UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA

FACULTAD DE PRODUCCIÓN Y SERVICIOS
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

SEGURIDAD INFORMATICA

INVESTIGACION FORMATIVA 1.1

INTEGRANTES:

- Cozco Mauri Yoset

DOCENTE: LUCY ANGELA DELGADO BARRA

AREQUIPA – PERÚ
2023

https://www.nist.gov/cybersecurity NIST

Tópicos considerados :

- Criptografía
- Educación y desarrollo de la fuerza laboral en ciberseguridad
- Medición de la ciberseguridad
- Gestión de la identidad y el acceso
- Ingeniería de la privacidad
- Gestión del riesgo
- Seguridad de las tecnologías emergentes
- Redes confiables
- Plataformas confiables

ENSAYO

Ingeniería de la privacidad

Introducción

La ciberseguridad es un aspecto crucial en la actualidad para salvaguardar la información y los sistemas de las organizaciones frente a las amenazas y ataques que pueden comprometer su integridad, confidencialidad y disponibilidad. Para ello, es necesario realizar una gestión permanente y adaptable de los riesgos asociados al uso de las tecnologías de la información y la comunicación.

Una de las agencias federales que se encarga de elaborar estándares, guías, mejores prácticas y otros recursos para la ciberseguridad en Estados Unidos es el Instituto Nacional de Estándares y Tecnología (NIST). El marco de ciberseguridad del NIST ofrece una guía voluntaria y flexible para mejorar la gestión de riesgos de ciberseguridad en las organizaciones, que se basa en un enfoque basado en riesgos con tres componentes principales: el núcleo, los niveles de implementación y los perfiles.

En este contexto, se ha analizado cómo la inteligencia artificial (IA) puede contribuir a mejorar la gestión de riesgos de ciberseguridad siguiendo el marco del NIST, gracias a su capacidad para incrementar la eficiencia y efectividad de las medidas de ciberseguridad, así como para afrontar los desafíos y amenazas emergentes en el ámbito digital.

La gestión de riesgos de ciberseguridad no solo es importante a nivel nacional, sino también a nivel internacional, existiendo diversas iniciativas y certificaciones internacionales que buscan armonizar y elevar los estándares y las buenas prácticas en materia de ciberseguridad. Recientemente, hemos sido testigos de varios ataques cibernéticos de gran magnitud que han afectado a empresas y organizaciones, lo que demuestra la importancia de la ciberseguridad y la necesidad de seguir avanzando en su mejora y fortalecimiento. Entre ellos se encuentran el ataque a SolarWinds, el ransomware a Colonial Pipeline y el ataque a Microsoft Exchange, entre otros. Es necesario estar al tanto de estos ataques y de las medidas que se están tomando para prevenirlos y enfrentarlos.

Desarrollo

La ingeniería de la privacidad es una disciplina que busca aplicar los principios y las prácticas de la protección de la privacidad en el diseño y el desarrollo de los sistemas informáticos. La ingeniería de la privacidad se inspira en el concepto de privacidad por diseño, que propone que la privacidad sea una característica integrada y no una opción añadida de los productos y servicios tecnológicos.

La importancia y los beneficios de la ingeniería de la privacidad se pueden apreciar desde diferentes perspectivas. Por un lado, desde el punto de vista normativo, la ingeniería de la privacidad ayuda a cumplir con las regulaciones y los estándares de privacidad que existen en diferentes países y regiones,

como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea o la Ley de Privacidad del Consumidor de California (CCPA). Estas regulaciones establecen una serie de derechos y obligaciones para los usuarios y los responsables del tratamiento de los datos personales, respectivamente, y exigen que se adopten medidas técnicas y organizativas para proteger la privacidad. Un ejemplo de cómo la ingeniería de la privacidad facilita el cumplimiento normativo es el caso de Apple, que ha implementado en sus dispositivos y servicios funciones como el identificador aleatorio de Bluetooth, el cifrado diferencial o las etiquetas de privacidad en las aplicaciones.

Por otro lado, desde el punto de vista del usuario, la ingeniería de la privacidad favorece la confianza y la satisfacción, ya que responde a las demandas y expectativas de los usuarios con respecto al uso que se hace de sus datos personales. Los usuarios quieren transparencia, control y seguridad sobre sus datos, y valoran positivamente que se respete su privacidad. La ingeniería de la privacidad permite ofrecer a los usuarios soluciones que les informen, les den opciones y les protejan frente a posibles amenazas o abusos. Un ejemplo de cómo la ingeniería de la privacidad mejora la experiencia de los usuarios es el caso de Signal, una aplicación de mensajería que utiliza protocolos criptográficos avanzados para garantizar la confidencialidad e integridad de las comunicaciones.

Por último, desde el punto de vista organizacional, la ingeniería de la privacidad impulsa la innovación y la competitividad, ya que permite crear productos y servicios diferenciados, que generen valor añadido para los usuarios y para las organizaciones. Además, la ingeniería de la privacidad ayuda a prevenir o mitigar posibles riesgos legales, reputacionales o financieros derivados de incidentes o violaciones de la privacidad. Un ejemplo de cómo la ingeniería de la privacidad genera ventajas competitivas es el caso de Microsoft, que ha obtenido certificaciones internacionales como ISO 27001 o ISO 27701 por su gestión eficaz del riesgo y la privacidad.

Conclusión

En conclusión, la ingeniería de la privacidad se presenta como una disciplina clave para el desarrollo tecnológico y social, ya que fomenta el cumplimiento normativo, la confianza y la satisfacción de los usuarios, e impulsa la innovación y la competitividad. En la actualidad, la inteligencia artificial (IA) está cada vez más presente en diversos ámbitos y aplicaciones, planteando importantes desafíos y oportunidades para la privacidad. La IA tiene la capacidad de procesar grandes cantidades de datos personales, extraer patrones y conocimientos, y tomar decisiones que pueden afectar a los derechos y libertades de las personas. Por tanto, es crucial que los sistemas de IA se diseñen y desarrollen con criterios éticos y responsables que garanticen el respeto a la privacidad y a otros principios como la transparencia, la comprensibilidad, la equidad o la seguridad. La ingeniería de la privacidad ofrece las herramientas y las metodologías para integrar estos principios en los sistemas de IA desde su concepción hasta su implementación.

En este sentido, se recomienda a las organizaciones que adopten un enfoque proactivo y sistemático para integrar la privacidad en sus procesos y productos que involucren IA. Al hacerlo, se logrará que la IA sea una aliada en la protección de la privacidad, contribuyendo al bienestar y al progreso de la sociedad. Asimismo, la ingeniería de la privacidad puede ser un factor clave para la competitividad de las empresas en un mercado cada vez más exigente y consciente de la importancia de la privacidad de los datos. En definitiva, la ingeniería de la privacidad es un campo en constante evolución y desarrollo, que requiere de la colaboración y el compromiso de todos los actores involucrados en su aplicación y difusión.

Bibliografia

[1] AEPD, “Ingeniería de la Privacidad”, 2019. [En línea]. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/ingenieria-de-la-privacidad. [Accedido: 04-May-2023].

[2] Protección de datos, “Ingeniería de la privacidad”, 2020. [En línea]. Disponible en: https://www.protecciondatos.org/ingenieria-de-la-privacidad/. [Accedido: 04-May-2023].

[3] NIST, “Privacy Engineering Program”, 2021. [En línea]. Disponible en: https://www.nist.gov/privacy-engineering. [Accedido: 04-May-2023].

[4] Apple, “Privacidad”, 2021. [En línea]. Disponible en: https://www.apple.com/es/privacy/. [Accedido: 04-May-2023].

[5] Signal, “Signal >> Home”, 2021. [En línea]. Disponible en: https://signal.org/es/. [Accedido: 04-May-2023].

[6] Microsoft, “Microsoft Trust Center | Home”, 2021. [En línea]. Disponible en: https://www.microsoft.com/es-es/trust-center. [Accedido: 04-May-2023].

[7] OHCHR, “Los riesgos de la inteligencia artificial para la privacidad exigen medidas urgentes – Bachelet”, 2021. [En línea]. Disponible en: https://www.ohchr.org/es/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet. [Accedido: 04-May-2023].

[8] KPMG, “Privacidad e inteligencia artificial: las reglas de la AEPD”, 2020. [En línea]. Disponible en: https://www.tendencias.kpmg.es/2020/02/privacidad-inteligencia-artificial-rgpd/. [Accedido: 04-May-2023].

[9] RedesZone, “Cómo la Inteligencia Artificial puede afectar a la privacidad de los usuarios”, 2019. [En línea]. Disponible en: https://www.redeszone.net/noticias/seguridad/inteligencia-artificial-problemas-privacidad-usuarios/. [Accedido: 04-May-2023].

[10] HubSpot, “7 ejemplos de inteligencia artificial en las empresas (2023)”, 2019. [En línea]. Disponible en: https://blog.hubspot.es/marketing/ejemplos-inteligencia-artificial. [Accedido: 04-May-2023].