

## Continuación de la matriz de requerimientos:

1. ¿El proveedor acepta una cláusula en el contrato que especifique el mecanismo de entrega de los datos del cliente al mismo ante necesidades puntuales o decisión del contrato, manteniendo la integridad de los mismos, así como el borrado de la información en sus sistemas al finalizar el servicio?
  1. Ver las regulaciones → hay que entregarla al autor o al cliente.
  2. Ver que a la hora de entregar la info se haga con **integridad** y confidencialidad. A la hora de la entrega era tal como llegó, no hay modificaciones (te desligas legalmente, digamos).
  3. Qué mecanismos están definidos para esto, cuáles son los proceso a seguir.
2. ¿El proveedor posee algún mecanismo o proceso para evitar la fuga de información, detectar y prevenir violaciones de datos, filtraciones o destrucción no deseada de datos del cliente?
  1. **Detección de intrusión** en logs.
  2. **Marcas de agua:** Insertar algunos datos o información modificada por mí y que posee una apariencia solo conocida por mí (y difícil de replicar) → ¿Me roban una base de datos... como pruebo que era mía?
  3. **Robo de información:**
3. ¿El proveedor notifica a sus clientes cuando realiza cambios en el entorno productivo de la infraestructura y/o servicio que brinda con el fin de que este pueda tomar las medidas mitigantes en caso de pérdida de servicio?
  1. Bueno... puede o no que notifiquen.
  2. La gracia es garantizar la disponibilidad máxima, como puedas.
  3. Si hacemos una actualización a los servicios transaccionales (por ejemplo, un coso que maneja compras), no podés dejar fuera de servicio a los clientes porque perdés mucha plata → **Solución:** Load balancer empieza a redirigir al nuevo servicio e ir cambiando gradualmente. ¿Una transacción se perdió en el medio (en la mini ventana en que se realiza el cambio)? Usas el load balancer como caché.
4. ¿El proveedor utiliza buenas prácticas?
5. ¿El proveedor tiene acuerdos que garantizan que sus proveedores se adhieren a sus políticas de seguridad de la información y la privacidad?
6. ¿El proveedor tiene actualizados todos los componentes de su solución a la última versión o a la versión n-1 disponible por el fabricante/desarrollador del componente?
  1. Hay que hacer un plan de rollback.. Si las cosas no funcionan, volvemos para atrás, pero ¿Cómo?
  2. OpenSource WaZuh.
7. ¿El proveedor tiene la capacidad de acordar esquemas de retención que se adecuen a las políticas de retención de datos de los clientes?
  1. Guardar datos por 10 años → Para trazabilidad.

## Investigar:

- OWAS.
- OpenSource WaZuh.
- <https://echo.labstack.com/>