



Revista
Ciberespacio, Tecnología e Innovación

Volumen 2, número 3, enero-junio 2023

Bogotá, D.C, Colombia

ISSN: 2955-0270 • eISSN: 3028-3310

Página web: <https://esdegrevistas.edu.co/index.php/rcit>



Entrevista a Lucas Giraldo Ríos. Resiliencia genética: estrategias para proteger y recuperar datos frente a amenazas cibernéticas.

Interview with Lucas Giraldo Ríos. Genetic resilience: strategies to protect and recover data from cyber threats

Angélica María González González 

CITACIÓN APA:

González González, A. M. (2023). Entrevista a Lucas Giraldo Ríos. Resiliencia genética: estrategias para proteger y recuperar datos frente a amenazas cibernéticas. *Ciberespacio, Tecnología e Innovación*, 2(3), 91-96.

<https://doi.org/10.25062/2955-0270.4809>



Publicado en línea: **Junio 30 de 2023**



[Enviar un artículo a la Revista](#)



Los artículos publicados por la *Revista Ciberespacio, Tecnología e Innovación* son de acceso abierto bajo una licencia *Creative Commons: Atribución - No Comercial - Sin Derivados*.

Entrevista a Lucas Giraldo Ríos. Resiliencia genética: estrategias para proteger y recuperar datos frente a amenazas cibernéticas.

Interview with Lucas Giraldo Ríos. Genetic resilience: strategies to protect and recover data from cyber threats

DOI: <https://doi.org/10.25062/2955-0270.4809>

Angélica María González González 

Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Biografía


Lucas Adolfo Giraldo Ríos

Docente de la Maestría en Ciberseguridad y
Ciberdefensa de la Escuela Superior de Guerra
"General Rafael Reyes Prieto", Colombia.



Entrevista

Recibido: 15 de junio de 2023 • Aceptado: 12 de mayo de 2023

Contacto: Angélica María González González  angelica.gonzalez@esdeg.edu.co

Resiliencia Genética: Estrategias para proteger y recuperar datos frente a amenazas cibernéticas

Para dar inicio a la discusión, podría explicar ¿Qué es la información genética?

La información genética se refiere al conjunto de instrucciones codificadas en el ADN de un organismo que determina sus características hereditarias y el funcionamiento de sus células. Esta información se encuentra en forma de genes, segmentos específicos de ADN que contienen las instrucciones para la síntesis de proteínas y otros componentes celulares. La información genética es fundamental para la herencia de rasgos biológicos de una generación a la siguiente, y juega un papel crucial en la regulación de la estructura y función de los organismos vivos. La decodificación de la información genética ha sido un avance significativo en la comprensión de la biología y la genética, y ha permitido avances en la medicina, la biotecnología y la investigación científica.

¿Por qué son importantes los datos genéticos?

Los datos genéticos son de suma importancia debido a la riqueza de información que contienen sobre la composición genética única de un individuo. Estos datos revelan detalles fundamentales sobre la predisposición genética a enfermedades, la eficacia de tratamientos médicos específicos, la herencia de rasgos y condiciones genéticas, así como la relación entre las variantes genéticas y la salud en general. Esta información es crucial en el campo de la medicina personalizada, ya que permite a los profesionales de la salud adaptar tratamientos y terapias de manera más precisa, lo que puede mejorar significativamente los resultados médicos y reducir los efectos secundarios no deseados.

Además, los datos genéticos también tienen implicaciones en la genealogía, la identificación de parentesco, la investigación científica y la comprensión de la diversidad genética de las poblaciones, lo que los convierte en una herramienta invaluable en diversas áreas de la ciencia y la salud. Sin embargo, la importancia de los datos genéticos va de la mano con la necesidad de proteger su privacidad y seguridad, ya que su divulgación indebida o uso inapropiado puede tener graves consecuencias para la vida de las personas y la sociedad en general.

¿Por qué debería preocuparle a una persona la seguridad de sus datos genéticos?

La seguridad de los datos genéticos debería ser una preocupación primordial para cualquier persona debido a las implicaciones tanto personales como sociales que

conlleva. En el ámbito personal, los datos genéticos contienen información íntima sobre la salud, predisposiciones genéticas a enfermedades, parentesco y otros aspectos de la identidad. Su filtración o mal uso podría tener consecuencias graves, como la discriminación en seguros de salud o empleo, así como la exposición de información altamente privada. Además, a nivel social, la seguridad de los datos genéticos es esencial para proteger la privacidad de toda la comunidad familiar, ya que compartir material genético implica también la exposición de información de parientes. Por lo tanto, mantener la seguridad de los datos genéticos es crucial para salvaguardar tanto la privacidad individual como la colectiva.

¿Qué es la ciberseguridad de la información y por qué se debe tener en cuenta en salud?

La ciberseguridad de la información se refiere a la práctica de proteger los datos digitales y los sistemas informáticos de amenazas, ataques y accesos no autorizados. En el contexto de la salud, es de vital importancia debido a la naturaleza altamente sensible y confidencial de los datos médicos y personales que se almacenan electrónicamente. Los registros de salud de los pacientes contienen información crítica, como diagnósticos, historiales médicos, resultados de pruebas y detalles de tratamientos, que deben mantenerse seguros para garantizar la privacidad de los pacientes y la integridad de los datos. La falta de ciberseguridad en la atención médica puede exponer a los pacientes a riesgos significativos, como el robo de identidad, la alteración de registros médicos o incluso la interrupción de los servicios de atención médica, lo que podría tener graves consecuencias para la salud de las personas.

Además, la ciberseguridad en salud es esencial para proteger la infraestructura de atención médica en su conjunto, ya que los ataques cibernéticos pueden afectar la disponibilidad de servicios críticos, como sistemas de emergencia, comunicaciones hospitalarias y equipos médicos conectados a la red. En un mundo cada vez más digitalizado, la atención médica depende en gran medida de la tecnología, lo que la hace vulnerable a amenazas cibernéticas. Por lo tanto, la ciberseguridad de la información en el ámbito de la salud no solo protege la privacidad de los pacientes, sino que también garantiza la continuidad de la atención médica y la integridad de los sistemas que respaldan la atención médica moderna.

A.M.G: ¿Cuál es el tópico más importante en ciberseguridad en temas de datos genéticos?

Uno de los temas más importantes en ciberseguridad relacionados con datos genéticos es la protección de la privacidad y la confidencialidad de la información genética. Dado que los datos genéticos son altamente sensibles y contienen información íntima sobre la salud y la identidad de una persona, es crucial garantizar que estos

datos estén resguardados contra accesos no autorizados, filtraciones y mal uso. La privacidad de los datos genéticos es esencial para prevenir la discriminación genética, el robo de identidad y otros riesgos asociados con la exposición de esta información. La regulación de quién puede acceder a los datos genéticos y cómo se almacenan y comparten es un tema crítico en ciberseguridad en este campo, y se han establecido normativas rigurosas, como el Reglamento General de Protección de Datos (GDPR) en Europa, para abordar estos desafíos.

¿Cómo la ciberseguridad apoya el cuidado de los datos genéticos?

La ciberseguridad desempeña un papel crucial en la protección de los datos genéticos al salvaguardar la privacidad y la integridad de la información personal almacenada en bases de datos genómicas y registros médicos. Dado que estos datos contienen información altamente sensible sobre la salud y la identidad de las personas, es esencial prevenir el acceso no autorizado, el robo de datos o la manipulación maliciosa. La implementación de medidas de seguridad robustas, como la encriptación de datos, el control de acceso, la autenticación multifactorial y la detección de intrusiones, ayuda a prevenir brechas de seguridad y garantiza que los datos genéticos estén protegidos de amenazas cibernéticas. De esta manera, la ciberseguridad contribuye a mantener la confidencialidad y la confianza en la gestión de información genética, lo que es esencial para la investigación médica, la atención de la salud y la protección de la privacidad de los individuos.

¿Cómo podría un ciberdelincuente usar los datos genéticos robados u obtenidos de manera ilícita?

Un ciberdelincuente podría aprovechar los datos genéticos robados o adquiridos de manera ilícita para llevar a cabo diversas actividades perjudiciales. En primer lugar, estos datos podrían ser utilizados en estafas de suplantación de identidad, lo que implica la creación de perfiles falsos o la obtención de servicios financieros bajo una identidad fraudulenta. Además, los datos genéticos son extremadamente personales y sensibles, por lo que su divulgación no autorizada podría resultar en chantaje o extorsión, donde el delincuente amenaza con revelar información genética confidencial a menos que se cumplan sus demandas. Además, existe el riesgo de discriminación genética, donde los datos podrían ser utilizados por empleadores o aseguradoras para tomar decisiones injustas sobre la contratación, el seguro o el acceso a servicios médicos.

En un contexto más amplio, la información genética podría ser vendida en el mercado negro o en la dark web, donde criminales podrían aprovecharla para actividades ilegales como el tráfico de órganos o la creación de perfiles de ADN falsos para encubrir la identidad de otros delincuentes. En resumen, la utilización indebida

de datos genéticos por ciberdelincuentes representa un riesgo significativo para la privacidad y la seguridad de las personas, lo que subraya la importancia de una ciberseguridad sólida y la implementación de leyes y regulaciones que protejan adecuadamente esta información delicada.

¿Qué herramientas de ciberseguridad pueden utilizarse para proteger los datos genéticos de las personas?

Para proteger los datos genéticos de las personas, se pueden utilizar una serie de herramientas y estrategias de ciberseguridad. En primer lugar, la encriptación de datos desempeña un papel fundamental. La encriptación asegura que los datos genéticos estén codificados y no sean legibles sin la clave adecuada, lo que añade una capa adicional de seguridad. Los sistemas de gestión de claves sólidos son esenciales para garantizar que solo las personas autorizadas tengan acceso a la información genética.

La autenticación de múltiples factores es otra herramienta valiosa. Requerir múltiples métodos de autenticación, como contraseñas, tarjetas inteligentes y escaneos biométricos, puede dificultar significativamente el acceso no autorizado a los datos genéticos. Además, las soluciones de monitoreo y detección de amenazas pueden ayudar a identificar actividades sospechosas o intrusiones en tiempo real, lo que permite una respuesta rápida ante posibles violaciones de seguridad.

Por último, la educación y la concienciación son fundamentales. Capacitar a las personas que trabajan con datos genéticos y a los propios individuos para que comprendan los riesgos y las mejores prácticas en ciberseguridad puede ser la primera línea de defensa contra amenazas. La ciberseguridad en el ámbito de la genética debe ser una prioridad constante y adaptarse a medida que evolucionan las amenazas cibernéticas y las tecnologías de protección de datos.

¿Principales consejos para abordar la seguridad de los datos genéticos tanto en personas como en empresas?

La seguridad de los datos genéticos es fundamental tanto para individuos como para empresas. Aquí hay algunos consejos clave para abordar este importante aspecto: **Encriptación y almacenamiento seguro:** Tanto las personas como las empresas deben garantizar que los datos genéticos se almacenen de manera segura y estén encriptados. Esto implica utilizar sistemas de almacenamiento protegidos por contraseñas y cifrado avanzado para proteger los datos de accesos no autorizados. Las empresas deben considerar el uso de sistemas de almacenamiento en la nube seguros o servidores locales con medidas de seguridad robustas.

Control de acceso y autenticación: Implementar un control estricto de acceso es esencial. Esto incluye el uso de autenticación de múltiples factores para garantizar

que solo las personas autorizadas tengan acceso a los datos genéticos. Las empresas deben establecer políticas de acceso basadas en roles, limitando el acceso solo a aquellos empleados que necesitan los datos para fines específicos.

Educación y concienciación: Tanto las personas como las empresas deben educar a su personal sobre la importancia de la seguridad de los datos genéticos y proporcionar capacitación sobre buenas prácticas en ciberseguridad. Las empresas deben tener políticas y procedimientos claros en vigor y fomentar una cultura de seguridad que promueva la concienciación sobre la privacidad de los datos genéticos y las consecuencias de un mal manejo de esta información.

¿Qué puede hacer la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra para cuidar los datos de tipo genético en las organizaciones?

La Maestría en Ciberseguridad de la Escuela Superior de Guerra podría desempeñar un papel esencial en el cuidado de los datos genéticos desde una perspectiva de ciberseguridad al ofrecer capacitación y formación especializada en la protección de información sensible. Los estudiantes de esta maestría podrían adquirir conocimientos avanzados sobre las amenazas y los riesgos cibernéticos que enfrentan las bases de datos genómicas, así como las mejores prácticas para implementar medidas de seguridad sólidas. Además, podrían colaborar en la investigación y desarrollo de estrategias de ciberseguridad específicas para proteger los datos genéticos, y podrían desempeñar un papel importante en la creación de políticas y regulaciones que garanticen la privacidad y la integridad de esta información.

En definitiva, esta maestría podría contribuir de manera significativa al cuidado de los datos genéticos al formar profesionales altamente capacitados en ciberseguridad que pueden abordar los desafíos emergentes en la protección de datos genéticos en el entorno digital actual.

Autor

Angélica María González González. Magíster en Estrategia y Geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Politóloga con Énfasis en Seguridad, Paz y Conflicto, Universidad del Rosario, Colombia. Gestora de Investigación Maestría en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia.

Orcid: <https://orcid.org/0000-0003-0881-5530>

Contacto: angelica.gonzalez@esdeg.edu.co