¿Qué son las Prácticas de ciberseguridad de la industria de la salud (HICP) y por qué son importantes?

Las prácticas de ciberseguridad de la industria de la salud (Health Industry Cybersecurity Practices, HICP) tienen como objetivo aumentar la concienciación, proporcionar prácticas de ciberseguridad seleccionadas y avanzar hacia la coherencia en la mitigación de las amenazas actuales a la ciberseguridad más pertinentes para el sector. Su objetivo es ayudar a las organizaciones de atención médica y de salud pública a desarrollar objetivos y resultados significativos en materia de ciberseguridad. La publicación describe las cinco principales amenazas a las que se enfrenta el sector de la atención médica y las diez prácticas de mitigación para combatirlas. La edición 2023 de las HICP incluye:

- **Documento principal:** proporciona una descripción general de las cinco amenazas a las que se enfrenta el sector de la atención médica e instrucciones sobre cómo utilizar esta publicación.
- **Volumen técnico 1:** proporciona las diez prácticas de ciberseguridad y muchas subprácticas para pequeñas entidades que se pueden implementar para combatir las cinco amenazas.
- **Volumen técnico 2:** proporciona las diez prácticas de ciberseguridad y muchas subprácticas para entidades medianas y grandes que se pueden implementar para combatir las cinco amenazas.

¿Ya conoce las HICP? Por esto debería leer la edición 2023:

Las amenazas a la ciberseguridad evolucionan cada año y con ellas vienen nuevas prácticas de mitigación. La edición 2023 de las HICP recibió una actualización por parte de profesionales de la industria y del gobierno para incluir las formas más relevantes y rentables de mitigar las amenazas de ciberseguridad actuales a las que se enfrenta el sector de la atención médica. Esta edición de HICP incluye las nuevas cinco amenazas principales y muchas prácticas de mitigación nuevas que usted debería implementar en su organización para continuar manteniendo seguros a los pacientes. La ciberseguridad requiere que seamos flexibles y preventivos. Esta nueva edición aborda las tendencias de ciberseguridad que contempla el sector de atención médica y ayudará a sus objetivos de resguardar la seguridad del paciente en su organización.

Novedades de la edición 2023 de las HICP

HHS 405(d)
Aligning Health Care Industry Security Approaches

El documento principal de las HICP incluye nuevas estrategias de ciberseguridad

El documento principal de las HICP se actualizó para renovar nuestro llamado a la acción para preservar la seguridad del paciente e incluye nuevas estrategias de ciberseguridad como **Zero Trust** y **Defense in Depth.** Ahora también incluye una sección sobre la importancia de la capacitación y la concienciación en el lugar de trabajo y proporciona orientación sobre por qué cada función en una organización de atención médica es importante para mantener a los pacientes a salvo de las amenazas cibernéticas.

AMENAZAS ACTUALIZADAS

La amenaza de *phishing* por correo electrónico ahora se etiqueta como ingeniería social

Aunque las definiciones entre ambas ediciones son similares, las amenazas de ingeniería social abarcan más que solo el *phishing* por correo electrónico. Algunos elementos nuevos abordados por esta nueva amenaza: *smishing*, *whaling*, compromiso de correo electrónico empresarial y más.

PRÁCTICAS ACTUALIZADAS

La práctica de ciberseguridad n.º 9 en dispositivos médicos conectados en red se actualizó por completo

Esta sección tuvo una actualización exhaustiva con nuevas subprácticas para garantizar la protección del uso creciente de dispositivos médicos conectados a la red en el sector de la atención médica.

La práctica de ciberseguridad n.º 10 se actualizó de las Políticas de ciberseguridad a la Supervisión y gobernanza de ciberseguridad

Además de las políticas, esta sección incluye estructuras de gobernanza y supervisión que cada organización debe tener implementadas para tener un programa de ciberseguridad eficaz.

NUEVAS SUBPRÁCTICAS

Las nuevas subprácticas que se añadieron son las siguientes:

- **Simulaciones de ataque (práctica n.º 7):** esta sección proporciona a las entidades una guía sobre la importancia de efectuar simulaciones de ataques y describe qué incluir en sus propias simulaciones.
- **Seguro de ciberseguridad (práctica n.º 10):** esta sección proporciona a las entidades novedades sobre por qué el seguro cibernético es importante y qué deberían cubrir sus pólizas de ciberseguridad.
- **Evaluación y gestión de riesgos de ciberseguridad (práctica n.º 10):** esta sección menciona a las entidades cómo llevar a cabo evaluaciones de riesgos e incluso proporciona herramientas federales gratuitas que pueden utilizar para hacer su propia evaluación de riesgos.

PRÁCTICAS Y AMENAZAS ACTUALIZADAS

Las cinco principales amenazas

1. **Ingeniería social**
2. *Ransomware*
3. Pérdida por robo de equipos o datos
4. Pérdida de datos internos de forma accidental o maliciosa
5. Ataques contra dispositivos médicos conectados a la red

Diez prácticas

1. Sistemas de protección de correo electrónico
2. Sistemas de protección de puntos de conexión
3. Gestión de acceso
4. Protección de datos y prevención de pérdidas
5. Gestión de activos
6. Gestión de redes
7. Gestión de vulnerabilidades
8. Respuesta ante incidentes
9. **Seguridad de dispositivos médicos conectados a la red**
10. **Supervisión y gobernanza de ciberseguridad**

Si bien las mencionadas anteriormente son las actualizaciones principales, tenga en cuenta que cada una de las diez prácticas enumeradas se revisó y actualizó para garantizar que se proporcionen las mitigaciones de ciberseguridad más actualizadas y que puedan implementarse hoy en organizaciones de todos los tamaños. Animamos a todos, incluidos aquellos familiarizados con las HICP, a leer la nueva edición 2023 para garantizar que su organización incorpore las mejores prácticas probadas en la industria para combatir las ciberamenazas de hoy en día.

Para leer la publicación completa, visite nuestro sitio web 405d.hhs.gov.

Novedades de la edición 2023 de las HICP

HHS 405(d)
Aligning Health Care
Industry Security Approaches

¿Qué son las Prácticas de ciberseguridad de la industria de la salud (HICP) y por qué son importantes?

Las prácticas de ciberseguridad de la industria de la salud (Health Industry Cybersecurity Practices, HICP) tienen como objetivo aumentar la concienciación, proporcionar prácticas de ciberseguridad seleccionadas y avanzar hacia la coherencia en la mitigación de las amenazas actuales a la ciberseguridad más pertinentes para el sector. Su objetivo es ayudar a las organizaciones de atención médica y de salud pública a desarrollar objetivos y resultados significativos en materia de ciberseguridad. La publicación describe las cinco principales amenazas a las que se enfrenta el sector de la atención médica y las diez prácticas de mitigación para combatirlas. La edición 2023 de las HICP incluye:

- **Documento principal:** proporciona una descripción general de las cinco amenazas a las que se enfrenta el sector de la atención médica e instrucciones sobre cómo utilizar esta publicación.
- **Volumen técnico 1:** proporciona las diez prácticas de ciberseguridad y muchas subprácticas para pequeñas entidades que se pueden implementar para combatir las cinco amenazas.
- **Volumen técnico 2:** proporciona las diez prácticas de ciberseguridad y muchas subprácticas para entidades medianas y grandes que se pueden implementar para combatir las cinco amenazas.

¿Ya conoce las HICP? Por esto debería leer la edición 2023:

Las amenazas a la ciberseguridad evolucionan cada año y con ellas vienen nuevas prácticas de mitigación. La edición 2023 de las HICP recibió una actualización por parte de profesionales de la industria y del gobierno para incluir las formas más relevantes y rentables de mitigar las amenazas de ciberseguridad actuales a las que se enfrenta el sector de la atención médica. Esta edición de HICP incluye las nuevas cinco amenazas principales y muchas prácticas de mitigación nuevas que usted debería implementar en su organización para continuar manteniendo seguros a los pacientes. La ciberseguridad requiere que seamos flexibles y preventivos. Esta nueva edición aborda las tendencias de ciberseguridad que contempla el sector de atención médica y ayudará a sus objetivos de resguardar la seguridad del paciente en su organización.

Aquí tiene una descripción general de las novedades de la edición 2022 de las HICP:

El documento principal de las HICP incluye nuevas estrategias de ciberseguridad

El documento principal de las HICP se actualizó para renovar nuestro llamado a la acción para preservar la seguridad del paciente e incluye nuevas estrategias de ciberseguridad como **Zero Trust** y **Defense in Depth**. Ahora también incluye una sección sobre la importancia de la capacitación y la concienciación en el lugar de trabajo y proporciona orientación sobre por qué cada función en una organización de atención médica es importante para mantener a los pacientes a salvo de las amenazas cibernéticas.

AMENAZAS ACTUALIZADAS

La amenaza de *phishing* por correo electrónico ahora se etiqueta como ingeniería social

Aunque las definiciones entre ambas ediciones son similares, las amenazas de ingeniería social abarcan más que solo el *phishing* por correo electrónico. Algunos elementos nuevos abordados por esta nueva amenaza: *smishing*, *whaling*, compromiso de correo electrónico empresarial y más.

PRÁCTICAS ACTUALIZADAS

La práctica de ciberseguridad n.º 9 en dispositivos médicos conectados en red se actualizó por completo

Esta sección tuvo una actualización exhaustiva con nuevas subprácticas para garantizar la protección del uso creciente de dispositivos médicos conectados a la red en el sector de la atención médica.

La práctica de ciberseguridad n.º 10 se actualizó de las Políticas de ciberseguridad a la Supervisión y gobernanza de ciberseguridad

Además de las políticas, esta sección incluye estructuras de gobernanza y supervisión que cada organización debe tener implementadas para tener un programa de ciberseguridad eficaz.

NUEVAS SUBPRÁCTICAS

Las nuevas subprácticas que se añadieron son las siguientes:

- **Simulaciones de ataque (práctica n.º 7):** esta sección proporciona a las entidades una guía sobre la importancia de efectuar simulaciones de ataques y describe qué incluir en sus propias simulaciones.
- **Seguro de ciberseguridad (práctica n.º 10):** esta sección proporciona a las entidades novedades sobre por qué el seguro cibernético es importante y qué deberían cubrir sus pólizas de ciberseguridad.
- **Evaluación y gestión de riesgos de ciberseguridad (práctica n.º 10):** esta sección menciona a las entidades cómo llevar a cabo evaluaciones de riesgos e incluso proporciona herramientas federales gratuitas que pueden utilizar para hacer su propia evaluación de riesgos.

PRÁCTICAS Y AMENAZAS ACTUALIZADAS

Las cinco principales amenazas

6. **Ingeniería social**
7. *Ransomware*
8. Pérdida por robo de equipos o datos
9. Pérdida de datos internos de forma accidental o maliciosa
10. Ataques contra dispositivos médicos conectados a la red

Diez prácticas

11. Sistemas de protección de correo electrónico
12. Sistemas de protección de puntos de conexión
13. Gestión de acceso
14. Protección de datos y prevención de pérdidas
15. Gestión de activos
16. Gestión de redes
17. Gestión de vulnerabilidades
18. Respuesta ante incidentes
19. **Seguridad de dispositivos médicos conectados a la red**
20. **Supervisión y gobernanza de ciberseguridad**

Si bien las mencionadas anteriormente son las actualizaciones principales, tenga en cuenta que cada una de las diez prácticas enumeradas se revisó y actualizó para garantizar que se proporcionen las mitigaciones de ciberseguridad más actualizadas y que puedan implementarse hoy en organizaciones de todos los tamaños. Animamos a todos, incluidos aquellos familiarizados con las HICP, a leer la nueva edición 2023 para garantizar que su organización incorpore las mejores prácticas probadas en la industria para combatir las ciberamenazas de hoy en día.