Nexo
Oposiciones

TEMA 10

TIC EN EL SAS

Indice:

Introducción

Las Tecnologías de la Información y la Comunicación (TIC) se han convertido en un pilar fundamental del sistema sanitario moderno. En el Servicio Andaluz de Salud (SAS), las TIC son la columna vertebral que permite gestionar eficientemente los procesos asistenciales y administrativos, mejorando la calidad de la atención, la accesibilidad y la transparencia. La digitalización abarca desde la historia clínica electrónica de los pacientes hasta la gestión de los recursos humanos y económicos, integrando todos los niveles asistenciales. En los últimos años (especialmente a partir de 2022) se ha acelerado la transformación digital con nuevas herramientas, mayor enfoque en ciberseguridad y la consolidación de un puesto de trabajo digital para los profesionales sanitarios, todo ello bajo normas y códigos de conducta que aseguran un uso adecuado de la tecnología. En esta introducción, presentamos la importancia de las TIC en el SAS y cómo contribuyen a un sistema sanitario más eficaz, conectado y seguro. A continuación, desarrollaremos en detalle los principales sistemas corporativos del SAS, las medidas de ciberseguridad, la configuración del puesto digital del profesional, el código de conducta TIC vigente y la normativa aplicable. Este tema está orientado a opositores de cualquier perfil sanitario (TCAE, enfermería, medicina, fisioterapia, etc.), por lo que ofrece una visión global y práctica de las TIC en el SAS, con información actualizada al año 2025.

1. Sistemas corporativos del SAS

El SAS cuenta con numerosos sistemas de información corporativos, tanto de carácter clínico-asistencial como de gestión interna, que integran la información y soportan los procesos clave del servicio de salud. A continuación, se describen los sistemas más relevantes y sus funciones principales:

Diraya (Historia Clínica Electrónica)

Es el sistema unificado de historia clínica electrónica del SAS, que soporta la gestión clínica en todos los niveles asistenciales. Diraya integra toda la información de salud de cada paciente en un registro único regional, de forma que esté disponible en el lugar y momento necesarios para su atención. Sobre Diraya pivota la mayor parte de la actividad asistencial: incluye módulos avanzados como receta electrónica (Receta XXI), el sistema de citas centralizado y registros de pruebas diagnósticas, entre otros. Gracias a esta integración, Diraya enlaza la información de atención primaria, consultas de especialidades, hospitales, urgencias, farmacia comunitaria, laboratorio, radiología, telemedicina, derivaciones y más. Es considerado un sistema pionero a nivel nacional y europeo, ya que Andalucía fue de las primeras en implantar la receta electrónica (desde 2003) y el acceso compartido a la historia clínica única en todo el servicio de salud. Diraya facilita así la continuidad asistencial y evita la fragmentación de la información, permitiendo que cualquier profesional autorizado acceda a la historia de salud digital del paciente con los datos actualizados. Por ejemplo, un médico de urgencias puede ver las alergias, medicación o últimos informes del paciente registrados en atención primaria u hospitalaria. Todo ello se logra mediante el Número Único de Historia de Salud de Andalucía (NUHSA) que identifica a cada persona en el sistema.

Receta Electrónica (Receta XXI)

Es el módulo de prescripción y dispensación farmacéutica electrónica integrado en Diraya. Implantado inicialmente en 2003, fue el primer sistema de receta electrónica operativa en Europa. Permite que los profesionales prescriban medicamentos de forma digital y que las farmacias accedan a las prescripciones para dispensarlas, eliminando la receta en papel. Receta XXI facilita el control de tratamientos, evitando interacciones y duplicidades, ya que el historial farmacoterapéutico del paciente está disponible en su historia clínica. Los farmacéuticos registran en el sistema las dispensaciones realizadas e incluso pueden comunicar incidencias al médico, logrando un ciclo cerrado de información. Este sistema ha sido reconocido internacionalmente y Andalucía, junto con el Ministerio de Sanidad, lideró proyectos europeos de interoperabilidad de receta electrónica. Actualmente, la receta electrónica del SAS es interoperable con otras comunidades autónomas de España y con países europeos, de modo que un ciudadano andaluz pueda retirar su medicación en otra región/país y viceversa, en el marco de la Receta Electrónica Europea.

Citación (Gestión de agendas)

Es la aplicación de gestión de citas integradas en Diraya, encargada de administrar las agendas de Atención Primaria, Consultas Externas de especialistas y Pruebas diagnósticas. A través del módulo de Citación, los profesionales disponen de la lista de pacientes citados y se coordina el flujo de pacientes en cada nivel asistencial. Todas las agendas están unificadas, de modo que una cita para una consulta o prueba puede gestionarse desde cualquier centro una vez autorizada la petición. Este módulo se integra con otros sistemas de acceso del ciudadano: por ejemplo, Salud Responde (centro de llamadas) utiliza Citación para asignar telefónicamente citas de medicina de familia y pediatría, Inters@s (oficina internet) también se conecta para la solicitud de cita con el médico de cabecera, y existe incluso un sistema de cita por SMS para primaria. Gracias a esta centralización (TARS, sistema de cita telefónica del SAS), se evitan duplicidades y se mejora la accesibilidad, permitiendo que un usuario pueda gestionar sus citas a través de múltiples vías que realmente operan sobre una misma agenda única.

ClicSalud+ (Portal web del paciente)

Es el portal web interactivo para la ciudadanía, que ofrece acceso seguro en línea a su información de salud y a servicios electrónicos sanitarios. Lanzado en 2018 como evolución de la antigua plataforma ClicSalud, ClicSalud+ actúa como una oficina virtual donde cualquier usuario del Sistema Sanitario Público de Andalucía puede consultar sus datos personales (por ejemplo, centro de salud y profesionales asignados) y datos clínicos (informes, resultados de análisis, lista de medicación, vacunas, etc.). Asimismo, permite realizar trámites esenciales en línea: solicitar o cambiar citas en el centro de salud, elegir médico o centro sanitario, renovar la tarjeta sanitaria, descargar el certificado COVID de vacunación, entre otros. Para acceder a información clínica sensible, el portal exige una autenticación robusta (certificado digital, Cl@ve PIN permanente, DNIe, etc.), garantizando la confidencialidad. ClicSalud+ se ha convertido en un canal masivo de relación con el paciente: en 2020 alcanzó casi 16 millones de accesos, reflejando la demanda de servicios digitales (consultas de informes, vacunas, citas, etc.). El diseño de ClicSalud+ se centra en la seguridad y facilidad de uso para promover la autonomía del paciente. Cabe destacar que ClicSalud+ complementa otros canales de atención al ciudadano, como el teléfono de Salud Responde y la App móvil, ofreciendo así atención 24x7 todos los días. Por su carácter innovador,

este portal ha sido reconocido internacionalmente como ejemplo de acceso ciudadano a datos sanitarios.

Salud Responde (Teléfono y App móvil)

Aunque no mencionado explícitamente en el enunciado, es importante ubicarlo entre los sistemas corporativos orientados a la ciudadanía. Salud Responde es el servicio multicanal de atención al usuario del SAS, que incluye un call- center (teléfono 955 545 060), una aplicación móvil y servicios de notificación. Se integra con Diraya para diferentes funciones: gestión de citas primarias (como vimos con TARS), información sanitaria general, coordinación de urgencias y recordatorios (por ejemplo, aviso de citas hospitalarias o campañas preventivas). Desde 2023, Salud Responde emite las llamadas salientes desde un número único identificable (955800008) para mejorar la seguridad y confianza de los pacientes, previniendo fraudes. La app Salud Andalucía (antes Salud Responde) permite igualmente pedir cita, acceder a información COVID, programa de vacunación, etc. En conjunto, Salud Responde + ClicSalud+ + App constituyen la Atención Digital al Ciudadano, un ecosistema por el cual el SAS ofrece servicios personalizados, continuos y seguros a la población.

Otros sistemas asistenciales corporativos

Además de Diraya y sus módulos, el SAS dispone de otras aplicaciones específicas para soporte al diagnóstico y a la actividad clínica. Por ejemplo, existen sistemas de gestión de imagen médica (RIS/PACS) para radiología que integran las imágenes con la historia clínica; sistemas de laboratorio (SIL) conectados al Módulo de Pruebas Analíticas de Diraya; aplicaciones como Delta (notificación de enfermedades profesionales y accidentes laborales, integrada con prevención de riesgos) o Gestión de listas de espera quirúrgica; y plataformas de telemedicina y consulta telemática (especialmente impulsadas tras 2020). Un término citado en el enunciado, JARA, merece aclaración: JARA es en realidad el nombredelproyectodehistoria clínica digital del Servicio Extremeño de Salud (Extremadura), y no un sistema del SAS.En Andalucía,el sistema equivalente es Diraya ; portanto ,JARA no se utiliza en el SAS, aunque conceptualmente es similar (unificar HCE a nivel regional). Es posible que en el estudio comparativo de sistemas sanitarios se mencione JARA como referencia de otra comunidad autónoma, pero en nuestro contexto andaluz, Diraya es el núcleo de la información clínica.

Sistemas de gestión económica y de recursos humanos

El funcionamiento corporativo del SAS se apoya en plataformas integrales para la gestión administrativa, logística, financiera y de personal, alineadas con los sistemas de la Junta de Andalucía. Destacan cuatro siglas clave: GERHONTE, SIGLO, GIRO y SUR. GERHONTE (Gestión de Recursos Humanos del SAS) es la plataforma corporativa que centraliza todas las funciones de RRHH: desde el registro completo de datos del personal, la gestión de nóminas y cotizaciones, hasta los procesos selectivos, traslados, bolsa de empleo, formación, control de jornada, incidencias y prevención de riesgos. Implantado en todos los centros del SAS, GERHONTE actúa como el sistema único de personal, con miles de usuarios internos (equipos de gestión de personal) y funcionalidades avanzadas como expediente electrónico del profesional y currículum digital. SIGLO (Sistema Integral de Gestión Logística) es el sistema de compras y logística sanitaria del SAS, que abarca la contratación pública electrónica, la gestión de almacenes y

suministros, el control de stock de medicamentos y material, la distribución interna y la facturación a terceros. Facilita una gestión centralizada y trazable de todos los bienes y servicios en el SAS, integrándose con catálogos de productos corporativos y módulos de inventario. GIRO (Gestión Integral de Recursos Organizativos) es la aplicación contable-presupuestaria común de la Junta de Andalucía (sustituta del antiguo sistema Júpiter), utilizada por el SAS para contabilidad financiera y control presupuestario en coordinación con la Intervención General. En GIRO se registran, por ejemplo, las obligaciones de gasto derivadas de nóminas (enviadas desde Gerhonte) o de facturas de compras (enviadas desde Siglo), y se consolida el presupuesto del SAS dentro del presupuesto autonómico. Por último, SUR (Sistema Unificado de Recursos) es la plataforma corporativa de la Junta para la gestión de ingresos públicos y tributos, que completa el ciclo económico registrando tasas, ingresos por prestación de servicios sanitarios a terceros, etc., alimentando también la información a GIRO. Estos cuatro sistemas internos (GERHONTE, SIGLO, GIRO, SUR) están interconectados para garantizar la coherencia de la información administrativa y financiera. Su conocimiento es más propio de perfiles administrativos, pero cualquier empleado del SAS debería entender su existencia, ya que de ellos depende el pago de nuestras nóminas, el aprovisionamiento de material sanitario o la tramitación de contrataciones y presupuestos.

Registro Electrónico del SAS (RECSAS)

En línea con la transformación digital de la Administración, el SAS cuenta (o está implantando plenamente desde 2022) con un Registro Electrónico corporativo para la entrada y salida de documentos oficiales. Esto permite a los profesionales y usuarios presentar solicitudes, escritos o documentación de forma telemática, sin tener que acudir físicamente a un registro presencial, cumpliendo con la Ley 39/2015 de Procedimiento Administrativo Electrónico. El RECSAS (término no oficial pero útil para referirse al Registro Electrónico del SAS) se integra en la sede electrónica de la Junta de Andalucía, aportando beneficios como disponibilidad 24/7, acreditación digital de la identidad y trazabilidad de los trámites. Esta iniciativa surgió ante las limitaciones del registro en papel (horarios, presencialidad, riesgo de extravío) y supone una mejora en eficiencia y servicio. Todos los hospitales y distritos sanitarios del SAS están incorporados en el ámbito de este registro electrónico, de modo que cualquier comunicación oficial (por ejemplo, instancias de opositores, solicitudes de segunda opinión médica, recursos administrativos, etc.) pueda cursarse electrónicamente con plena validez legal.

En resumen, los sistemas corporativos del SAS abarcan tanto el ámbito asistencial (historia clínica digital, receta electrónica, citas, portal del paciente, etc.) como el ámbito organizativo (gestión de personal, logística, finanzas, etc.). Esta arquitectura integrada permite que el SAS funcione como una única entidad cohesionada en cuanto a información, a pesar de su gran tamaño (más de 100.000 profesionales y centenares de centros sanitarios). Cada sistema tiene módulos específicos, pero todos comparten objetivos comunes: mejorar la calidad asistencial, optimizar recursos, facilitar la toma de decisiones informadas y, en definitiva, ofrecer un servicio de salud público más eficiente y centrado en el ciudadano.

(Se adjunta a continuación, a modo de síntesis, una tabla resumen de los principales sistemas mencionados y su propósito):

Sistema	Descripción y funciones principales
Diraya	Historia clínica electrónica unificada de Andalucía: integra datos clínicos de todos los niveles asistenciales (primaria, especializada, urgencias, farmacia, etc.). Incluye receta electrónica, gestión de citas, módulos de laboratorio, imagen médica, etc., sobre un registro único por paciente (NUHSA).
Receta XXI	Módulo de receta electrónica dentro de Diraya: permite prescripción y dispensación digital de medicamentos. Implantado en 2003 (pionero en Europa); accesible en todas las farmacias andaluzas y operable desde cualquier centro sanitario.
ClicSalud+	Portal web del ciudadano (oficina virtual de salud): acceso a datos personales y clínicos (informes, medicamentos, pruebas) y realización de trámites sanitarios en línea (citas, tarjeta sanitaria, etc.). Requiere autenticación segura; complementa a Salud Responde brindando atención 24/7.

Sistema	Descripción y funciones principales
Centro de atención telefónica (955 545060) y App móvil para gestiones Salud sanitarias: cita previa, consultas de información, recordatorios, coordinación de Responde urgencias. Integrado con Diraya-Citación para asignar citas por teléfono. Opera 24/7 y sirve de apoyo directo al ciudadano.	
GERHONTE	Sistema de Gestión de Recursos Humanos del SAS. Plataforma integral web para nóminas, expediente del profesional, contratación y oposiciones, bolsa de empleo, turnos, formación, prevención de riesgos, etc. Interconectado con finanzas (GIRO) y demás sistemas corporativos de la Junta.
SIGLO	Sistema Integral de Gestión Logística del SAS. Gestiona compras y contrataciones (expedientes electrónicos), almacenes y stocks de material sanitario, distribución a centros, facturación logística, catálogo corporativo de productos. Conectado con GIRO para registro contable de gastos.
GIRO	

Gestión Integral de Recursos Organizativos (Junta de Andalucía). Sistema contable-presupuestario común. En SAS se usa para la contabilidad financiera: contabiliza nóminas (datos de Gerhonte) y facturas/contratos (datos de Siglo), y consolida el presupuesto sanitario en el autonómico.

SUR

Sistema Único de Recursos (Junta de Andalucía). Plataforma de ingresos y recaudación: tasas sanitarias, ingresos por conciertos, pagos de terceros, tributos. Proporciona información de ingresos a GIRO para cerrar el ciclo económico-financiero.

Registro Electrónico (RECSAS)

Registro Electrónico del SAS para trámites administrativos digitales. Permite la entrada/salida de documentos de forma telemática en hospitales, distritos y servicios centrales. Mejora eficiencia (sin papel, sin horario limitado) y cumple con normativa de administración electrónica.

2. Ciberseguridad en el SAS

El creciente uso de herramientas digitales en sanidad exige una atención prioritaria a la ciberseguridad. Por ciberseguridad entendemos el conjunto de medidas y prácticas destinadas a proteger los sistemas de información, las comunicaciones y los datos frente a amenazas y usos no autorizados. En el contexto del SAS, la información manejada es altamente sensible (datos personales de salud, historiales clínicos, resultados de investigación, etc.), por lo que su protección es crucial tanto por imperativo legal como ético. A continuación, se abordan los principios básicos, las principales amenazas, las medidas de protección implantadas y el marco normativo vigente en materia de seguridad de la información.

Principios de la seguridad de la información: El SAS, como parte de la Administración andaluza, adopta los principios clásicos de la seguridad TIC, resumidos en la tríada CID: Confidencialidad, Integridad y Disponibilidad. La confidencialidad garantiza que solo el personal autorizado acceda a la información sanitaria (por ejemplo, solo sanitarios implicados pueden ver la historia de un paciente, bajo el principio de "necesidad de saber"). La integridad asegura que los datos no sean alterados o eliminados de forma indebida (cualquier modificación en una historia clínica queda registrada y debe ser legítima). La disponibilidad implica que los sistemas estén operativos cuando se necesitan, evitando caídas que impidan atender pacientes o recuperar información crucial. Junto a estos, también se consideran la autenticidad (verificar la identidad de usuarios y la procedencia de la información) y la trazabilidad o registro (capacidad de auditar quién accede o modifica datos, a fin de detectar ususindebidos). Estos principios están recogidos en la Política de Seguridad TIC de la Junta de Andalucía (Decreto 1/2011) y en el Esquema Nacional de Seguridad (ENS) aplicable a todos los sistemas públicos, y son la base sobre la cual se desarrolla la estrategia de ciberseguridad.

Amenazas habituales en el entorno sanitario: Los sistemas del SAS pueden enfrentar diversas amenazas cibernéticas, similares a las de cualquier gran organización pero con ciertos objetivos específicos. Algunas de las más relevantes son:

- Malware (software malicioso): virus informáticos, gusanos, ransomware y troyanos que pueden afectar a equipos clínicos o administrativos. En sanidad destaca el riesgo de ransomware (secuestro de datos a cambio de rescate), como se ha visto en incidentes a hospitales a nivel mundial.
- Phishing y ataques dirigidos: intentos de engaño vía correo electrónico u otros medios para obtener credenciales de profesionales o distribuir malware. Dada la naturaleza confiada del entorno sanitario, los ciberdelincuentes a veces se hacen pasar por organismos oficiales (p. ej. Correos, Ministerio de Sanidad) para que el personal haga clic en enlaces maliciosos.
- Accesos indebidos internos: a diferencia de otros sectores, en sanidad existe el riesgo de curiosidad maliciosa por acceder a historiales de pacientes famosos, vecinos o familiares sin justificación. Esto constituye una grave violación de la confidencialidad.
- Errores humanos y fugas de información: enviar información sensible al destinatario equivocado, pérdida de pendrives o portátiles sin cifrar, o conversaciones en entornos no seguros que revelen datos de pacientes. El factor humano sigue siendo una de las mayores vulnerabilidades.
- Ataques a infraestructuras críticas: interrupción de servicios mediante ataques de denegación de servicio (DDoS) a páginas web o sistemas, sabotaje a redes internas, o explotación de vulnerabilidades en equipos médicos conectados (IoMT, Internet de las Cosas Médicas).
- Amenazas avanzadas (APT): aunque menos común, un servicio de salud público podría ser objetivo de ataques persistentes avanzados, ya sea con motivación activista (exfiltrar datos para denunciar algo) o incluso geopolítica (espionaje de investigaciones, caos en infraestructuras).

Estas amenazas se han visto incrementadas con la mayor digitalización y especialmente durante la pandemia COVID-19, donde la expansión del teletrabajo y la necesidad de intercambio ágil de datos abrieron nuevos vectores de ataque.

Medidas de protección y buenas prácticas: Para contrarrestar dichas amenazas, el SAS ha desplegado un conjunto amplio de medidas de seguridad tanto técnicas como organizativas. Entre las principales cabe destacar:

- Control de accesos y autenticación: todos los profesionales acceden a los sistemas mediante credenciales individuales (usuario y contraseña) dentro del Dominio Corporativo SAS (DMSAS). Se exige el uso de contraseñas robustas (complejas y renovadas periódicamente) y no compartidas

  En ciertos entornos, se emplea autenticación multifactor o certificados digitales de empleado público (por ejemplo, Gerhonte requiere certificado digital personal para entrar). Asimismo, se definen perfiles de acceso según rol profesional, de manera que cada usuario solo pueda ver la información pertinente a su puesto.
- Cifrado y protección de datos: Los equipos corporativos tienen herramientas de cifrado de

disco y de dispositivos USB autorizados, para que si se pierde un portátil o memoria no se pueda leer su contenido. Las comunicaciones sensibles (p. ej., conexión de la historia clínica desde un centro remoto) viajan cifradas vía VPN o túneles seguros. También se anonimiza o seudonimiza la información en proyectos de investigación o entornos de prueba.

- Sistemas perimetrales de seguridad: La red corporativa del SAS está protegida por firewalls, sistemas de prevención de intrusiones (IPS/IDS) y filtros de contenido. Se monitoriza el tráfico entrante y saliente para detectar patrones anómalos o malware conocido. Además, se segmentan las redes: por ejemplo, la red asistencial está separada de la red de invitados WiFi o de la red industrial de equipos médicos, limitando la propagación de posibles infecciones.
- Antivirus y actualizaciones: Todos los puestos de trabajo digitales tienen antivirus/antimalware corporativo con actualizaciones frecuentes, y los servidores críticos igual. Se aplican parches de seguridad al sistema operativo y aplicaciones en cuanto están disponibles (según procedimiento de Gestión de Vulnerabilidades y Parches). El SAS sigue las alertas de ciberseguridad (del CCN- CERT, INCIBE, etc.) para corregir vulnerabilidades relevantes (ej: fallo de Windows, log4j, etc.).
- Backups y planes de contingencia: La información crítica (historias clínicas, bases de datos de gestión) se respalda periódicamente en sistemas de backup seguros. Existen CPDs redundantes y planes de recuperación ante desastres (DRP) para garantizar continuidad asistencial incluso si un centro pierde sus sistemas localmente. Por ejemplo, Diraya tiene alta disponibilidad y copias en tiempo real; ante una caída mayor, se pueden activar procedimientos manuales contingentes para seguir atendiendo (aunque sea en papel temporalmente).
- Concienciación y formación: El SAS insiste en que la seguridad es responsabilidad de todos los profesionales. Hay campañas de concienciación periódicas (cartelería, emails, cursos en la intranet de capacitación) sobre buenas prácticas: no abrir correos sospechosos, no introducir pendrives desconocidos, bloquear la sesión al ausentarse, etc. Por ejemplo, se ha distribuido una Guía de Ciberseguridad para nuevos profesionales con recomendaciones básicas. Además, se realizan simulacros de phishing internos para educar al personal a identificar amenazas.
- Políticas y procedimientos: Existen normativas internas como la mencionada Política de Seguridad TIC del SAS (alineada con el ENS) que establece responsabilidades (p. ej., la existencia de un Responsable de Seguridad, Comités de Seguridad TIC, etc.), clasificación de la información y medidas según nivel (básico, medio, alto). También procedimientos para gestión de incidentes de seguridad: si ocurre una brecha o incidente, el personal debe notificarlo inmediatamente (por ejemplo, al correo abuse@juntadeandalucia.es para incidentes de phishing, o a través de la plataforma AyudaDIGITAL), tras lo cual se activan protocolos de respuesta, contención, análisis forense y notificación a autoridades competentes (como la Agencia de Protección de Datos, si afecta a datos personales).
- Medidas organizativas: El SAS cuenta con un Comité de Seguridad TIC (CSISTIC-SAS) que define estrategias y aprueba normativas como el Código de Conducta TIC. Asimismo, hay un Delegado de Protección de Datos (DPD) en el seno de la Consejería de Salud que vela por el cumplimiento de la normativa de privacidad. Se llevan a cabo auditorías periódicas de seguridad y evaluaciones de riesgos de los sistemas, conforme exige el ENS, para detectar puntos débiles y fortalecerlos de manera proactiva.

Legislación y normativa vigente en seguridad: La ciberseguridad en el SAS no es opcional, sino que está respaldada por un robusto conjunto normativo de ámbito europeo, nacional, autonómico y corporativo. Algunos de los textos legales y reglamentarios más relevantes son:

- Reglamento General de Protección de Datos (RGPD, UE 2016/679): normativa europea de protección de datos personales, de aplicación obligatoria desde 2018, que establece principios como minimización de datos, seguridad y confidencialidad, y notificación de brechas en 72 horas. En salud, los datos de pacientes son categorías especiales (sensibles) que requieren medidas de seguridad reforzadas (art. 32 RGPD).
- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): norma española que adapta el RGPD y añade disposiciones específicas. Impone, por ejemplo, la obligación de designar un DPD en el SAS y detalla sanciones en caso de vulneraciones.
- Esquema Nacional de Seguridad (ENS): conjunto de medidas de seguridad obligatorias para los sistemas de información de las administraciones públicas en España. Establecido por el RD 3/2010 y actualizado por el RD 311/2022, clasifica los sistemas por niveles (básico, medio, alto) y define requisitos organizativos, operacionales y de protección técnica para cada nivel. El SAS, al manejar datos de salud (críticos) y proveer servicios esenciales, debe cumplir con nivel ALTO en muchos de sus sistemas, siguiendo las guías del Centro Criptológico Nacional (CCN-STIC).
- Ley 41/2002, básica reguladora de la autonomía del paciente: regula los derechos de los pacientes sobre su información clínica. Obliga a las instituciones sanitarias a garantizar la confidencialidad de la historia clínica, estableciendo que solo personal asistencial involucrado puede acceder a ella, y prevé sanciones y responsabilidades por accesos indebidos. Esta ley refuerza el principio de secreto profesional y el derecho del paciente a la privacidad, que en el mundo digital se traduce en control estricto de accesos y registro de auditoría.
- Ley 40/2015, de Régimen Jurídico del Sector Público: contiene en su artículo 156 y siguientes obligaciones en materia de seguridad de los sistemas de información públicos, indicando la adopción del ENS y la necesidad de políticas de seguridad y gobernanza de la ciberseguridad en cada organismo. El SAS, como entidad pública, se adhiere a esta ley mediante su normativa interna (p. ej., Decreto 1/2011 de la Junta, citado abajo).
- Decreto 1/2011, de 11 de enero (Junta de Andalucía): establece la política de seguridad de las TIC en la Administración andaluza. Este decreto sienta las bases de organización de la seguridad (roles, comités, responsabilidades), las normas de uso de medios electrónicos y la obligatoriedad de cumplir ENS a nivel autonómico. A raíz de él, se han desarrollado políticas específicas en cada Consejería y entes como el SAS, y por ejemplo la aprobación del Código de Conducta TIC en 2020 (ver sección 5).
- Real Decreto-ley 12/2018 (derogado por nueva normativa NIS2 pendiente de transposición): transponía la Directiva (UE) 2016/1148, conocida como Directiva NIS, sobre seguridad de redes y sistemas de información para operadores de servicios esenciales (entre ellos la asistencia sanitaria). Esta norma identificó a los servicios de salud como críticos, imponiendo medidas de seguridad similares al ENS y obligaciones de notificación de incidentes graves al CCN-CERT/ INCIBE. En 2022 se aprobó la Directiva NIS2 que endurece requisitos, y España deberá adaptarla; el SAS previsiblemente será considerado operador esencial con mayores exigencias de ciber-resiliencia.

- Normativa interna SAS: incluye la Política de Seguridad TIC del SAS, las Normas de Uso de Recursos TIC, y el Código de Conducta TIC (detallado en sección 5). También manuales y procedimientos específicos (gestión de incidencias de seguridad, uso del correo corporativo, teletrabajo seguro, etc.). Un ejemplo es la Instrucción 1/2023 de la Dirección General de Estrategia Digital (Consejería) sobre uso y funcionamiento de sistemas de información, que actualiza directrices de seguridad en el trabajo diario. Todo el personal del SAS debe conocer y acatar estas normas internas, disponibles en la intranet corporativa.

En conclusión, el SAS afronta la ciberseguridad de forma integral, combinando tecnología, procesos y concienciación humana. Los profesionales sanitarios que opositan deben no solo memorizar estos conceptos, sino entender su importancia práctica: un pequeño descuido (como dejar una sesión abierta o caer en un correo fraudulento) puede comprometer datos de miles de pacientes. Por ello, el SAS promueve una cultura de seguridad donde cada empleado actúa con responsabilidad y diligencia en el uso de las TIC, protegiendo así la confidencialidad de los usuarios y la continuidad de unos servicios sanitarios cada vez más digitales.

3. El puesto de trabajo digital en el SAS

El puesto de trabajo digital se refiere al conjunto de medios tecnológicos que el SAS proporciona a sus profesionales para desempeñar su labor diaria. Tradicionalmente, esto incluye el ordenador en la consulta o unidad, pero el concepto abarca hardware, software, conectividad y servicios asociados que configuran la experiencia digital del empleado público sanitario. En esta sección describiremos qué componentes conforman un puesto digital típico en el SAS, qué herramientas se utilizan en el día a día y cuáles son las buenas prácticas asociadas a su uso.

Componentes del puesto digital (hardware y sistemas operativos):

- Equipos informáticos: La mayoría de profesionales disponen de ordenadores de sobremesa corporativos en sus puestos (consultas, despachos, unidades), equipados con monitor, teclado y ratón. Estos PCs suelen operar con sistema Windows (versión adaptada al entorno corporativo, actualmente Windows 10/11) y están conectados a la red corporativa para acceder a aplicaciones y recursos ofimáticos. También existen ordenadores portátiles asignados a ciertos perfiles (dirección, personal que deba moverse, o teletrabajo puntual), los cuales se conectan vía red local o mediante VPN si operan desde fuera (por ejemplo, un médico coordinador que accede desde su domicilio).
- Terminales ligeros (thin clients): En muchos centros de atención primaria y áreas de atención al usuario, el SAS desplegó terminales ligeros en lugar de PCs convencionales. Estos son dispositivos de tamaño reducido sin disco duro, que se conectan a servidores centrales para ofrecer la sesión de trabajo (es decir, funcionan en modo cliente/servidor). Para gestionarlos eficientemente, el SAS desarrolló un sistema operativo ligero propio basado en Linux llamado LetSAS. LetSAS proporciona a esos terminales el acceso a las aplicaciones corporativas (Diraya y demás) de forma centralizada: las aplicaciones realmente se ejecutan en servidores y el terminal actúa como interfaz. Actualmente, unos 17.000 terminales ligeros en la red SAS usan LetSAS, lo que facilita actualizaciones uniformes y seguridad (los parches se aplican en el servidor y se propagan a todos). Este

entorno está optimizado para las consultas de primaria, mejorando tiempos de carga y simplificando el mantenimiento (pues desde la central se pueden actualizar todos en pocos días).

- Periféricos y otros dispositivos: Junto a los ordenadores, el puesto suele incorporar impresoras (ya sean personales USB en cada consulta para recetas e informes, o impresoras de red departamentales compartidas). También se utilizan lectores de tarjeta sanitaria (chip o banda magnética) para identificar pacientes en admisión, escáneres (especialmente en Historia Digitalizada, aunque casi todo nuevo documento ya nace digital en Diraya), cámaras web y auriculares para videoconsulta (servicios de telemedicina, muy impulsados para ciertas especialidades o seguimiento telemático). En las áreas administrativas es común el teléfono IP fijo en cada puesto (telefonía VoIP integrada en la red de datos) y en algunos casos terminales móviles corporativos (smartphones) para directivos o para servicios como 061 (emergencias) o unidades que requieren movilidad (p. ej. enfermeras gestoras de casos). Los móviles corporativos pueden llevar aplicaciones específicas (p.ej., una app de gestión de camas o de notificaciones internas). Por último, existe equipamiento especial como monitores de videoconferencia para sesiones clínicas remotas, etc., y en salas de reunión equipamiento colaborativo (pantallas inteligentes, etc.) que también forman parte del ecosistema digital del SAS.

Software y herramientas digitales del profesional:

El SAS ofrece un entorno estandarizado en cuanto a software para garantizar la compatibilidad y seguridad. En un puesto de usuario típico encontraremos:

- Sistemas operativos corporativos: Windows con las configuraciones de seguridad del dominio SAS (políticas de grupo que establecen contraseñas, bloqueo automático tras X minutos, etc.), y en terminales ligeros el mencionado LetSAS (Linux).
- Suite ofimática: Se dispone de herramientas de productividad como LibreOffice (suite ofimática de código abierto) en prácticamente todos los equipos. En algunos puestos también hay Microsoft Office según necesidades (por ejemplo, dirección y unidades específicas). Además, herramientas de visualización de PDF y otros formatos estándar.
- Aplicaciones corporativas del SAS: Aquí destacan todas las mencionadas en el apartado 2: Diraya (con sus diferentes módulos de Historia de Salud, Receta XXI, Citación, Urgencias, etc.), aplicaciones de gestión de pruebas (laboratorio, radiología), Gestión de Pacientes (para admisión, listas de espera), etc. Estas aplicaciones suelen ser web (accesibles via navegador corporativo) o cliente-servidor con accesos directos en el menú. Por ejemplo, el profesional de primaria tiene acceso a Diraya AP (atención primaria), si es en hospital tendrá Diraya Hospitalización/Consultas, etc. Asimismo, vía web están disponibles ClicSalud+ profesional (para ver información del paciente desde la perspectiva profesional) o el Nodo SNS (HCDSNS) para consultar historiales de otras comunidades.
- Herramientas de comunicación y colaboración: Todo empleado SAS tiene un correo corporativo (@juntadeandalucia.es o específico de sspa) accesible vía Webmail/Outlook. Además, existe una plataforma de firma electrónica (Port@firmas) para firmar documentos digitalmente con certificado (p. ej., resoluciones o informes). Para reuniones virtuales, se pueden emplear herramientas como WebEx o similares (la Consejería ha habilitado sistemas seguros para videoconferencia, especialmente útil post-2020). También se dispone de una

intranet con foros y un portal llamado Colabora (Junta) para compartir documentos internamente.

- Aplicaciones de apoyo clínico: Como parte de la estrategia de salud digital, hay accesos a bases de datos clínicas (GuíaFarmacoterapéutica online, UpToDate, etc.), sistemas de ayuda a la decisión (por ejemplo, módulos de prescripción que alertan de interacciones), y la Red de conocimiento (Portal Picuida para enfermería, etc.), todas accesibles desde el puesto digital.
- Ayuda e información interna: El SAS ha implementado AyudaDIGITAL, un servicio integral de soporte TIC. En cada puesto hay instalada la aplicación AyudaDIGITAL Escritorio que permite consultar manuales, notificaciones TIC (por ejemplo "cambiar contraseña antes de que caduque") y abrir tickets de soporte directamente. También está la app de AyudaDigital y un chatbot (AYDI) por WhatsApp para asistencia informática. Esto facilita al profesional resolver problemas técnicos rápidamente o aprender a usar alguna herramienta nueva.

Buenas prácticas en el uso del puesto digital:

Para que toda esta tecnología sea útil y segura, es esencial seguir unas pautas de utilización responsable, muchas de las cuales se derivan del Código de Conducta TIC (ver sección 5). Algunas recomendaciones y obligaciones clave son:

- Uso profesional exclusivo: Los equipos y cuentas corporativas del SAS deben emplearse solo para fines laborales. Está prohibido instalar software no autorizado o usar el ordenador del trabajo para asuntos personales (navegar por webs no relacionadas, redes sociales privadas, etc.). Esto evita riesgos de malware y fugas de datos. Del mismo modo, no se deben conectar dispositivos externos no provistos por el SAS (ej. USB personales) sin autorización.
- Protección de credenciales: Cada usuario es responsable de sus contraseñas y certificados. Deben mantenerse confidenciales (no anotarlas en papel a la vista, no compartirlas con compañeros). Al terminar la jornada o ausentarse, se debe cerrar sesión o bloquear el equipo, para que nadie pueda usarlo indebidamente. Nunca se debe dejar una historia clínica abierta en pantalla sin supervisión de un profesional.
- Atención al correo y webs: En la navegación por Internet y uso del email corporativo, se debe actuar con precaución. No abrir correos sospechosos ni pinchar en enlaces dudosos (phishing), no descargar archivos de fuentes no confiables. El SAS filtra spam, pero el mejor filtro es el propio usuario alertado. Asimismo, evitar visitar sitios web no permitidos (el filtrado web corporativo bloquea muchos por seguridad).
- Respeto a la confidencialidad: Al trabajar con datos de pacientes, hay que extremar el cuidado: no dejar informes impresos olvidados en impresora, no comentar datos clínicos en pasillos o fuera del ámbito profesional, y asegurarse de que cualquier copia digital de datos esté en entornos seguros (por ejemplo, si se extrae información para sesiones clínicas, anonimizarlas). Cualquier documento con datos personales debe guardarse en las carpetas de red corporativas (que están cifradas y respaldadas) y no en el escritorio local, para que esté protegido.
- Mantenimiento y reportes: Permitir que se apliquen las actualizaciones de sistema cuando se

- programan (a veces se avisa al usuario de reiniciar). Si se detecta una anomalía (computadora muy lenta, ventana extraña, posible virus), reportarlo inmediatamente a Soporte (AyudaDigital) para que revisen. Igual ante cualquier incidente de seguridad (p.ej. se envió un email con datos al destinatario equivocado) hay que notificarlo sin miedo; se busca corregir, no culpar, salvo negligencias graves.
- Teletrabajo seguro: Si en situaciones excepcionales se trabaja desde fuera (como ocurrió durante picos pandémicos), usar únicamente los equipos corporativos provistos con VPN y no compartirlos con familiares. Mantener conversaciones de video o audio confidenciales en entornos privados, evitando asistentes tipo Alexa encendidos cerca, etc.
- Ergonomía digital: Aunque no es ciberseguridad, es parte del puesto saludable: hacer pausas visuales cada cierto tiempo, tener una correcta postura con la computadora, ajustar la iluminación. Un profesional que oposita debe recordar que la salud digital incluye cuidarse a uno mismo en el uso de las TIC.

El SAS provee formación continua en muchas de estas prácticas a través de cursos on-line (IECS, etc.) y manuales disponibles en la intranet. Al final, el puesto digital bien aprovechado permite que el sanitario tenga al alcance de un clic toda la información y herramientas para atender mejor al paciente, reducir cargas burocráticas (gracias a recetas electrónicas, peticiones online, etc.) y colaborar eficientemente con otros profesionales. Saber manejar con soltura los sistemas corporativos mencionados (Diraya, etc.) es hoy tan importante para un buen profesional sanitario como sus conocimientos clínicos, y por ello en las oposiciones cada vez se incluyen más temas relacionados con las TIC.

4. Código de Conducta TIC del SAS

El Código de Conducta en el uso de las TIC es un documento normativo que establece las reglas de comportamiento que deben seguir los empleados públicos de la Junta de Andalucía (y por tanto del SAS) al utilizar los recursos tecnológicos proporcionados. Este código, de obligado cumplimiento para todo el personal, fue aprobado por la Junta en 2020 (Resolución de 22 de octubre de 2020 de la Secretaría General para la Administración Pública), y adaptado en el SAS mediante acuerdo de su Comité de Seguridad TIC en enero de 2022. Su finalidad es promover un uso ético, seguro y responsable de las TIC, detallando qué se considera uso correcto o incorrecto, y cuáles son las responsabilidades (derechos, deberes y sanciones) asociadas.

Algunos puntos esenciales del Código de Conducta TIC son:

- Ámbito de aplicación: Abarca a todos los profesionales públicos, independientemente de su puesto o categoría, y aplica a todos los recursos TIC de la organización: equipos informáticos, redes, sistemas de información, correo electrónico, Internet corporativo, aplicaciones, dispositivos móviles corporativos, etc. Es decir, siempre que usemos medios del SAS o tratemos datos del SAS, debemos seguir estas normas.
- Obligaciones del usuario: El empleado debe utilizar los medios solo para fines profesionales autorizados, proteger las credenciales de acceso, respetar la confidencialidad de la información, cumplir las medidas de seguridad establecidas (ej: cifrado, bloqueo de sesión),

y notificar incidentes o vulneraciones de las que tenga conocimiento. También incluye el deber de formarse e informarse sobre las políticas TIC vigentes (el SAS facilita cursos, y se espera que el profesional dedique tiempo a conocer el código). En definitiva, trata de inculcar que cada usuario es responsable de sus acciones en el ciberespacio corporativo.

- Usos permitidos y prohibidos: El código describe qué se entiende por uso correcto. Por ejemplo, permite lógicamente el uso de herramientas TIC para las tareas asignadas, comunicación interna, formación relacionada con el puesto, etc. En cambio, prohíbe expresamente usos indebidos como: instalar software no autorizado o con licencias no verificadas, usar el correo para difundir contenidos ilícitos o inapropiados, navegar por sitios web de juego, pornografía o contrarios a la dignidad, realizar actividades privadas lucrativas usando recursos públicos, descargar o almacenar información personal ajena al trabajo, etc. También se considera uso indebido acceder a datos o sistemas para los que uno no esté autorizado (por curiosidad o cualquier fin). Un ejemplo grave sería consultar la historia clínica de un paciente sin relación asistencial: eso atenta contra el deber de confidencialidad y está terminantemente prohibido, salvo que medie una solicitud justificada (investigación autorizada, petición del propio paciente, etc.). El código subraya que incluso disponer de permisos de acceso no legitima moralmente su uso si no está dentro de las funciones (principio de finalidad).
- Protección de datos personales: Dado que gran parte de la información tratada son datos personales (muchos, sensibles), el código recuerda el deber legal de secreto profesional y cumplimiento de LOPDGDD/RGPD. Cualquier vulneración puede tener consecuencias disciplinarias y sanciones por la Agencia de Protección de Datos. Recomienda siempre seguir el principio de mínima exposición: por ejemplo, al enviar un email con datos de salud, verificar que va cifrado o usar soluciones internas seguras; no utilizar WhatsApp u otras vías informales para transmitir datos clínicos (salvo en herramientas corporativas cifradas, si existieran, y con consentimiento).
- Uso de herramientas corporativas: Se destaca que existen canales oficiales para la comunicación y compartición de información, y deben usarse en vez de alternativas externas. Por ejemplo, para enviar documentos, se debe usar el correo corporativo (nunca nuestro Gmail personal) o la herramienta de intercambio seguro proporcionada; para videoconferencia, las plataformas aprobadas por la institución (no videollamadas por apps no autorizadas con pacientes, por seguridad).
- Registro de actividades: El código informa de que, para velar por la seguridad, la Administración puede realizar controles y registros de la actividad en los sistemas, siempre respetando la legalidad (principio de proporcionalidad). Esto significa que hay logs de accesos a historias clínicas (y se revisan periódicamente buscando accesos indebidos) y que el uso de Internet/correo podría ser monitorizado en caso de sospecha de mal uso. No es espionaje indiscriminado, pero sí un aviso de que la red corporativa no es un ámbito privado del todo, sino un recurso público sujeto a supervisión.
- Medidas disciplinarias: El código describe las consecuencias de incumplir sus preceptos. Dependiendo de la gravedad, un uso inadecuado puede constituir falta disciplinaria leve, grave o muy grave, conforme al régimen disciplinario del empleado público. Por ejemplo, romper la confidencialidad de datos de salud es típicamente una falta muy grave (difusión de secretos) que puede conllevar sanciones severas: desde suspensión de empleo y sueldo, hasta el despido (en el personal estatutario del SAS, la separación del servicio, regulada en la Ley 55/2003). Menos grave sería un uso esporádico personal de Internet que se corrija con un

aviso (tirón de orejas), pero si es reiterado puede escalar. El código remite al Estatuto Marco del personal estatutario (Ley 55/2003) y al EBEP (Texto Refundido de la Ley del Empleado Público) en cuanto a tipificación de faltas y sanciones. Además de lo administrativo, ciertos abusos pueden acarrear responsabilidad civil o penal: p. ej., acceder sin autorización a datos médicos vulnerando medidas de seguridad podría encajar en el delito de descubrimiento y revelación de secretos (art. 197 CP). Por eso el código insiste: "¡No te la juegues!", el uso irregular o ilegal de los recursos TIC es un delito y conllevará exigencia de responsabilidades.

- Referencias legales y coordinación: El Código de Conducta TIC complementa otras normas internas y leyes ya mencionadas (LOPDGDD, ENS, etc.), actuando como una guía práctica. Su aprobación en 2020 lo convierte en relativamente reciente, adaptado a la evolución tecnológica (por ejemplo, contempla temas como el teletrabajo y la desconexión digital, o la protección de la identidad digital del empleado). Asimismo, se alinea con las políticas nacionales de eGobierno y con iniciativas de ciberseguridad (INCIBE, CCN). En su difusión, la Junta ha empleado incluso formatos amenos (vídeos explicativos, infografías) para que cale su contenido.

En suma, el Código de Conducta TIC es el marco deontológico-tecnológico que guía a los trabajadores del SAS en el uso de la tecnología. Para un opositor, es importante no solo conocer su existencia sino comprender su espíritu: busca asegurar que la transformación digital se haga con ética, respeto y responsabilidad. Esto redunda en proteger al ciudadano (sus datos, su privacidad) y también al profesional (evitándole incurrir en faltas sin quizá saberlo). Por ello, es recomendable leer el código completo disponible en la web corporativa y tenerlo siempre presente al desempeñar funciones en el SAS.

5. Normativa actual aplicable

La actividad del SAS en materia de TIC y manejo de información está sujeta a múltiples normas vigentes, de diversos niveles (europeo, estatal, autonómico e interno). A continuación se listan las principales leyes, reglamentos y disposiciones que un profesional sanitario debe conocer, al menos conceptualmente, al trabajar en el SAS:

- Reglamento (UE) 2016/679 General de Protección de Datos (RGPD): Marco europeo de protección de datos personales, aplicable desde mayo de 2018. Establece obligaciones al SAS como responsable de datos de salud (licitud del tratamiento, consentimiento informado, medidas de seguridad apropiadas, evaluación de impacto, notificación de brechas) y reconoce derechos a los ciudadanos (acceso, rectificación, supresión, portabilidad, limitación y oposición al tratamiento de sus datos). Es directamente aplicable y supuso un avance unificador en toda la UE.
- Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD): Norma española que complementa al RGPD. Entre otras cosas, especifica aspectos como el tratamiento de datos de fallecidos, regula la figura del Delegado de Protección de Datos en organismos públicos (el SAS tiene el suyo), contempla derechos digitales (ej. derecho a la desconexión digital de los empleados, muy relevante en salud para respetar descansos) y articula el régimen sancionador nacional en protección de datos.

- Ley 41/2002, básica de Autonomía del Paciente: Norma fundamental en sanidad que, además de regular el consentimiento informado y otros derechos del paciente, define el régimen jurídico de la historia clínica. Obliga a custodiarla con confidencialidad, da derecho al paciente a acceder a su propia información y establece que el acceso de terceros solo puede darse por razones justificadas (asistenciales, epidemiológicas, judiciales...). Esta ley junto con las de protección de datos configuran el núcleo de la privacidad en salud.
- Ley 14/1986 General de Sanidad y Ley 44/2003 de Ordenación de las Profesiones Sanitarias: Marcos generales sanitarios. La Ley General de Sanidad consagra el derecho a la información sanitaria y el deber de secreto profesional. La Ley de Profesiones (LOPS) reitera esos deberes de sigilo y buen uso de la información por parte de los sanitarios colegiados. Ambas establecen bases éticas y legales sobre cómo tratar datos sensibles.
- Ley 55/2003, del Estatuto Marco del personal estatutario: Rige las relaciones laborales del personal sanitario estatutario (la gran mayoría en SAS). Contiene un régimen disciplinario (capítulo IV) que tipifica infracciones muy graves, graves y leves. Muchas de ellas se relacionan con TIC: por ejemplo, la violación del secreto profesional o uso indebido de información confidencial es falta muy grave; el uso de medios públicos para fines particulares es falta grave, etc. También obliga a cumplir las normas internas (como el código TIC). Conocer esta ley es crucial para saber a qué atenernos si quebrantamos las reglas.
- Leyes 39/2015 y 40/2015 de Procedimiento Administrativo y Régimen Jurídico: Impulsan la Administración electrónica. La Ley 39/2015 establece el derecho de la gente a relacionarse electrónicamente con las Administraciones y obliga a estas a ofrecer registros electrónicos, notificaciones telemáticas, archivo electrónico de expedientes, etc. El SAS, como entidad administrativa, se ha adaptado a ello con su sede electrónica, firma digital en expedientes, etc. La Ley 40/2015, por su parte, en materia TIC ordena la interoperabilidad y la seguridad (mencionado ENS) y promueve la cooperación interadministrativa vía medios electrónicos (por ej., intercambio de datos entre SAS y otras consejerías en vez de pedir documentos al ciudadano). Estas leyes explican medidas como RECSAS (registro electrónico SAS) y portales como ClicSalud+ (oficina virtual).
- Esquema Nacional de Seguridad (ENS): Regulación técnica aprobada por RD 3/2010, modificado por RD 311/2022, que es de obligado cumplimiento en SAS. Marca las líneas de defensa y gestión de la seguridad TIC en entes públicos. Incluye requisitos como tener una política de seguridad aprobada, análisis de riesgos regulares, clasificación de sistemas, medidas concretas (control de accesos, protección de instalaciones, cifrado, monitorización, etc.) según nivel de criticidad. El SAS tiene muchos sistemas de nivel Alto (por datos de salud), lo que implica medidas rigurosas. El ENS también exige concienciación y formación (de ahí guías como la que vimos) y auditorías bienales de seguridad.
- Esquema Nacional de Interoperabilidad (ENI): Aprobado por RD 4/2010, obliga a usar estándares abiertos o interoperables, formatos comunes de datos, y mantener la historia clínica interoperable. Gracias a esto, SAS participa en la Historia Clínica Digital del SNS (HCDSNS), compartiendo datos con otras CCAA, y puede integrar sistemas de distintos fabricantes. El ENI influye en Diraya (usa estándares HL7, etc.), en la firma de documentos (usa formatos XAdES, etc.), y en la preservación a largo plazo de los documentos electrónicos sanitarios.
- Normativa autonómica (Junta de Andalucía): Además del citado Decreto 1/2011 de

seguridad TIC, hay otras normas andaluzas relevantes: la Ley 1/2014 de Transparencia Pública de Andalucía (afecta a la publicación de datos y reutilización, pero con cuidado de no exponer datos personales), el Decreto 622/2019 de Administración electrónica (desarrolla en Andalucía la Ley 39/2015, dando base a cosas como notificaciones electrónicas en salud, receta electrónica interoperable, etc.), y normas específicas de SAS como el Plan de Sistemas de Información Sanitarios vigente o instrucciones internas sobre protección de datos (el SAS tiene su propio Comité de Protección de Datos con procedimientos, p.ej. evaluación de impacto en proyectos de Big Data sanitario).

- Código de Conducta TIC (Resolución 22/10/2020): Ya desarrollado en la sección 5, es normativa interna autonómica que aplica en SAS. Recalcamos su importancia normativa aquí: su aprobación formal lo hace vinculante, y complementa lo dispuesto en ENS y leyes de función pública. Es la referencia para juzgar qué usos de TIC son aceptables en el SAS.
- Convenios y estándares internacionales: Por completitud, mencionamos que existen normas ISO/UNE de calidad y seguridad de la información (ISO 27001 para SGSI, ISO 27799 específica de seguridad de información de salud, etc.) que, aunque no obligatorias por ley, son guías seguidas por el SAS para autoevaluarse. Igualmente, el Reglamento UE 910/2014 (eIDAS) sobre identificación y firma electrónica regula el uso de certificados que aplicamos (tarjetas criptográficas de empleados, certificados de sello de organismo en documentos clínicos).

Toda esta normativa conforma un marco legal robusto que busca garantizar que la transformación digital del SAS se haga protegiendo derechos fundamentales (como la privacidad) y brindando seguridad jurídica a los procesos electrónicos. Para los opositores, es importante conocer al menos las siglas y el ámbito de cada norma, ya que en exámenes suelen preguntar, por ejemplo, qué ley regula la protección de datos de salud o qué es el ENS. Además, en la práctica profesional, estas leyes se traducen en políticas concretas del centro de trabajo: por ejemplo, gracias a ellas sabemos que un paciente puede solicitar su historia (Ley 41/2002) o que no podemos instalar software pirata (Código TIC y LPI). Estar al día en normativa es parte del ejercicio responsable de la profesión en el siglo XXI.

6. Conclusión práctica orientada a opositores

En esta exposición hemos recorrido los elementos clave de las TIC en el SAS: desde los sistemas corporativos que usamos a diario (Diraya, ClicSalud+, etc.), pasando por la importancia de la ciberseguridad y las normas de buen uso (puesto digital y código de conducta), hasta el entramado legislativo que sustenta todo. Para finalizar, conviene resaltar algunas ideas prácticas y consejos de estudio para los opositores sanitarios:

- Integrar conocimiento teórico con situaciones reales: No se trata solo de memorizar nombres de sistemas o leyes, sino de entender cómo impactan en el trabajo. Por ejemplo, imaginar el flujo completo de atención a un paciente en consulta: cita asignada vía Diraya, registro de antecedentes en historia electrónica, prescripción por receta XXI, entrega de informe que el paciente luego ve en ClicSalud+, etc. Esto ayuda a conectar conceptos y recordarlos mejor en el examen. Asimismo, reflexionar sobre casos reales de seguridad (un compañero curioseó un historial y fue sancionado; un virus paralizó un hospital en otra región...) nos conciencia de la relevancia de estos temas.

- Mantenerse actualizado: El ámbito TIC evoluciona rápido. En el SAS, lo visto a partir de 2022 incluye nuevas versiones de sistemas, la App unificada Salud Andalucía, mejoras en ciberseguridad, etc. Es crucial revisar las últimas novedades antes del examen. Fuentes oficiales como la web del SAS (sección de profesionales > sistemas de información), boletines oficiales (BOJA, BOE) y comunicados de la Consejería son referencias válidas para encontrar datos actualizados (por ejemplo, si se implantó un nuevo módulo o si cambió alguna normativa). Nosotros hemos incorporado información al día hasta 2025, pero siempre conviene verificar cambios de último momento.
- Estructurar la respuesta como se ha hecho aquí: En una prueba escrita u oral, organizar la respuesta con claridad es fundamental. Usar epígrafes similares a los presentados (Introducción, sistemas, ciberseguridad, puesto digital, normativa, conclusión) ayuda al tribunal a ver que se ha cubierto todo el temario solicitado. Emplear listados (por ejemplo, enumerar 4-5 sistemas con sus funciones) da una imagen de dominio sintetizado. Además, citar alguna referencia normativa o plan oficial da rigor (mencionar RGPD, Estatuto Marco o Código TIC con su fecha muestra que conocemos la base legal).
- Priorizar la aplicabilidad para cualquier perfil: Dado que el tema es común a distintas categorías sanitarias, es bueno mencionar ejemplos que atañen tanto a enfermería, médicos, TCAE, fisioterapeutas, etc. Las TIC nos afectan a todos: el enfermero registra en Diraya cuidados de enfermería, el médico prescribe en Receta XXI, el TCAE puede gestionar petición de materiales vía SIGLO, el fisioterapeuta consulta pruebas en PACS, etc. Incluir esa visión plural (como hemos intentado) hará que cualquier opositor se sienta identificado y entienda que este conocimiento es transversal.
- Ética y responsabilidad profesional: Un opositor no debe ver las TIC solo como un examen teórico, sino como un compromiso práctico. El Código de Conducta TIC y la normativa de confidencialidad deben asumirse desde ya, incluso al estudiar. Por ejemplo, si se usan casos reales para aprender, hay que anonimizar la información. Al aprobar la oposición y tomar posesión, se firmará seguramente un compromiso de cumplir estas normas. Demostrar en la oposición una actitud consciente de la privacidad y la seguridad (por ejemplo, mencionando la importancia del secreto profesional digital) puede sumar puntos, pues muestra madurez profesional.

En conclusión, el SAS es puntero en la implantación de las TIC sanitarias, lo que redunda en beneficios para pacientes y profesionales. Temas como Diraya o la ciberseguridad no son "complementarios" sino centrales en el día a día asistencial. Un opositor bien preparado en este ámbito será capaz de integrarse rápidamente en la dinámica de trabajo actual, usando eficientemente los sistemas corporativos y respetando los protocolos de seguridad y conducta. Esperamos que este tema, desarrollado de forma clara y rigurosa, sirva de guía de estudio y referencia rápida. La transformación digital del SAS es una realidad y, como futuros integrantes del mismo, nuestra responsabilidad es conocerla y contribuir a ella con un uso adecuado de la tecnología, manteniendo siempre el foco en la mejora de la atención al paciente y en la protección de sus derechos.

7. Referencias Bibliográficas:

- **Consejería de Salud y Consumo, Junta de Andalucía.** (2022). AyudaDIGITAL – Manual de usuario y recursos TIC para profesionales. Junta de Andalucía. https://www.juntadeandalucia.es
- **Consejería de Salud y Familias, Junta de Andalucía.** (2020, 22 de octubre). Resolución de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de los sistemas de información y comunicaciones de la Administración de la Junta de Andalucía. Boletín Oficial de la Junta de Andalucía, (214). https://www.juntadeandalucia.es/eboja
- **Consejería de Salud y Familias, Servicio Andaluz de Salud.** (2023). Guía de ciberseguridad para nuevos profesionales del SAS. Junta de Andalucía. https://www.sspa.juntadeandalucia.es
- **Consejería de Salud y Familias, Servicio Andaluz de Salud.** (2024). Portal Diraya: Historia de Salud Digital de Andalucía. Junta de Andalucía. https://www.sspa.juntadeandalucia.es/servicioandaluzdesalud
- **Servicio Andaluz de Salud.** (2021). ClicSalud+: Oficina virtual de salud del SAS. Junta de Andalucía. https://www.clicsalud.es
- **Servicio Andaluz de Salud.** (2025). Sistemas corporativos de información en el SAS: GERHONTE, SIGLO, GIRO y SUR. Blog Innovación en Tecnología Sanitaria. https://innovacionentecnologiasanitaria.com