

Universidad Interamericana de Puerto Rico

Recinto Ponce

COMP 4910

Prof. Raquel Lugo

Edgar Rivera Plaza

Ética informática o Ciber Ética

La ética informática o ciber ética es un conjunto de principios, valores y normas que rigen el comportamiento de los empleados y organizaciones en el ámbito de la tecnología de la información y la comunicación (TIC). La ciber ética se enfoca en cómo las personas y organizaciones deben interactuar con las TIC, y cómo deben ser utilizadas de manera responsable y ética.

La ética informática tiene diferentes campos, incluyendo la privacidad, la seguridad, el acceso a la información, la propiedad intelectual, la responsabilidad social y ambiental, la identidad digital, entre otras. Algunos ejemplos de temas relevantes para la ética informática incluyen el uso de datos personales, la ciberseguridad, el plagio y la piratería informática, el cyberbullying, la adicción a la tecnología y la inteligencia artificial.

La ciber ética es importante porque la tecnología de la información juega un papel cada vez más importante en nuestras vidas, y su uso puede tener implicaciones significativas en nuestra privacidad, libertad, seguridad y bienestar. La ética informática busca promover el uso responsable y ético de la tecnología, y ayudar a garantizar que las TIC se utilicen para el beneficio de la sociedad.

Teorías éticas

1. Utilitarismo: La teoría ética utilitarista nos dice que una acción es éticamente correcta si produce la mayor cantidad de felicidad o bienestar posible para la mayoría de las personas afectadas por esa acción. En el contexto de los delitos informáticos, un estudiante podría decir que el plagio o el fraude en línea están justificados si le permiten obtener una mejor nota o más éxito académico. Sin embargo, esta práctica ignora el daño que puede causar a otras personas, como los autores originales de los trabajos copiados y a su desarrollo de pensamiento crítico y creativo.
2. Deontologismo de Kant: La teoría ética de Kant nos habla sobre la idea de que ciertas acciones son buenas o malas, sin importar de las consecuencias. Desde este punto de vista, el plagio, el fraude y el robo de datos personales son básicamente inmorales y, por lo tanto, siempre están mal. Los estudiantes que adoptan esta perspectiva pueden decir que es importante respetar la propiedad intelectual y la privacidad de los demás, incluso si eso significa que tienen que trabajar más duro en sus propias tareas académicas.
3. Realismo ético: El realismo ético se centra en la idea de que las acciones éticas son aquellas que son aceptables dentro de una comunidad o sociedad. En el contexto de los delitos informáticos, los estudiantes que adoptan una perspectiva realista pueden argumentar que el plagio y el fraude son aceptables porque son comunes en la cultura académica actual. Aun así no cambia que estén cometiendo un fraude ético.
4. Pragmatismo: El pragmatismo se centra en la idea de que una acción es éticamente correcta si funciona o es útil en un ejemplo particular. Desde esta perspectiva, los estudiantes podrían argumentar que el plagio o el fraude en línea son éticamente

justificados si les permiten alcanzar sus objetivos académicos. Sin embargo, esta perspectiva ignora el impacto a largo plazo que tales acciones pueden tener en la integridad y credibilidad de la educación y de la propia carrera del estudiante. Llevar a cabo el plagio retrasa mucho el aprendizaje y el pensamiento creativo.

5. Egoísmo ético: La teoría ética del egoísmo sostiene que una acción es éticamente correcta si beneficia al individuo que la realiza. En el contexto de los delitos informáticos, los estudiantes que adoptan esta perspectiva podrían argumentar que el plagio y el fraude son éticamente justificados si les permiten obtener mejores notas o beneficios en su carrera.

Codigos de ética

- Se debería promover el uso responsable y ético de la tecnología
- Respetar la privacidad y la privacidad de los datos personales y de las empresas
- Proteger los derechos de autor
- Comprometerse a informar y denunciar cualquier actividad sospechosa o ilegal relacionada con la tecnología
- Comprometerse a respetar las leyes y regulaciones aplicables a la tecnología
- Comprometerse a mantener la confidencialidad y la privacidad de la información de los clientes y los empleados.
- Fomentar el desarrollo de tecnologías y sistemas que sean seguros y confiables, y que minimicen el riesgo de errores y fraudes.

Como debe aplicar la ciber ética en su campo laboral.

Mi campo laboral es el desarrollo de software o Backend Developer y estos son algunos ejemplos de como debe aplicarse la ciber ética en mi campo:

- Como backend developer, puedo tener acceso a datos confidenciales del usuario y debo ser responsable de manejarlos de manera segura y ética. Esto implica comprender las políticas de privacidad de la aplicación y asegurarse de que se cumplan.
- Se debe tener en cuenta y respetar los derechos de propiedad intelectual de otros desarrolladores y compañías. Esto puede incluir el uso de licencias de código abierto y la atribución adecuada del código utilizado en la aplicación.
- Debo trabajar para garantizar que la aplicación sea segura y protegida contra vulnerabilidades. Esto puede incluir la implementación de medidas de seguridad, como el cifrado de datos y la autenticación de usuarios.

References

Bynum, T. (2001, Aug 14). *Computer and Information Ethics*. Retrieved from Stanford.edu:
<https://plato.stanford.edu/archives/sum2020/entries/ethics-computer/>

Cyber Ethics. (n.d.). Retrieved from The Knowledge Review: <https://theknowledgereview.com/cyber-ethics/>

Merced, R. G. (2017, Jun 30). *El uso del ciberespacio: Consideraciones éticas y legales*. Retrieved from UPR Rio Piedras: <https://cie.uprrp.edu/cuaderno/2017/06/30/el-uso-del-ciberespacio-consideraciones-eticas-y-legales/>

What is cyber ethics. (2022, Feb 24). Retrieved from Geek for Geeks:
<https://www.geeksforgeeks.org/what-is-cyberethics/>