



CIRCULAR No. 01
RESPUESTAS A INQUIETUDES PROCEDIMIENTO DE EXCEPCIÓN
POR PROVEEDOR ÚNICO No. PEPU-CPJ-003-2020:
ADQUISICIÓN DE LICENCIAS ADICIONALES PARA LA
SOLUCIÓN DE FIRMA ELECTRONICA DEL PODER JUDICIAL.

Tenemos algunas consultas relacionadas con los TDR del proyecto PEPU-CPJ-003-2020.

Algunas están relacionadas con los **requerimientos técnicos** enumerados en la descripción de los bienes y servicios del **apartado 6** de los TDR, concretamente:

- Uno de esos requerimientos enumerados en la página 3, recoge la necesidad de un servicio de adaptación del producto utilizado, para habilitar la autenticación de múltiples factores por distintos métodos. A este respecto, tenemos dudas:
 1. Lo que se solicita, ¿es un segundo factor de autenticación (2FA), es decir, se pide después de un login correcto con user/password, o se desea disponer de esta alternativa como mecanismo principal para hacer login sin user/password?

Respuesta: Se debe habilitar para que cuando el usuario y contraseña sean validados sea requerido el segundo factor de autenticación, en adición, sin reemplazar el mecanismo de autenticación por contraseña.

2. Si es un 2FA, ¿sería obligatorio? ¿Opcional a nivel de usuario? Normalmente, si se activa como obligatorio, el único segundo factor que podría garantizarse es el OTP al email, porque el usuario debería introducir después de un login su celular -salvo que ya esté informado- para SMS o enrolar una semilla para un Authenticator.

Respuesta: Debemos tener la posibilidad de habilitar y deshabilitar el MFA de manera global y para usuarios específicos. No debe estar limitado a OTP-Email, sino incluir también aplicaciones de generación de tokens.

3. Cuando se dice Google Authenticator, Microsoft Authenticator, ¿se deben implantar ambos o basta con uno -sería el de Google-?

Respuesta: Debe ser posible asociar cualquier aplicación de generación de tokens, las más conocidas son Google Authenticator, Microsoft Authenticator.

4. Si no fuese un 2FA, sino el método principal de autenticación, ¿cómo funcionaría? En este caso sería más pesado para el usuario. El usuario debería meter su email o teléfono en una pantalla; el sistema debería verificar que realmente ese email o teléfono está registrado (y si no lo estuviera... ¿qué debería hacer? No parece idóneo decir que no lo está por seguridad, dado que proporciona pistas a un potencial atacante). Y si lo está, proceder a enviar un OTP al email o teléfono para hacer el login. Y en el caso de Authenticator, el usuario debería proporcionar su código de usuario.



Respuesta: Cuando el colaborador coloca su usuario y contraseña, estos serán validados, si uno de estos no es correcto se arroja un mensaje indicando que el usuario o contraseña no son correctos, no se debe indicar que no existe en caso de ser la situación. Cuando sean validados correctamente, entonces solicitara el segundo factor de autenticación que puede ser un OTP-Mail o un Token generado por una aplicación.

5. En el caso del envío de SMS, ¿tiene ya Poder Judicial un proveedor de SMS que debamos integrar en la solución? ¿Podrían darnos más detalles?

Respuesta: No, esto debe ser parte de la propuesta.

6. Otro de esos requerimientos, enumerados en este caso en la página 4, se refiere a la migración de lo servicios, En este punto queríamos recibir confirmación de que no se requiere la migración de Viafirma Fortress, por lo que la firma desatendida con certificado en HSM seguirá haciéndose las premisas de Viafirma. ¿Es así?

Respuesta: No es requerida la migración de Viafirma Fortress.

Hay otra consulta relacionada con la **documentación requerida del apartado 12**, en concreto, uno de los puntos de la letra **C** (página 7):

7. Cuando se pide el "servicio de instalación y configuración de licencias, se está haciendo referencia a la documentación relativa a un manual de administrador que permita crear nuevos usuarios/licencias en el software. ¿es así? La pregunta viene porque esa documentación ya la tienen disponible y queríamos confirmar si es la misma, por si no lo fuera, tener claro qué debemos aportar.

Respuesta: El servicio de instalación y configuración de las licencias hace referencia a la necesidad de que el proveedor habilite estas licencias en la plataforma. La documentación suministrada deberá estar asociada a las nuevas funcionalidades habilitadas según los términos de referencia.

GERENCIA DE COMPRAS Y CONTRATACIONES.