Documentación disponible bajo confidencialidad

Los tres niveles de documentación, qué se facilita en sesión de evaluación y el procedimiento: solicitud, acuerdo de confidencialidad, sesión supervisada sin copias y registro en bitácora.

Tres niveles de documentación

La documentación del producto se clasifica en tres niveles. Esta clasificación es pública: clasifica sin revelar.

Documentación pública

Puede circular sin trámite adicional. Comprende la identidad y la ficha del producto, la arquitectura a nivel de diseño, el inventario de algoritmos con su estado frente a esquemas, la existencia de cada mecanismo de protección, los datos titulares de la evidencia —identificador, fecha, metodología y resultados— y las llaves **públicas** de verificación. Esta biblioteca forma parte de ese nivel.

Documentación bajo confidencialidad, en evaluación

Se muestra o se facilita al evaluador acreditado durante una evaluación, bajo acuerdo de confidencialidad, y no circula fuera de ella. Comprende el detalle cuya divulgación abierta degradaría una protección concreta o expondría la instancia en operación.

Material que, por diseño, no existe en documentos

Hay material que no puede entregarse ni siquiera bajo acuerdo de confidencialidad, **porque el sistema está construido para que no exista fuera de su sitio**: los fragmentos de custodia y las llaves protegidas, los sobres sin abrir, los códigos impresos de ceremonia y las llaves privadas de los autenticadores de cada custodio. Los fragmentos jamás se almacenan —solo se conservan metadatos y huella—, la llave reconstruida vive solo durante la ceremonia, los códigos impresos residen en el sistema únicamente como huellas unidireccionales y la llave privada de una llave de acceso nunca sale del autenticador de su titular. Ningún acuerdo puede prometer entregar lo que el sistema no guarda.

Qué se facilita en sesión de evaluación

Bajo confidencialidad, y solo por su título genérico, puede facilitarse:

- El diseño completo del Protocolo de Custodia de Llaves.
- Los informes íntegros de validación y de auditoría de seguridad.
- Los parámetros operativos de ceremonia y de supervisión de custodia.
- El código fuente, examinado en sesión o mediante depósito contractual en custodia de terceros.
- El detalle de laboratorio de la verificación de recuperación a un punto en el tiempo.

Procedimiento de facilitación

1. **Solicitud.** La institución o el evaluador solicita el acceso identificando el material por su título.
2. **Acuerdo de confidencialidad.** El acceso exige el acuerdo de confidencialidad suscrito por el evaluador acreditado que va a examinar el material.
3. **Sesión supervisada.** La facilitación se realiza en sesión de evaluación, presencial o remota supervisada, con acceso de lectura al documento o al sistema, **sin copias, sin descarga y sin fotografiar**, salvo autorización escrita registrada.
4. **Registro.** Cada facilitación se asienta en la **bitácora del expediente**: qué material, a quién, en qué sesión, con qué alcance y con qué autorización. La bitácora demuestra la trazabilidad de la facilitación sin revelar el contenido facilitado.
5. **Cierre.** Al cerrar la evaluación, el acceso se revoca y la bitácora se archiva con el expediente. Un informe propio del evaluador puede citar el material facilitado por su título, sin reproducir su contenido.