3. Requerimientos de seguridad

Identificación y autenticación		
Requerimientos	**Preguntas asociadas**	**Equivalencia con HL7**
La gestión de identificación / autenticación comienza con la asignación de un identificador a una entidad, que debe verificarse en un proceso de autenticación. La autenticación puede basarse en conocimiento que solo la persona tiene (por ejemplo, contraseñas), en un token certificado, elemento que ha sido otorgado por una autoridad (por ejemplo, tarjeta inteligente, clave criptográfica, etc.), o en propiedades que caracterizan al individuo (por ejemplo, biometría, voz, escritura a mano, etc.).	• ¿Dispone el Sistema de un mecanismo de control de acceso para acceder a información protegida basado en usuario y contraseña *(username/password)*? • ¿Dispone el Sistema de un mecanismo de control de acceso para acceder a información protegida basado en certificado digital? • ¿Dispone el Sistema de un mecanismo de control de acceso para acceder a información protegida basado en un token seguro? • ¿Dispone el Sistema de un mecanismo de control de acceso para acceder a información protegida basado en información biométrica? • ¿Ofrece el sistema al usuario la posibilidad de cambiar su contraseña? • ¿Ofrece el sistema al usuario la posibilidad de generar una nueva contraseña cuando la ha olvidado?	CPS1.1. TI1.

	• ¿Tiene el sistema un procedimiento y mecanismo que permite identificar de forma única a un paciente? Por ejemplo, para distinguir entre personas que tienen nombre y apellido parecidos que puedan inducir a confusión. En estos casos, deben confirmarse otros datos de identificación, por ejemplo, fecha y lugar de nacimiento y nombre de los padres. • ¿Tiene el sistema la capacidad de gestionar más de un código de identificación para cada paciente? Por ejemplo, número de historia clínica del establecimiento de salud, código de identificación de la red asistencial y código de identificación nacional. • ¿Tiene el sistema conexión con un MPI[6] local? • ¿Tiene el sistema conexión con un MPI externo perteneciente a la organización, pero no de ámbito nacional? • ¿Tiene el sistema conexión con un MPI externo de ámbito nacional? • ¿Dispone el Sistema de un mecanismo de autenticación para acceder a información protegida acreditado según los estándares de internacionales de autenticación (por ejemplo, SAML, WS-Trust, Kerberos)?	

[6] Master Patient Index

	• ¿Tiene el sistema mecanismos para administrar las identidades digitales (cuentas, claves, tokens) a lo largo de su ciclo de vida, desde el registro hasta la terminación? • ¿Tiene el sistema capas de Hardware/Software donde aplique protocolo de validación AAA (autenticación, autorización y contabilización)?	
Se deben contemplar mecanismos de renovación de contraseña, de caducidad de sesión, de control de autenticación inválida o maliciosa. Las contraseñas deben guardarse de forma encriptada y segura y deben obedecer a unas normas para asegurar el máximo nivel de seguridad posible.	• ¿Tiene el sistema un mecanismo de autorización que imponga el bloqueo de límites de tiempo en caso de error de inicio de sesión y los privilegios mínimos predeterminados? • ¿Tiene el sistema un mecanismo de caducidad de sesión por inactividad del usuario conectado? • ¿Tiene el sistema un mecanismo de administración de contraseñas que siga los estándares de seguridad actuales (NIST SP 800-57 o similar)? • ¿El sistema emplea medidas específicas para proteger los servicios de acceso remoto? • ¿Tiene el sistema mecanismos de generación de Tokens?	CPS1.1. TI1.
Se deben contemplar mecanismos para el tratamiento de personas dependientes, menores o tutelados, su identificación y autenticación.	• ¿Tiene el sistema un mecanismo para identificar y autenticar pacientes cuando uno de ellos es representante de otro? (menores, tutelados…)	

Permisos y roles de los actores		
Requerimientos	**Preguntas asociadas**	**Equivalencia con HL7**
El control de acceso, incluidas las acciones permitidas, puede basarse en privilegios y roles asignados a una entidad (o persona) por una autoridad de acuerdo con el atributo de la entidad o un conjunto de competencias y / o desempeños que son asociados con un perfil profesional y una tarea, respectivamente. La autorización y el control de acceso también pueden basarse no solo en políticas que reflejen la legislación y regulaciones incluyendo los consentimientos establecidos por el sujeto o su representante, pero también por condiciones ambientales o contextuales. Sobre todo, por una buena organización del establecimiento sanitario	• ¿Tiene el sistema una política de control de acceso para autorizar y revocar los derechos de acceso a los sistemas de información? • ¿Tiene el sistema la capacidad de configurar estas reglas de acceso con facilidad? • ¿Tiene el sistema un proceso para otorgar y revocar el acceso de usuario apropiado? • ¿Tiene el sistema procedimientos para revisar periódicamente el acceso de los usuarios a fin de garantizar que solo se apliquen los privilegios necesarios? • ¿Tiene el sistema un sistema de autenticación que aplica niveles más altos de autenticación para proteger los recursos con niveles más altos de sensibilidad? • ¿Tiene el sistema una guía de uso establecida para dispositivos informáticos móviles (independientemente de la propiedad) que almacenan, procesan o transmiten datos del sistema? • ¿Tiene el sistema mecanismos para posibilitar que las historias de usuario y las funciones contengan restricciones de seguridad funcionales? Por ejemplo, que determinados perfiles	TI1

	(o roles) solo puedan acceder a la información de los pacientes con quienes tienen relación asistencial. Por ejemplo, los pacientes de mi servicio, o de mi zona básica de salud, o los pacientes de radiología. • ¿Tiene el sistema mecanismos para asegurar que el control de acceso está basado en atributos o características mediante el cual el código verifica la autorización del usuario para una característica / elemento de datos en lugar de solo su función?	
Trazabilidad de las acciones		
Requerimientos	**Preguntas asociadas**	**Equivalencia con HL7**
Un Sistema EHRS debe tener incorporados mecanismos internos de auditoría y trazabilidad para registrar la actividad relacionada con eventos clave en tiempo real, tanto desde un punto de vista de actividad de un usuario como del propio sistema en cuanto a procesos internos (por ejemplo, alertas o notificaciones) o de administración de sus componentes (backups, extracciones de información, etc.). El registro de auditoria debe contemplar toda la información necesaria (quién, qué, cuándo, dónde) y ser accesibles y consultables durante un periodo de tiempo suficiente. En algunos casos, con carácter indefinido. Por ejemplo quién ha elaborado, editado, firmado un informe médico, cuándo,	• ¿Tiene el sistema la capacidad de generar un registro de auditoría para toda acción de autenticación/Conexión (exitosa o no), o cambio de contraseña realizada por el usuario? • ¿Tiene este registro de auditoría de usuario toda la información relativa a quién, qué, cuándo, dónde? • ¿Tiene el sistema la capacidad de generar un registro de auditoría para toda acción realizada por el usuario contra datos o funcionalidades sensibles? • ¿Tiene este registro de auditoría de usuario toda la información relativa a quién, qué, cuándo, dónde?	TI2

dónde etc.) ¿"Dónde" se refiere a lugar físico (tiene su importancia) o a lugar de la información? PE acceso a los resultados de laboratorio, a un episodio etc.	• ¿Tiene el sistema la capacidad de generar un registro de auditoría contra acciones del propio sistema que afecten a datos sensibles? Es decir, acciones internas que realiza el sistema por su cuenta, sin la intervención de un usuario logado, como puede ser por ejemplo la limpieza o archivado de información antigua de una historia, la sincronización de información, etc. • ¿Tiene este registro de auditoría de procesos internos del sistema toda la información relativa a quién, qué, cuándo, dónde? • ¿Tiene el Sistema la capacidad de generar un log de auditoría con herramientas estándares? • ¿Guarda el sistema estos registros de auditoría accesibles para ser consultados durante más de 6 meses?	
Integridad, disponibilidad y confidencialidad de la información		
Requerimientos	**Preguntas asociadas**	**Equivalencia con HL7**
En toda solución debe aplicarse una serie de normas y buenas prácticas que aseguren que los datos sean fidedignos, actualizados y estén disponibles según la ley y la normativa actual.	• ¿El sistema utiliza métodos de cifrado apropiados o comprobados para proteger los datos confidenciales en tránsito?	TI1

	• ¿Están las comunicaciones entre los componentes de la aplicación, incluidas las API, el middleware y las capas de datos, autenticadas? • ¿El sistema cuenta con políticas que indiquen cuándo se debe utilizar el cifrado (por ejemplo, en reposo, en tránsito, con datos sensibles o confidenciales, etc.)? • ¿Se contemplan las normativas de seguridad y el cumplimiento de protección de datos que aplican a nivel nacional del país en que se ha de implantar el sistema? • ¿El sistema emplea tecnologías para bloquear o restringir la información confidencial no cifrada para que no viaje a redes que no son de confianza? • ¿Las bases de datos seguras utilizan niveles de cifrado de base de datos? • ¿El sistema requiere cifrado en dispositivos informáticos móviles (es decir, portátiles, tabletas, etc.)? • ¿Tiene el sistema restricciones de acceso lógico a los componentes internos del sistema? • ¿Cuenta la comunicación entre sistemas con identificación entre partes mediante Certificado Digital? • ¿Tiene el sistema identificados y clasificados los datos sensibles en niveles de protección? • ¿Tiene el sistema la capacidad de rectificar los datos de un usuario cuando estos están asociados erróneamente?	

	• ¿El sistema cuenta con elementos de gestión de cambios? • ¿Tiene el sistema políticas de identificación de datos sensibles? • ¿Tiene el sistema mecanismos específicos para tratar y almacenar de forma anonimizada los datos sensibles?	
Gestión de riesgos		
Requerimientos	**Preguntas asociadas**	**Equivalencia con HL7**
Toda organización o proyecto IT debe tener una metodología de la gestión del riesgo, que se base en las buenas prácticas y la aplicación de la normativa actual y estándares, tales como, ISO, COBIT, etc. En este sentido, se debe contemplar prácticas de gobierno y gestión de IT de extremo a extremo	• ¿El sistema tiene una persona o grupo con la responsabilidad de un proceso continuo de evaluación de la probabilidad de que las amenazas conocidas exploten las vulnerabilidades y, como resultado, el impacto en activos valiosos? • ¿Tiene el sistema un proceso para identificar y evaluar riesgos internos y externos razonablemente previsibles para la seguridad, confidencialidad y / o integridad de cualquier registro electrónico, en papel o de otro tipo que contenga información sensible? • ¿Se llevan a cabo sobre el sistema evaluaciones de riesgo de rutina para identificar los objetivos clave que deben ser respaldados por el programa de seguridad de la información? • ¿Se lleva a cabo documentación del riesgo?	

El sistema debe contar con mecanismos de protección web adecuados (incluido WAF, restricciones de puerto y protecciones DDoS).	• ¿Tiene el sistema mecanismos de protección de su aplicación web (por ejemplo, WAF, restricciones de puerto y protecciones DDoS)?	
Estándares y seguimiento de regulaciones		
Requerimientos	**Preguntas asociadas**	**Equivalencia con HL7**

Los elementos relativos a seguridad, cifrado, comunicaciones, etc. deben seguir una serie de normas o estándares reconocidos a nivel nacional o internacional, a la vez que deben ser aplicadas las normativas de seguridad y regulaciones definidas por organismos competentes como por ejemplo la GDPR[7] en el ámbito de la Unión Europea.	• ¿Están documentados y empleados los estándares para la gestión de claves?
	• ¿Utiliza el sistema estándares de comunicación segura (TLS 1?3, SSL v3, etc.)?
	• ¿Utiliza el sistema un nivel de cifrado de las comunicaciones SHA 1024 o similar?
	• ¿Cuenta el sistema con estándares para aislar datos y procedimientos y tecnologías sensibles para protegerlos del acceso no autorizado y la manipulación?
	• ¿Bajo qué normativa de protección, difusión y autorizaciones sobre los datos se rigen?
	  ○ ISO 27002
	  ○ GDPR o equivalente	

[7] General Data Protection Regulation de la Comisión Europea

	○ OWASP ○ CEW ○ NIST • ¿El proveedor del sistema participa con grupos, asociaciones y agencias de seguridad locales, nacionales o internacionales?	