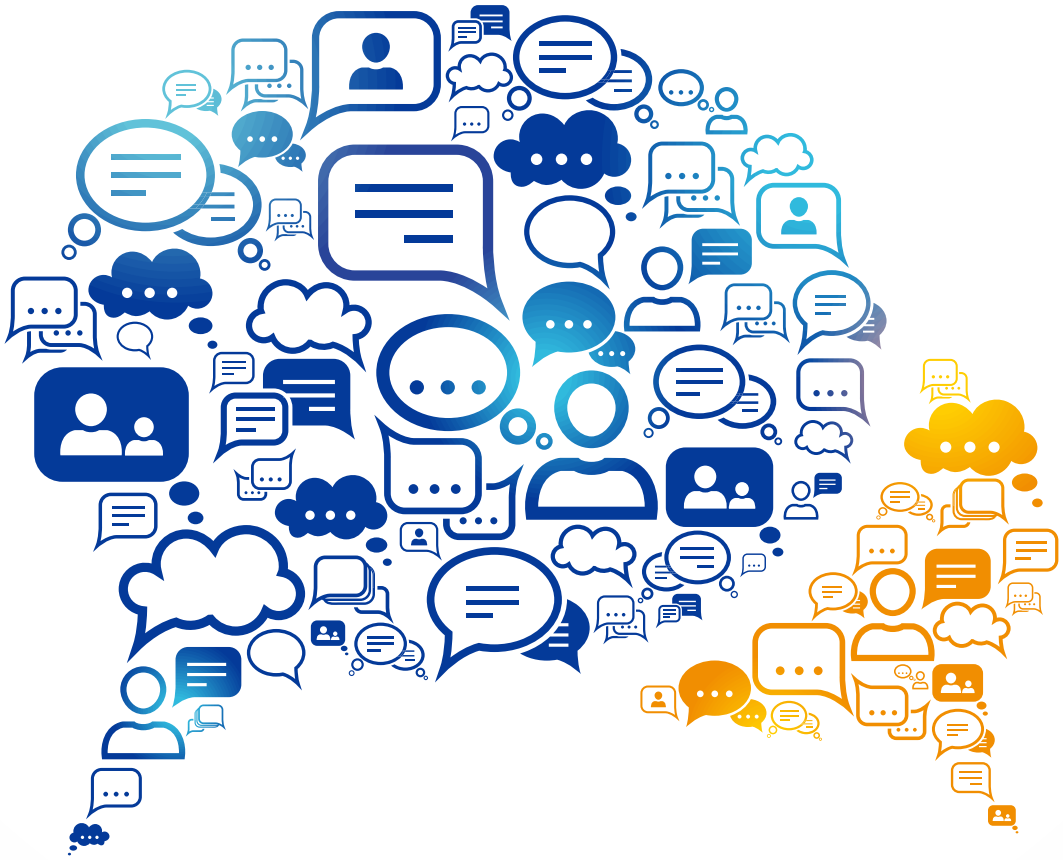
HERRAMIENTAS DE SOPORTE / ASISTENCIA REMOTA EN TIEMPO REAL EN EL ÁMBITO DE LA SALUD

GUÍA TÉCNICA PARA LA INSTALACIÓN Y USO SEGURO Y EFICIENTE DE HERRAMIENTAS DE SOPORTE / ASISTENCIA EN TIEMPO REAL EN CENTROS HOSPITALARIOS



SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Abbott

Edita
Sociedad Española de Informática y Salud

SEIS
Con la colaboración de Abbott

Edición julio 2024

DL LE 363-2024

CONTENIDO

Antecedentes

Antecedentes

En el ecosistema sanitario español, y casi mundial, se da con cierta frecuencia la necesidad que tiene el personal facultativo de tener asistencias muy especializadas en ciertos tipos de intervenciones.

Este tipo de necesidades representan un reto ante el actual panorama de inseguridad en el entorno TIC que nos rodea y más en un área tan sensible como la salud.

Por ello, este documento borrador trata de recopilar buenas normas y/o recomendaciones mínimas que deberían implementar los centros y los servicios clínicos que deseen estas asistencias, para mantener un mínimo de seguridad. Estas recomendaciones han sido elaboradas por reconocidos asesores en el área de ciberseguridad de los distintos sistemas regionales de salud que conforman el espacio sanitario español.

Para realizarlo, los integrantes del grupo se han basado en las recomendaciones del Esquema Nacional de Seguridad (ENS), y se han ido analizando cada uno de los aspectos donde se pueden aplicar los epígrafes.

Como metodología, se ha tomado la base que expone el propio ENS, de "abrir" la seguridad de la forma más restrictiva y, por dicho motivo, de entre la matriz propuesta se hace la recomendación sobre la propuesta más restrictiva a falta de una revisión posterior.

Solo se han desarrollado las variables que los expertos han considerado, por lo que aquellas que no aparezcan reflejadas, no es por omisión, simplemente no aplican.

Para aplicar las recomendaciones siguientes hay que observar el entorno donde se desarrollarán, ya que nos encontramos dependiendo del desarrollo tecnológico, e incluso de las personas, situaciones muy diferentes. Los escenarios más comunes que nos encontramos son:

1. La acción por parte del proveedor no requiere de conexión a los SSII del centro sanitario ni a la red
2. La acción por parte del proveedor requiere de conexión a los SSII del centro sanitario y por tanto también a la red.
3. La acción por parte del proveedor no requiere de conexión a los SSII del centro sanitario, pero sí a la red para utilizarla de transporte.

En aquellos escenarios donde exista necesidad de conexión a la red con acceso a datos de los SSII deberían realizarse, al menos, los siguientes actos:

- análisis de riesgos
- evaluación de impacto
- construcción de un entorno seguro con herramientas que permitan proteger extremo a extremo la veracidad y confidencialidad de las comunicaciones, cumpliendo siempre los requerimientos mínimos del ENS.

En aquellos escenarios donde la intervención de la empresa no requiera ninguna interactuación con la red del centro, las actuaciones descritas se deberán limitar a la protección de datos, toda vez que se entienda que el **paciente ha firmado un consentimiento informado** para cumplir el RGPD si aplica.

En este caso, una solución podría ser tener un segmento de red aislado, desde el armario RITI del centro hasta el repartidor, bien por cable o por fibra óptica dependiendo de las distancias, que dé cobertura a las áreas que se deseen proveer de este acceso. En dicho armario, podría conectarse un pequeño conmutador de red enlazado con el parcheo de las tomas y de esa manera se aislaría el transporte de la señal en capa 1 y no habría acceso a datos de ningún tipo. Esta solución debería ser proporcionada por el centro sanitario en cuestión, como un elemento facilitador y de "polo de atracción" para que las empresas que den este tipo de coberturas perciban la colaboración institucional y sus actos se incrementen, no siendo onerosa para el presupuesto del centro y teniendo todas las medidas de seguridad a nivel físico.

Desarrollo

Desarrollo

A continuación, vamos a ir analizando cada uno de los epígrafes. Cabe reseñar que estas acciones se han marcado por uno de los expertos con el nivel más restrictivo, que es el ALTO.

Marco organizativo

En este apartado los expertos han analizado la situación y entienden que la parte del marco organizativo debe estar instaurada en las organizaciones como algo natural y, por tanto, no debería tratarse de marcar el nivel, pero hay una puntualización sobre los distintos aspectos.

1. **POLÍTICA DE SEGURIDAD**
   Es una obligación normativa y, como tal, debe ser pública, como base y preámbulo para este tipo de conexiones con empresas externas.

2. **NORMATIVA DE SEGURIDAD**
   Deberá existir la documentación donde se especifique el uso correcto de equipos, servicios e instalaciones y lo que se considerará uso indebido. Además, deberá estar establecida la responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

3. **PROCEDIMIENTOS DE SEGURIDAD**
   Existirá una documentación que detalle de manera clara y concisa, cómo se debe operar con el sistema de información en cuestión. En concreto:
   - el control de acceso
   - almacenamiento de la información
   - copias de la información
   - identificación de soportes
   - modos y métodos de transmisión telemática
   - cualquier otra actividad relacionada con el acceso a dicha información

4. **PROCESO DE AUTORIZACIÓN**
   Se establecerá un proceso formal que cubra los accesos al centro, con las debidas autorizaciones del responsable del tratamiento de la información, del responsable de seguridad y del responsable del sistema,

además del "cliente" interno que solicita la asistencia. Para ello deberán adecuarse a los estándares de la política de seguridad los siguientes aspectos:

- uso de instalaciones del centro
- entrada de equipos y aplicaciones del proveedor
- establecimiento de comunicaciones externas
- uso de cualquier dispositivo móvil
- contratación de terceras empresas

Como se ha indicado, el nivel de severidad a aplicar a estas medidas es ALTO.

Marco operacional

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

PLANIFICACIÓN

1. Análisis de riesgos

   Elemento indispensable que será abordado tanto por el centro sanitario como por la empresa que desea realizar la conexión externa. El nivel de severidad aplicado es alto y el análisis deberá ser formal.

2. Arquitectura del sistema

   Se detallará desde el punto de vista de redes y sistemas, incluyendo el programa/aplicativo/plataforma que usará la empresa. Se exigirá además una declaración responsable de las medidas de seguridad aplicadas a nivel tanto de arquitectura como de puesto de trabajo, acorde con el nivel de severidad que será ALTO.

3. Dimensionamiento/gestión de la capacidad

   Nos parece importante que, con carácter previo a la puesta en explotación, se realice un estudio que cubra los siguientes aspectos:

   - necesidades de comunicación
   - necesidades de personal: cantidad y cualificación profesional
   - necesidades de instalaciones y medios auxiliares

   Es una medida donde no hay unanimidad y, por tanto, a debatir con posterioridad. Se postula siempre en nivel más restrictivo y por tanto será de carácter MEDIO.

4. Componentes certificados

   Se deberá utilizar el máximo número de certificaciones. Habrá que especificar las mínimas. El nivel de severidad es ALTO.

CONTROL DE ACCESO

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.

Como se está planteando, la interconexión de sistemas en los que la identificación, autenticación y autorización tienen lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, las medidas de segu-

ridad locales se acompañarán de los correspondientes acuerdos de colaboración. Estos delimitarán los mecanismos y procedimientos para la atribución y ejercicio efectivo de las responsabilidades de cada sistema.

1. Identificación

   Nivel de severidad ALTO. Los accesos a los sistemas internos deben ser nominales. El sistema deberá conservar un registro de auditoría de accesos al sistema que identifique nominalmente a la persona que ha accedido a los sistemas internos.

2. Requisitos de acceso

   Medida de nivel ALTO. Se deberá realizar un documento indicando dichos requisitos. Se dispondrá de soluciones que permitan establecer controles de acceso a los dispositivos en función de la política de seguridad de la organización. Se establecerá el mínimo privilegio posible. Si es VPN, mediante configuración de ACLs; si es vía Internet, URLs completamente identificadas, etc.

3. Segregación de funciones y tareas

   Existe discrepancia entre los asesores. Se aplica el nivel más restrictivo, nivel ALTO. Se deberán identificar los distintos perfiles de acceso. Las personas que autorizan y controlan el uso del sistema deberán ser distintas.

4. Proceso de gestión de derechos de acceso

   Si aplica mínimo privilegio, la política de acceso remoto es responsabilidad del hospital. Existe discrepancia entre los asesores, se establece el nivel de severidad más restrictivo, nivel ALTO.

5. Mecanismo de autenticación

   Doble factor de autenticación. Política de contraseñas. Acceso tras la autorización de una persona de la organización (vía herramientas PAM o teniendo que autorizar la conexión en la solución de acceso remoto que proporciona el proveedor). Medidas de nivel MEDIO con medidas de refuerzo.

EXPLOTACIÓN

1. Inventario de activos

   Se especificará un inventario del material a usar identificando a su responsable. En este punto hay discrepancia, siendo el nivel más elevado el ALTO.

2. Configuración de seguridad

   Nivel ALTO indicado por todos los expertos. En este epígrafe se revisarán los equipos para cumplir con las políticas de seguridad, eliminando cuentas anónimas, aplicando la mínima funcionalidad, estando la maquina en un parcheado adecuado según la política de seguridad del centro, incluyendo los antivirus y otras medidas que eleven el marco de seguridad existente.

3. Gestión de la configuración de seguridad

   La plataforma responderá al principio de "mínimo privilegio" tanto en el inicio del proyecto, durante la intervención a realizar y al recoger el aparataje, cualquier variación, supondría una reevaluación. Casi todos los expertos lo han notificado como severidad ALTA.

4. Mantenimiento y actualización de seguridad

La plataforma estará actualizada a los mayores niveles de parcheo y estos deberán cumplir las garantías de seguridad del momento actual. El nivel de seguridad es MEDIO con refuerzos obligatorios.

5. Gestión de cambios

Se mantendrá un control continuo de los cambios realizados en los dispositivos. El nivel de seguridad es MEDIO con refuerzos obligatorios.

6. Protección frente a código dañino

Se establecerán mecanismos de prevención y reacción frente a cualquier código que pueda ser inyectado a través de la plataforma del proveedor de servicio. Estos mecanismos deberán estar actualizados con sus últimos parches de actualización. El nivel de seguridad es MEDIO con refuerzos obligatorios.

7. Gestión de incidentes

Se tendrá por parte del centro, de un proceso extremo a extremo para hacer frente a los incidentes que provoquen eventos de seguridad, teniendo especial atención en que es un servicio que presta un tercero en régimen de concesión, encomienda de gestión o contrato. Las medidas de seguridad se corresponderán con las de la administración pública de origen y se ajustarán al Esquema Nacional de Seguridad. El nivel de severidad es ALTO, aunque existe una discrepancia.

8. Registro de la actividad

Se realizará un registro de auditoría con, al menos, la siguiente actividad:

a. identificador de usuario
b. entidad que presta el servicio
c. fecha y hora del evento
d. sobre qué información se ha producido el evento
e. tipo de evento
f. resultado del evento (fallo o éxito).

7. Registro de la gestión de incidentes

Nivel de severidad ALTO, por lo que se deberán realizar, al menos, todas las actuaciones derivadas del posible evento de seguridad. Se registrarán con especial cuidado aquellas acciones y variables de entorno susceptibles de usarse en un entorno formal que conlleve algún tipo de sanción.

8. Protección de claves criptográficas

Las claves criptográficas estarán protegidas durante toda la actuación de la empresa, tanto a nivel local como remoto. Nivel ALTO con discrepancias.

RECURSOS EXTERNOS

Epígrafe especialmente de impacto en este tipo de actuaciones, entendiendo que, aunque haya un acuerdo o contratación de servicios, las responsabilidades del centro no se transfieren. Deberá establecerse un ANS para posibles incidencias. En este epígrafe no hay tampoco unanimidad, pero el nivel de severidad se establece en ALTO.

1. Contratación y acuerdos de nivel de servicio
   Se establecerá, con anterioridad a las actuaciones, un acuerdo de nivel de servicio, atendiendo a la naturaleza del servicio que proporciona la empresa externa. Nivel de severidad ALTO.

2. Gestión diaria
   Se establecerá una métrica para comprobar el correcto uso del servicio proporcionado.

3. Protección de la cadena de suministros
   Tanto el centro como el proveedor deben disponer de medidas de actuación en caso de errores en la cadena de suministro del servicio proporcionado. Necesidad de plan de contingencia a evaluar. El proveedor pasa a ser parte de la cadena de suministro. Nivel de severidad ALTO.

4. Interconexión de sistemas
   La interconexión necesita una autorización previa del responsable del tratamiento de la información. Deberá documentarse detalladamente la forma de conexión y la información que fluirá. Si esa demanda del responsable del tratamiento se le pide al proveedor de la interconexión, hay que entender que los permisos los da el centro sanitario/Servicio regional de Salud. El nivel de seguridad es MEDIO con refuerzos obligatorios.

SERVICIOS EN LA NUBE

Perfil de cumplimiento nivel MEDIO. No se incluye información de cumplimiento de la nube del proveedor ante ENS, debería cumplir las guías del CCN-STIC.

1. Protección de servicios en la nube

   Cumplimiento de las guías del CCN-STIC sobre este tipo de servicio.

CONTINUIDAD DEL SERVICIO

1. Análisis de impacto

   Se deberá prever el impacto de una interrupción durante un periodo de tiempo indeterminado, identificando los elementos críticos que se necesitan. Nivel de severidad ALTO.

2. Plan de continuidad

   Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Nivel ALTO de severidad.

3. Pruebas periódicas

   No existe unanimidad y no se entiende en este contexto. Las pruebas periódicas están indicadas para detectar debilidades en el plan de acción ante desastre. En este caso podría ser una brecha de intrusión o un caballo de Troya o cualquier evento que pueda venir de la interconexión. Nivel ALTO.

4. Medios alternativos

   Deberá estar prevista en el plan de contingencia la alternativa para realizar la continuidad del servicio. Nivel ALTO de severidad.

MONITORIZACIÓN DEL SISTEMA

Se puede plantear la monitorización del sistema con alarmas en tiempo real. Habrá que ver si se aplica en todos los sistemas.

1. Detección de intrusos

   Esta se dará siempre que haya interconexión de los sistemas. El nivel de seguridad es MEDIO con refuerzos obligatorios.

2. Sistema de Métricas

   Se deberá conocer el grado de implantación de las medidas para el informe anual requerido por el artículo 32. El nivel de seguridad es MEDIO con refuerzos obligatorios.

3. Vigilancia

   Dispondrá, si aplica, de un sistema automático de recolección de eventos de seguridad. El nivel de seguridad es MEDIO con refuerzos obligatorios.

GESTIÓN DE PERSONAL

1. Caracterización del puesto de trabajo

   Deberán firmar los acuerdos de confidencialidad que tienen los trabajadores del centro. Se definirán las responsabilidades en base al análisis de riesgos.

2. Deberes y obligaciones

   Se informará a las personas de la empresa de servicios de los deberes y responsabilidades del puesto de trabajo que van a desarrollar durante su actuación. Se exigirá el acuerdo de confidencialidad (NDA) del personal proveedor. Nivel ALTO.

3. Concienciación

   No veo forma de aplicar y hay mucha discrepancia entre los expertos. Nivel ALTO siguiendo la norma establecida.

4. Formación

   Creo que no aplica a personal externo si ya vienen con los acuerdos de confidencialidad. El nivel de seguridad es MEDIO con refuerzos obligatorios.

PROTECCIÓN DE LOS EQUIPOS

1. Puesto de trabajo despejado

   No habrá material que no sea necesario para realizar el servicio. Nivel BAJO.

2. Bloqueo de puesto de trabajo

   Se deberá fijar un tiempo de bloqueo para el hardware en el hospital con un tiempo prudente (este permite desde 1 a 48h de inactividad). Nivel ALTO.

3. Protección de dispositivos portátiles

   Si el dispositivo portátil tiene conexión con la red, deberá encriptarse el disco duro. El nivel de seguridad es MEDIO con refuerzos obligatorios.

4. Otros dispositivos conectados a la red

   Equipo remoto: habrá que revisar la postura de seguridad del equipo. Equipo en la organización: antivirus/EDR, actualizaciones de Sistema Operativo. Nivel ALTO.

PROTECCIÓN DE LAS COMUNICACIONES

1. Perímetro seguro

   En el esquema de la documentación, si se cumple lo requerido, se establecerá que tipo de acceso perimetral tienen los componentes que aporte el sistema del proveedor. El proveedor puede pasar a ser parte responsable de la infraestructura de red. Nivel ALTO.

2. Protección de la confidencialidad

   Se usarán VPN's para la conexión que se realiza desde fuera de la red. Utiliza TLS 1.2 por lo que no habría que añadir nada. Los accesos que se realizan para proporcionar soporte sobre los dispositivos deberán hacerse mediante el uso de la VPN del hospital.

3. Protección de la integridad y de la autenticidad

   El perfil dice B. No se indica si se usarán VPN's para la conexión que se realiza desde fuera de la red. Utiliza TLS 1.2 por lo que no habría que añadir nada. Los accesos que se realizan para proporcionar soporte sobre los dispositivos deberán hacerse mediante el uso de la VPN del hospital. ¿Se valora la opción de obligar a que la VPN sea punto a punto? Certificados de máquina y personales. Revisar listado de algoritmos autorizados por el CCN. Nivel ALTO.

4. Separación de flujos de información de la red

   Deberá segmentarse la red en la sección donde se realice el servicio.

PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN

1. Custodia

   El nivel de seguridad es MEDIO con refuerzos obligatorios.

2. Borrado y Destrucción

   Aplicable a aquellos sistemas a los que se ha producido una conexión. Borrado mínimo de 7 pasadas. En casos de material magnético extraíble, se recomienda además magnetización completa. El nivel de seguridad es MEDIO con refuerzos obligatorios.

PROTECCIÓN DE LA INFORMACIÓN

1. Datos personales

   El nivel de seguridad es ALTO. El responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD.

2. Copias de seguridad

   Se indica que sí se hacen copias de respaldo. Se deberá indicar la frecuencia, requisitos de almacenamiento y cómo se controla el acceso a las copias de seguridad. El nivel de seguridad es MEDIO con refuerzos obligatorios.

PROTECCIÓN DE LOS SERVICIOS

1. Protección de servicios y aplicaciones web

   Se deberá incluir el resultado del análisis estático y dinámico de los aplicativos del sistema. Se tendrán en cuenta todo tipo de ataques, tipo manipulación de fragmentos de información, manipulación de url, inyección de código, acceso a documentación por vías distintas al protocolo autorizado y cualquier otro tipo de ataque que este identificado en el momento actual del servicio. Nivel de severidad ALTO.

2. Protección de la navegación web

   Se tomarán medidas contra accesos no autorizados a páginas web no clasificadas. Se establecerá un ACL solo para poder acceder a páginas del servicio que preste el proveedor. Se eliminará todo tipo de cookies. Nivel de severidad ALTO.

3. Protección frente a denegación de servicio

   Se desplegarán tecnologías de detección y reacción frente a ataques de denegación. Se deberán de probar antes del acto del servicio por parte del proveedor. Nivel ALTO.

CUADRO RESUMEN. Aquellos epígrafes que no tienen aplicación no se han puesto en el siguiente cuadro, aunque se ha aclarado su función en el documento.

APLICA		Centro sanitario	Proveedor
org	**Marco organizativo**		
org.1	**Política de seguridad**		
org.2	**Normativa de seguridad**		
org.3	**Procedimientos de seguridad**		
org.4	**Proceso de autorización**		
op	**Marco operacional**		
op.pl	**Planificación**		
op.pl.1	Análisis de riesgos	A	A
op.pl.2	Arquitectura de seguridad	A	A
op.pl.4	Dimensionamiento / gestión de la capacidad	M	
op.pl.5	Componentes certificados	A	A
op.acc	**Control de acceso**	**A**	**A**
op.acc.1	Identificación	A	A
op.acc.2	Requisitos de acceso	A	A
op.acc.3	Segregación de funciones y tareas	A	A
op.acc.4	Proceso de gestión de derechos de acceso	A	
op.acc.5	Mecanismo de autenticación (usuarios externos)	A	A
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	M	
op.exp	**Explotación**		
op.exp.1	Inventario de activos	A	
op.exp.2	Configuración de seguridad	A	A
op.exp.3	Gestión de la configuración de seguridad	A	A
op.exp.4	Mantenimiento y actualizaciones de seguridad	M	M
op.exp.5	Gestión de cambios	M	
op.exp.6	Protección frente a código dañino	M	A
op.exp.7	Gestión de incidentes	A	A
op.exp.8	Registro de la actividad	A	A
op.exp.9	Registro de la gestión de incidentes	A	A
op.exp.10	Protección de claves criptográficas	A	A
op.ext	**Recursos externos**	**A**	**A**
op.ext.1	Contratación y acuerdos de nivel de servicio	A	A
op.ext.2	Gestión diaria	A	A
op.ext.3	Protección de la cadena de suministro	A	A
op.ext.4	Interconexión de sistemas	M	

APLICA		Centro sanitario	Proveedor
op.nub	**Servicios en la nube**	**M**	**A**
op.nub.1	Protección de servicios en la nube	A	A
op.cont	**Continuidad del servicio**	**A**	**A**
op.cont.1	Análisis de impacto	A	A
op.cont.2	Plan de continuidad	A	A
op.cont.3	Pruebas periódicas	A	M
op.cont.4	Medios alternativos	A	A
op.mon	**Monitorización del sistema**	**A**	**A**
op.mon.1	Detección de intrusión	M	
op.mon.2	Sistema de métricas	M	
,	Vigilancia	M	
mp.per	**Gestión del personal**	**A**	
mp.per.2	Deberes y obligaciones	A	
mp.per.4	Formación	M	M
mp.eq	**Protección de los equipos**		
mp.eq.1	Puesto de trabajo despejado	B	
mp.eq.2	Bloqueo de puesto de trabajo	A	
mp.eq.3	Protección de dispositivos portátiles	M	
mp.eq.4	Otros dispositivos conectados a la red	A	A
mp.com	**Protección de las comunicaciones**	**A**	**A**
mp.com.1	Perímetro seguro	A	A
mp.com.2	Protección de la confidencialidad	A	A
mp.com.3	Protección de la integridad y de la autenticidad	A	A
mp.si	**Protección de los soportes de información**		
mp.si.3	Custodia	M	
mp.si.5	Borrado y destrucción	M	M
mp.info	**Protección de la información**		
mp.info.1	Datos personales	A	A
mp.info.6	Copias de seguridad	M	M
mp.s	**Protección de los servicios**		
mp.s.2	Protección de servicios y aplicaciones web	A	A
mp.s.3	Protección de la navegación web	A	A
mp.s.4	Protección frente a denegación de servicio	A	A

El presente documento ha sido elaborado por reconocidos expertos en seguridad en el área de la salud y validado por el Comité Técnico de Seguridad de la Información sobre Salud – CTSIS de la Sociedad Española de Informática de la Salud - SEIS, y patrocinado por la empresa ABBOTT.

Este documento será actualizado en el futuro por el CTSIS respondiendo a la evolución del entorno en salud y a cambios reglamentarios legales y normativos.

SOCIEDAD ESPAÑOLA DE

INFORMÁTICA DE LA SALUD