinas virtuales, **se recomienda realizar una copia del** estado **de las diferentes máquinas virtuales de forma periódica y almacenarlo en una ubicación segura**.

5.12 SERVICIOS DE SEGURIDAD

84. GLORIA es una plataforma para la gestión de incidentes y amenazas de ciberseguridad mediante la generación de alertas cuando encuentra patrones en los logs que almacena.
85. Mediante las reglas de correlación compleja, GLORIA detecta los posibles escenarios de ataque y los notifica en tiempo real, tanto a los analistas que puedan estar subscritos como a la consola de administración, para que las personas cualificadas puedan actuar en consecuencia.
86. GLORIA almacena logs de muchas fuentes diferentes mediante la recepción por syslog de multitud de dispositivos. Debido a la diversidad de estos logs, la configuración de estos registros la realiza un equipo especializado que analiza los logs de entrada y verifica el correcto funcionamiento de las reglas en los mismos.

6. FASE DE OPERACIÓN

87. Durante la fase de operación se pueden detectar y prevenir malfuncionamientos, para ello es recomendable realizar de forma periódica:

    - **Comprobaciones periódicas del *software* del producto** para comprobar que no se han introducido elementos no autorizados.
    - **Monitorización de argos**, que muestra información del estado de los discos, RAM, procesos y CPU.
    - En cada liberación de versión, **actualización de paquetería** que aplica las mejoras funcionales y correctivos de los módulos, así como los **parches de seguridad del sistema operativo base**.
    - Consulta al fabricante si existen **versiones nuevas del producto**.
    - Revisión periódica de los **registros de auditoría**.

7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Descarga del *firmware* y verificación de su integridad	☐	☐	
Instalación del *firmware* y registro de las licencias	☐	☐	
Cambio de contraseñas por defecto	☐	☐	
CONFIGURACIÓN			
ADMINISTRACIÓN DEL PRODUCTO			
Creación de usuarios y roles	☐	☐	
Configuración del bloqueo de usuarios	☐	☐	
Configuración de la caducidad de contraseñas	☐	☐	
SINCRONIZACIÓN			
Configuración de un servidor de hora NTP	☐	☐	
BACKUP			
Realización de copias y almacenamiento seguro de copias de *backup*.	☐	☐	
AUDITORÍA			
Configuración del envío de las alertas	☐	☐	
OPERACIÓN			
Comprobaciones periódicas del *software*	☐	☐	
Monitorización de argos	☐	☐	
Actualización de paquetes y parches de seguridad	☐	☐	
Despliegue de nuevas versiones	☐	☐	
Revisión de los registros de auditoría	☐	☐	

8. REFERENCIAS

REF1 Guía de administrador del producto

GLORIA_AGD_OPE_v5.6.0.pdf

Guía accesible tras adquirir el producto, desde el repositorio de distribución del fabricante.

REF2 CCN-STIC-807 Criptología de empleo en el ENS

9. ABREVIATURAS

CPD	Centro de Procesamiento de Datos
ENS	Esquema Nacional de Seguridad.
GUI	Interfaz gráfica de usuario
IT	Tecnologías de la Información
OT	Tecnologías de la Operación
SIEM	*Security Information and Event Management*
SO	Sistema Operativo
SSH	*Secure SHell*
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