Cumplimiento de requisitos de seguridad de la información en el PaP

A través del presente documento, el Responsable Funcional/BRM particulariza el estado del conjunto de medidas de seguridad de la información aplicadas en el proyecto.

Estas medidas de seguridad se detallaron **en el inicio del proyecto** a través del ANEXO IX '***Requerimientos de seguridad de la información para el desarrollo de aplicaciones y/o adquisición de equipamiento HW/SW relacionado con redes de comunicación y/o sistemas de información',*** incluido en el '*Pliego – Tipo de condiciones particulares para la contratación de servicios mediante procedimiento abierto'.*

Además, se requiere que las medidas previas al pase al estado de Producción de la aplicación, de la que es objeto este documento, cumplan los requisitos expuestos más adelante en el apartado REQUISITOS. También es necesaria la firma de este documento que implica el compromiso de renovación del certificado de las webs de la aplicación, así como la solicitud de pasar las pruebas de vulnerabilidad, con la herramienta Qualys, cada vez que haya una subida de versión de la aplicación y/o del middleware que le da soporte, sea de quien sea la solicitud de upgrade.

Es obligatorio rellenar todos los campos del formulario y, como se ha mencionado anteriormente, firmarlo electrónicamente.

Fecha	
Siglas / Código de proyecto (Nombre de la aplicación y/o código de proyecto)	
Nombre común por el que se conoce	
Persona responsable del proyecto	
Persona responsable de la aplicación (Gestionará las autorizaciones para las altas, bajas, modificaciones y revisiones de los usuarios de la aplicación)	
BRM	

Breve descripción de la aplicación	

REQUISITOS DE DESARROLLO:

Nombre del Integrador					
Cumplimiento de medidas de seguridad ¿Se cumplen todas las medidas de seguridad detalladas en el Anejo IX del Pliego de Contratación (Medidas de Seguridad de la información)?	Elegir uno				
Nivel de seguridad del sistema según el Esquema Nacional de Seguridad Ver **Anexo I** de este documento.	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Autenticidad**	**Trazabilidad**
	Bajo	Bajo	Bajo	Bajo	Bajo
	Valoración Final Bajo (Valor más alto de las dimensiones anteriormente detalladas)				

REQUISITOS DE IMPLANTACIÓN:

Se ha efectuado un análisis de vulnerabilidades de TODOS los SERVIDORES que dan soporte a la aplicación con la herramienta Qualys.	SI ◯	NO ◯
No hay vulnerabilidades de nivel superior a 2 en los informes proporcionado por Qualys.	SI ◯	NO ◯
Los accesos WEB están securizados por protocolo HTTPS.	SI ◯	NO ◯
Se ha utilizado certificado interno, externo o una Wild Card de Adif.	ELIGE UNO	
Nombre del certificado		

FIRMADO POR:

EN CALIDAD DE RESPONSABLE DEL INTEGRADOR.

FIRMADO POR:

EN CALIDAD DE: ELIGE UNO

FIRMADO POR:

EN CALIDAD DE JEFE DE ÁREA DE EXPLOTACIÓN

ANEXO I - NIVEL DE SEGURIDAD DEL SISTEMA SEGÚN EL ESQUEMA NACIONAL DE SEGURIDAD

Para clasificar el sistema de información, se tiene que valorar el impacto que tendría un incidente sobre éste, y que afecte a la seguridad de la información y los sistemas. Para determinar ese impacto hay que tener en cuenta las dimensiones de la seguridad: Disponibilidad [D], Integridad [I], Confidencialidad [C], Autenticidad [A], Trazabilidad [T], en adelante [DICAT]:

DISPONIBILIDAD DEL SERVICIO

¿Qué tiempo de recuperación es necesario para evitar daños (financieros, reputacionales, estratégicos y/o humanos) asociados con la no disponibilidad del servicio?

- Se permite la restauración del servicio en un periodo superior a 5 días (**N/A**)
- Se permite la restauración del servicio en un periodo comprendido entre 1 y 5 días (**BAJO**)
- Se permite la restauración del servicio en un periodo comprendido entre 4 y 24 h (**MEDIO**)
- Se permite la restauración del servicio en un periodo no superior a 4 horas (**ALTO**)

INTEGRIDAD DE LA INFORMACIÓN

¿Qué daños (financieros, reputacionales, estratégicos y/o humanos) implicaría para la organización, la inexactitud o perdida de la información?

- Se podría reemplazar fácilmente con un activo de igual calidad (**N/A**) (Copia de seguridad o restauración manual de la información)
- Se podría reemplazar con un activo de similar calidad con un esfuerzo razonable (**BAJO**) (Copia de seguridad o restauración manual de la información)
- Se podría reemplazar con un activo de similar calidad con un esfuerzo alto (**MEDIO**) (Copia de seguridad o restauración manual de la información)
- La calidad necesaria es difícil o imposible de reconstruir, o de muy alto coste (**ALTO**) (Copia de seguridad o restauración manual de la información)

CONFIDENCIALIDAD DE LA INFORMACIÓN

¿Qué daños (financieros, reputacionales, estratégicos y/o humanos) implicaría la divulgación de la información tratada, a organizaciones o terceros no autorizados?

- Información sin restricciones en su difusión. No ocasionaría daños (**N/A**)

- Perjuicios al ciudadano, incumplimiento leve de normativa, pérdidas económicas y/o daño reputacional apreciables, … (**BAJO**)
- Daños al ciudadano (subsanables), incumplimiento de normativa con sanción, pérdidas económicas y/o daño reputacional importantes, ... (**MEDIO**)
- Grave daño al ciudadano, incumplimiento grave de normativa, pérdidas económicas y/o daño reputacional grave, … (**ALTO**)

AUTENTICIDAD DEL SERVICIO

¿Qué requerimientos son aplicados para evitar daños (financieros, reputacionales, estratégicos y/o humanos) asociados con la suplantación de usuarios con acceso a la información?

- No se requiere conocer el usuario. Ej: Usuarios genéricos **(N/A)**
- Se requiere conocer el usuario. Ej: usuario y contraseña **(BAJO)**
- Se requiere conocer el usuario que accede y dónde accede en la aplicación (perfiles) **(MEDIO)**
- Se requiere conocer el usuario que accede, dónde accede en la aplicación (perfiles) y además la certificación del usuario por una tercera parte **(ALTO)**

TRAZABILIDAD

¿Qué registros son aplicados para evitar daños (financieros, reputacionales, estratégicos y/o humanos) asociados con la incapacidad de averiguar el origen de un fallo de seguridad en la información utilizada?

- No hay necesidad de registrar ninguna acción o evento **(N/A)**
- Se registran acciones de usuarios de forma genérica **(BAJO)**
- Se registran, a nivel de usuarios, las acciones críticas **(MEDIO)**
- Se registran, a nivel de usuarios, las acciones sensibles (críticas y otras de especial interés) **(ALTO)**