Servicio de Informática y Comunicaciones
Universidad de Sevilla

CUSTODIA DEL CERTIFICADO Y MEDIDAS DE SEGURIDAD EN EL SERVIDOR

En relación a la manipulación de los certificados de servidor, así como las claves asociadas, el usuario debe tener en cuenta lo siguiente:

- La clave privada sólo debe mantenerse en los servidores donde se vaya a instalar el certificado.
- Los certificados no deben instalarse nunca en servidores de desarrollo o equipos personales, ni en ningún equipo ajeno a la Universidad de Sevilla, a menos que se hayan solicitado expresamente con ese fin.
- No se recomienda realizar copias de seguridad en dispositivos portátiles como pendrives.
- Las claves no deben transferirse nunca por medios no cifrados.
- Las claves sólo deben ser manipuladas por el personal expresamente autorizado para ello.
- En caso de que la clave se vea comprometida o en caso de pérdida de la misma, se debe notificar al SIC para que proceda a la revocación del certificado.

En relación a la configuración segura del servidor el usuario se compromete a:

- Cambiar las credenciales que vengan por defecto.
- Aplicar la política de contraseñas de la US, con restricciones de la clave, cambios periódicos, bloqueo ante intentos de acceso reiterados, etc.
- Evitar guardar credenciales en ficheros de texto plano. Toda la información confidencial, incluidas las credenciales, debería de ser cifrada y solo accesible para los usuarios que estrictamente lo requieran.
- Ser lo más restrictivo posible a la hora de otorgar privilegios a las cuentas de usuarios.
- Eliminar todo aquel servicio o funcionalidad que no sea estrictamente necesario para la prestación el servicio.
- Comprobar la integridad de todo el software que sea necesario instalar.
- Mantener actualizado el firmware, el software y las aplicaciones, instalando los parches de seguridad a la mayor brevedad posible.
- Modificar los mensajes de error para que no proporcionen información sobre los sistemas y aplicaciones.
- Sincronizar las fechas y horas de todos los sistemas/dispositivos.
- Seguir una política de creación, revisión y almacenamiento de logs. Monitorizar y registrar los incidentes.
- Utilizar, en la medida de lo posible, protocolos que cifren las comunicaciones, como SSH, HTTPS, SFTP, etc. evitando el envío de información en texto claro. Evitar el uso de algoritmos de cifrado débiles.
- Controlar los accesos remotos y locales.
- Utilizar antivirus y cortafuegos para proteger el servidor y los servicios.
- Establecer un procedimiento de copias de seguridad periódicas.

- Registrar los posibles tratamientos de información de datos personales y aplicarles las medidas de seguridad que les correspondan.
- Revisar la documentación al menos una vez al año para mantenerla actualizada.