USTIC-CONC 02/22. Programa “La ciberseguridad comienza por la concienciación”. Capítulo 2. Normativa de Seguridad

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones **continúa con la publicación del segundo capítulo** del programa **de** sensibilización y **concienciación en ciberseguridad, dirigido a todos los profesionales de la STIC**, bajo el título “**La ciberseguridad comienza por la concienciación**. **Capítulo 2. Normativa de Seguridad”.**

Antecedentes

En capítulos anteriores…

El primer episodio de “La ciberseguridad comienza por la concienciación”, titulado “¿Y si fuera real?”, publicado hace varias semanas aquí https://ws001.sspa.juntadeandalucia.es/confluence/x/oCLGBg, sirvió de introducción para explicar el programa de sensibilización y concienciación en ciberseguridad para profesionales de la STIC y sus objetivos, siendo el principal de ellos el de crear una cultura de ciberseguridad.

Asimismo, presentamos un vídeo, denominado “*Cyber Europe 2022 (Former CE2020)*”, donde se mostraba una situación que podría darse en el ámbito sanitario y que nos dejaba la siguiente pregunta final a modo de reflexión: “¿Y si esto fuera real?”.

Como habréis podido comprobar al visionarlo, el escenario presentado pudiera resultar exagerado, alejado de la realidad. Sin embargo, es más común de lo que puede parecer, sobre todo, si no ponemos de nuestra parte y nos implicamos en la generación de una cultura de seguridad.

Las incidencias relacionadas con la seguridad de los sistemas de información son más frecuentes en la medida en que las organizaciones se digitalizan y se hacen más dependientes de ellos. El caso de la sanidad no escapa a esta norma. Cuando los servicios de salud o los hospitales dependen para su funcionamiento de que el sistema de citación, historia clínica o gestión administrativa de los pacientes operen adecuadamente, están ganando funcionalidad y eficiencia, pero a la vez muestran una posible debilidad, un flanco que hay que saber proteger.

Lo cierto es que cada vez es más frecuente que aparezcan noticias relacionadas con la ciberseguridad en el ámbito de las organizaciones sanitarias y, que tienen que ver fundamentalmente con dos fenómenos.

El primero, el de la seguridad en el acceso a datos clínicos, los que por su propia esencia son altamente reservados, pertenecientes a la esfera íntima del paciente, y a los que sólo pueden acceder los profesionales responsables del caso, y bajo determinadas condiciones.

Pero, el otro fenómeno que ha alcanzado notoriedad en relación con la ciberseguridad sanitaria, es el referido a la diseminación en las redes internas de programas maliciosos, el llamado ransomware, dedicado al secuestro de datos o al bloqueo de la operatividad de los ordenadores y servidores, que sólo se recupera si se paga una extorsión.

En el área sanitaria hay especificidades relacionadas con la ciberseguridad que no sólo se refieren a la elevada protección de la que hay que dotar a los contenidos de la información recogida y gestionada por los sistemas por su carácter tan relevante. También porque es necesario asegurar la protección de los dispositivos médicos de diagnosis o tratamiento conectados a las redes hospitalarias. La cada vez más frecuente interacción de estos equipos médicos con las redes corporativas facilita mucho el flujo de información y mejora los procesos de atención sanitaria, pero también hace más vulnerable la arquitectura tecnológica porque ofrece más puertas de entrada.

El vídeo presentado en el anterior capítulo del presente programa de concienciación, ejemplifica claramente la tendencia, cada vez más frecuente, por desgracia, con la que no estamos encontrando en las organizaciones sanitarias: algún incidente grave de ciberseguridad que ha comprometido funciones básicas de su día a día, que van desde el bloqueo en el acceso a los registros médicos, el funcionamiento defectuoso de los aparatos, o el impedimento persistente para la gestión administrativa de los pacientes. Véase el reciente ataque al Hospital Centro de Andalucía de Lucena: https://www.eldiadecordoba.es/provincia/Hospital-Centro-Andalucia-ataque-informatico_0_1646537254.html

Lo relevante aquí es que estas eventuales incidencias no son solo inconveniencias de carácter técnico, sino que finalmente pueden comprometer de manera grave la propia seguridad del paciente. Alterar la continuidad asistencial o el acceso a procedimientos pueden generar consecuencias directamente relacionadas con la salud de la persona que se encuentra en fase de tratamiento o diagnóstico dentro de un centro sanitario.

Los ciberataques en hospitales han aumentado desde la llegada del COVID-19, y algunos estudios cifran este incremento en hasta un 500 % a nivel mundial. El motivo es, en muchas ocasiones, el potencial lucrativo que tienen para los ciberdelincuentes el control de estos sistemas que se han revelado críticos y socialmente imprescindibles.

Un informe recientemente publicado, titulado *"The Impact of Ransomware on Healthcare During COVID-19 and Beyond*", elaborado por la consultora especializada *Ponemon Institut*, intenta mostrar la importancia de la ciberseguridad desde la perspectiva de los responsables tecnológicos, y pone de relieve un hecho muy importante: **la seguridad informática está directamente relacionada con la seguridad del paciente, hasta el punto de que determinados ataques pueden comportar consecuencias graves para estos.**

Este trabajo muestra que los ciberataques se traducen en un aumento de la tasa de mortalidad en una organización sanitaria, lo que se evidencia de manera muy directa después de sufrirlo. La razón principal es que los ciberataques pueden dar lugar a estancias hospitalarias más prolongadas y a retrasos en los procedimientos y pruebas relevantes dentro del circuito clínico. En numerosos casos, los pacientes informaron aumentos en los tiempos de espera, citas retrasadas, cirugías canceladas y otros problemas provocados por déficits en la funcionalidad de la red inducidos por ransomware.

"La Ciberseguridad comienza por la concienciación. Capítulo 2: Normativa de Seguridad. "

La seguridad de la información nos compete a todos y su objetivo es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Como ya se indicó en el episodio anterior, en cada entrega se distribuirían **diferentes tipos de material de sensibilización como pueden ser vídeos, infografías, documentos, consejos y buenas prácticas, recomendaciones, etc.,** destinados a fortalecer el conocimiento sobre aspectos clave de la seguridad de la información en todo el personal de la STIC.

En este segundo capítulo nos centraremos en conocer un pilar fundamental para todos los profesionales de la STIC en el uso de la seguridad y las implicaciones y riesgos de no asumirla: **la normativa vigente que aplica.**

Para ello, nos ocuparemos de **la Política de Seguridad y el Código de Conducta en el uso de las Tecnologías de la Información y Comunicaciones para profesionales del SAS**. Ambos documentos son el marco de referencia que deben guiar nuestras actuaciones, estableciendo los usos permitidos y prohibidos de los recursos informáticos y las obligaciones y deberes del personal en materia de tecnologías de la información.

La seguridad de la información es un aspecto clave en esta era digital en que vivimos y, por tanto, la formación y concienciación en esta materia son competencias básicas que debemos tener como profesionales de la STIC y de la sociedad en general.

---

1. Política de Seguridad TIC del SAS

El ofrecimiento de servicios sanitarios públicos de calidad, buscando la eficiencia, el aprovechamiento óptimo de los recursos, la accesibilidad, la equidad y satisfacción de los usuarios, requiere indiscutiblemente gestionar de forma segura la información como uno de los activos más importantes. Este hecho, y el uso extensivo de las tecnologías de la información y comunicaciones, ponen de manifiesto la necesidad de definir la Política de Seguridad TIC, con el objetivo de establecer directrices básicas y duraderas para una protección eficaz de los sistemas gestionados por el organismo y de la información almacenada en los mismos.

La política de Seguridad TIC vigente responde a las directrices marcadas por el artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) en el ámbito de la Administración Electrónica, donde se expresa el deber de disponer de un documento de Política de Seguridad que deberá ser aprobado por el titular del órgano superior correspondiente, tomando en consideración los principios básicos y requisitos mínimos señalados en el ENS.

Recientemente, el Real Decreto 3/2010, de 8 de enero, por el que se regulaba el ENS ha sido sustituido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. En este sentido, la actual Política TIC se encuentra en revisión para adecuarse a la nueva legislación.

Del mismo modo, nuestra actual política se dicta en desarrollo y respuesta concreta al artículo 10 del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (modificado por el Decreto 70/2017, de 6 de junio, con los cambios introducidos por el Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.

Este documento fue aprobado mediante Resolución de 8 de abril de 2021 y, manifiesta el interés de los órganos de gobierno del SAS en la gestión de la seguridad TIC. Con ella se establecen los objetivos y las responsabilidades necesarias para proteger los activos de información y los medios que se usen para su proceso, garantizando la integridad, disponibilidad y confidencialidad de estos, cumpliendo con el marco legal vigente y respetando las directrices, normas y procedimientos que oportunamente se establezcan.

Para ello, el SAS establecerá las medidas técnicas, organizativas y de control que garanticen la consecución de estos objetivos.

Objetivos

Con esta política de seguridad, el Servicio Andaluz de Salud asume los objetivos siguientes en materia de seguridad de la información:

1. Dirigir y dar soporte al gobierno y gestión de la seguridad TIC, entendida como un proceso de mejora continua.
2. Establecer el marco normativo de seguridad TIC, considerando especialmente la continuidad de los servicios y la gestión de incidencias.
3. Impulsar la formación y concienciación en materia de seguridad TIC del personal, garantizando el conocimiento del marco normativo de seguridad.
4. Definir la estructura organizativa en la que se apoyará el gobierno de la seguridad TIC, indicando comités, unidades, roles y figuras necesarias, así como sus funciones y responsabilidades.
5. Garantizar la ejecución de los análisis y planes de tratamiento del riesgo de los activos de información.
6. Garantizar la eficacia de las medidas de seguridad implantadas por medio de evaluaciones, auditorías y certificaciones.

Alcance

La política de seguridad TIC del Servicio Andaluz de Salud:

- Afecta a todos los activos TIC bajo su titularidad o cuya gestión tenga encomendada.
- Aplica a:
    - Sus Servicios Centrales, así como en sus diferentes órganos, centros e Instituciones sanitarias desplegadas en el territorio e integradas administrativamente en el mismo.
    - Centros y servicios de terceros concertados con el SAS o Consorcios que compartan información con el mismo.
    - Otros centros, servicios y establecimientos sanitarios que formen parte del Sistema Sanitario Público de Andalucía y que no encuentren cobertura en la política de seguridad TIC de la Consejería de Salud y Familias.

- Todas las personas que accedan a los Sistemas de Información como a la propia información que sea gestionada por el SAS, con independencia de cuál sea su destino, adscripción o relación con la misma.

Todas las personas y las instituciones que se comprenden en el ámbito de aplicación de esta política tienen la obligación de conocer y cumplir la presente Política de Seguridad TIC, así como la normativa de seguridad que emana de la misma. El incumplimiento de esta política de seguridad TIC podrá suponer el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales que correspondan.

Podéis consultar el texto íntegro de este documento aquí: Política de Seguridad TIC del SAS o en la la siguiente página de Confluence de la USTIC: https://ws001.sspa.juntadeandalucia.es/confluence/x/6nuOB

---

2. Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación

Para dar cumplimiento a la Política de Seguridad TIC, la organización desarrolla un conjunto de normas y planes que regulan qué se puede hacer y qué no, en relación con un cierto tema, desde el punto de vista de la seguridad, sin entrar en detalles de implementación ni tecnológicos.

Esta normativa es de obligado cumplimiento para todas las personas que trabajan en el Servicio Andaluz de Salud:

El Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales del SAS fue aprobado el 18 de enero de 2022 por el Comité de Seguridad TIC, CSISTIC-SAS, que es el órgano de dirección para la Política de Seguridad TIC de la Agencia.

Se ha adoptado la Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía.

Este Código de Conducta TIC describe:

1. El uso correcto de equipos, servicios e instalaciones.
2. Lo que se considerará uso indebido.
3. La responsabilidad de los profesionales con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

A continuación, se detallan los objetivos, principios y recomendaciones que emanan del Código de Conducta TIC. Algunos recursos utilizados son ofrecidos por el Instituto Andaluz de Administración Pública.

Presentación

Echa un vistazo al siguiente vídeo de presentación del Código de Conducta TIC:

Your browser does not support the HTML5 video element

Si no se reproduce anteriormente, puedes verlo desde aquí: Presentación del Codigo de Conducta TIC

Objetivos

1. Facilitar el uso adecuado de las tecnologías de la información y la comunicación (TIC) por los profesionales públicos.

2. Asegurar la protección de los derechos de la ciudadanía, de los profesionales públicos de la Administración de la Junta de Andalucía y de la propia Junta de Andalucía.
3. Mejorar los servicios que la Administración de la Junta de Andalucía presta a la ciudadanía.
4. Propiciar la seguridad de la información y de los sistemas frente a riesgos o actuaciones no adecuadas.
5. Fomentar el adecuado desarrollo de la sociedad de la información y facilitar el gobierno abierto

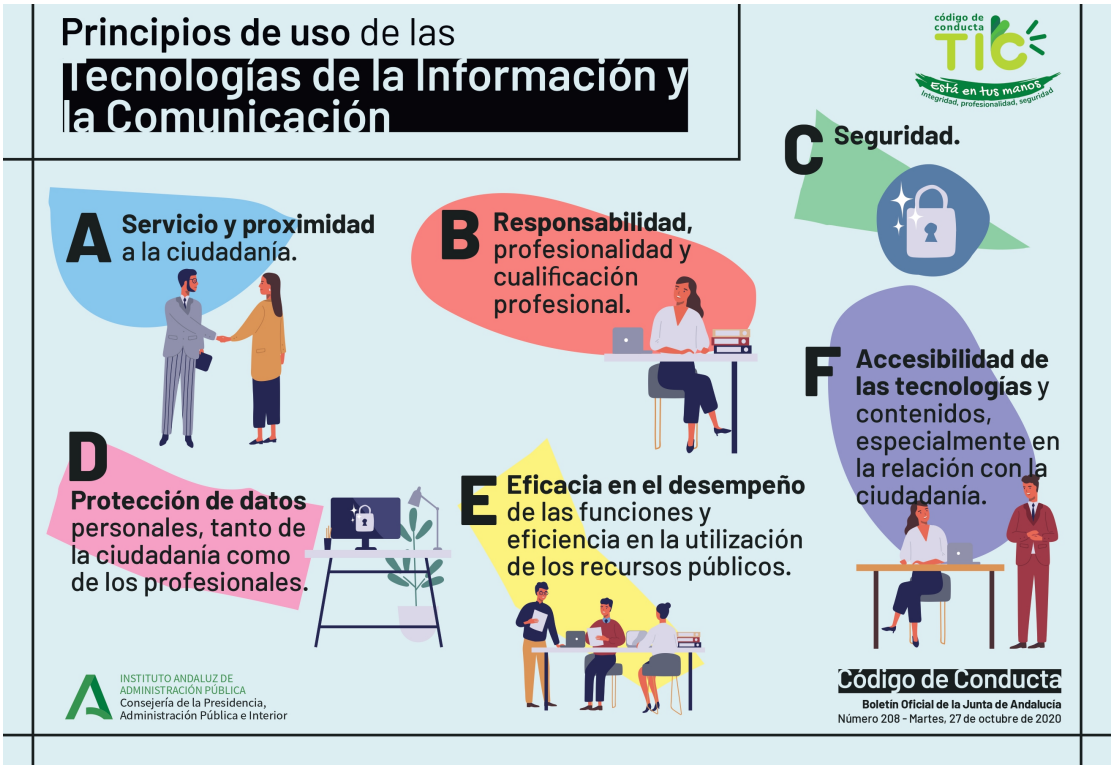
Objetivos Código de Conducta

Principios de uso de las TIC

Los profesionales deberán respetar, en el uso de las Tecnologías de la Información y la Comunicación, los siguientes principios:

1. Servicio y proximidad a la ciudadanía.
2. Responsabilidad, profesionalidad y cualificación profesional.
3. Seguridad.
4. Protección de datos personales, tanto de la ciudadanía como de los profesionales.
5. Eficacia en el desempeño de las funciones y eficiencia en la utilización de los recursos públicos.
6. Accesibilidad de las tecnologías y contenidos, especialmente en la relación con la ciudadanía.

Cartel divulgativo Principios de uso del Código de Conducta TIC (573.09 KB)



Recomendaciones de uso de las TIC

A continuación, se presentan una serie de recursos audiovisuales que recogen las principales recomendaciones de uso de las TIC:

Vídeos

- *Recomendaciones Generales de uso de las TIC:*

Your browser does not support the HTML5 video element

Si no se reproduce anteriormente, puedes verlo desde aquí: Recomendaciones Generales de Uso de las TIC

- *Uso Responsable de herramientas TIC*

Your browser does not support the HTML5 video element

Si no puedes reproducirlo anteriormente, puedes hacerlo desde aquí: Uso responsable de herramientas TIC

- *Uso del Correo Corporativo*

Your browser does not support the HTML5 video element

Puedes verlo aquí, si no se reproduce antes: Uso del Correo Corporativo

Infografías

Podéis acceder al texto íntegro del Código de Conducta aquí: Código de Conducta TIC o en la la siguiente página de Confluence de la USTIC: https://ws001.sspa.juntadeandalucia.es/confluence/x/6nuOB

Para cualquier consulta o sugerencia respecto a este programa de concienciación, podéis contactar con ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención y permaneced atentos al próximo capítulo… Saludos,

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud