

Pensamiento Computacional

Herramientas de análisis de datos

Clase 1

Ingeniería en ciberseguridad

La excelencia no se improvisa



CLASE 1

1.1. Alfabetización informática: Netiqueta y comportamiento en la red.

En los últimos años, el nexo entre la tecnología y la sociedad ha logrado avances significativos. Vivimos en un mundo interconectado donde realizamos actividades cotidianas a través del flujo constante de datos por internet. En este contexto, la alfabetización informática se convierte en una habilidad indispensable para la era moderna.

La alfabetización informática abarca un conjunto de habilidades que permiten a las personas comprender, evaluar críticamente y utilizar eficientemente la información en línea. Este concepto no solo incluye el conocimiento sobre dispositivos, software y navegación por la web, sino que también se centra en el desarrollo del pensamiento crítico para discernir la veracidad de la información, proteger la privacidad en línea y participar de manera responsable en la sociedad digital. Fomentar la alfabetización informática es, por tanto, un imperativo educativo y social que empodera a las personas y garantiza su participación plena y segura en un mundo digital en constante evolución.

Para entender mejor este concepto, comencemos con algunos términos clave.

1.1.1. ¿Qué es Netiqueta?

También conocido como **netiquette**, término que proviene del inglés «*network etiquette* (etiqueta de la red), se refiere a un conjunto de reglas que facilitan y regulan la interacción de los usuarios a través de las redes, especialmente al comunicarse mediante diversos canales como chats, mensajería instantánea, correos electrónicos, blogs o foros.

Figura 1

Nettiquette



Nota. Licencia Creative Commons

10 reglas de la netiqueta

1. **Siempre sé cordial.** Saluda, despídete y pide favores de manera educada.
2. **Crea un ambiente agradable.** Mantén una actitud positiva y amigable para favorecer la comunicación y las relaciones cordiales.
3. **Respeta las opiniones de los demás.** Aprende a aceptar tus errores.
4. **Protege la privacidad de los demás.** Pide autorización antes de publicar información relacionada con otra persona.
5. **Respeta el tiempo y el ancho de banda de los demás.** Evita enviar contenido poco interesante, incómodo o fuera de contexto.
6. **No escribas en mayúsculas.** En la red, las letras en mayúsculas significan que estás gritando o enojado.
7. **Publica contenido verdadero.** No difundas información falsa o sin contrastar. Verifica siempre las fuentes y comparte solo información de calidad, útil y veraz.
8. **Sé cuidadoso con el formato y el lenguaje.** Recuerda que el receptor de tu mensaje puede tener una cultura, idioma, humor o punto de vista diferente al tuyo. Esta norma es especialmente relevante en entornos virtuales de aprendizaje, donde interactúan estudiantes de diversas partes del mundo.
9. **Utiliza palabras neutras.** Esto ayudará a evitar malentendidos. Lee tu mensaje dos veces antes de enviarlo.
10. **Revisa la ortografía y la gramática.** Escribir con errores puede generar malentendidos y mostrar un cierto grado de descuido por parte del autor.

Figura 2

Reglas netiqueta



Nota. Licencia Creative Commons

1.1.2. ¿Qué es la Identidad digital?

Este término cobra cada vez más importancia en la forma en que interactuamos a través de los medios digitales.

La identidad digital se puede definir de dos maneras:

1. La primera es como la imagen que proyecta una persona u organización en Internet. Esta imagen se forma a partir del conjunto de datos personales, imágenes, noticias, comentarios, gustos y aficiones publicados en línea.
2. La segunda se refiere a un estándar que permite confirmar la identidad de un usuario que opera en línea.

Es importante que la sociedad tome conciencia sobre la privacidad de sus datos.

Figura 3

Identidad Digital



Nota. Licencia Creative Commons

1.1.3. ¿Qué es una Huella digital?

Cuando usamos cualquier dispositivo para navegar por sitios web, aplicaciones, foros o archivos, dejamos, de forma activa o pasiva, un rastro de nuestra actividad.

Una huella digital se define como el conjunto de datos que el software de seguimiento en línea utiliza para rastrearte en Internet, y constituye la base de tu identidad digital. Si utilizas Internet, no puedes evitar dejar una huella digital. En otras palabras, los datos (rastros) que dejas en Internet forman tu identidad digital.

Cuidar nuestra huella digital es importante porque es **fundamental** para nuestra **reputación en línea**. A través de ella, otras personas, como empleadores o agencias gubernamentales, pueden formarse una opinión sobre nosotros. Tu huella digital puede utilizarse para evaluar el tipo de persona que eres, para bien o para mal.

Figura 4

Huella Digital



Nota. Licencia Creative Commons

1.1.4. Protección de Datos Personales

“La protección de datos personales trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no, es decir, no solo a aquella información albergada en sistemas computacionales, sino en cualquier soporte que permita su utilización, almacenamiento, organización y acceso. Se ubica en el campo de estudio del Derecho Informático, del derecho de la información, de los derechos humanos y del derecho constitucional.

En algunos países, la protección de datos encuentra reconocimiento constitucional como derecho humano y en otros simplemente legal. Se protege también a través del derecho a la privacidad y del derecho a la inviolabilidad de las comunicaciones.” Wikipedia (2023)

Figura 5

Protección de datos



Nota. Licencia Creative Commons

Sobre la protección de datos: A continuación, se presentan algunos conceptos asociados a la Ley de Protección de Datos de 1998 del Reino Unido:

- **Controlador de datos:** Es “una persona u organización que, sola o junto con otras, determina los propósitos y la forma en que se procesan los datos personales”.
- **Procesador de datos:** Es una persona u organización externa designada por el controlador de datos. La responsabilidad de la protección de los datos siempre recae en el controlador.
- **Datos personales:** Son los registros u otra información que, por sí sola o vinculada a otros datos, puede revelar la identidad de una persona. Se consideran datos personales el número de teléfono, la edad, la dirección personal o laboral, la dirección IP, la geolocalización, el número de identificación, entre otros.

Figura 6

Datos personales.



Nota. Licencia Creative Commons

Datos personales “sensibles”: Además de los datos personales, existen aquellos que se consideran

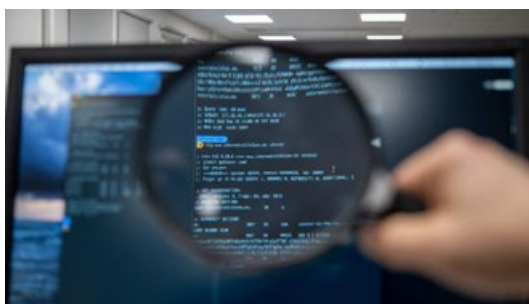
sensibles y requieren un tratamiento específico. Por ejemplo, la Unión Europea considera datos sensibles:

- Datos personales que revelan el origen racial o étnico, las opiniones políticas, o las convicciones religiosas o filosóficas.
- La afiliación sindical.
- Datos genéticos y datos biométricos tratados únicamente para identificar a un ser humano.
- Datos relativos a la salud.
- Datos relativos a la vida u orientación sexual de una persona.

¿Qué datos personales se consideran sensibles? Esta información se puede encontrar en el siguiente enlace: [Datos sensibles - Unión Europea](#).

Figura 7

Protección de datos.



Nota. Licencia Creative Commons

Protección de datos personales en Ecuador

La Constitución de la República de Ecuador, en el artículo 66, numeral 19, establece: “...el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley”.

El 26 de mayo de 2021, se publicó en el Registro Oficial la Ley de Protección de Datos Personales, que en su artículo 1 señala: “El objetivo y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto, regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela”.

Esta ley se aplicará tanto al sector público como al privado, y la Superintendencia de Protección de Datos Personales es el organismo encargado de desarrollar el registro nacional.

Puedes leer el documento completo en: [Ley Orgánica de Datos Personales](#).

Categorías especiales de datos en Ecuador: En nuestro país, los datos personales se han categorizado en:

- Datos sensibles
- Datos de niñas, niños y adolescentes
- Datos de salud
- Datos de personas con discapacidad y de sus representantes, relativos a la discapacidad.

La fuente de esta información es la Ley Orgánica de Protección de Datos del 26 de mayo de 2021.

Figura 8

Ecuador - Categorías especiales de Datos



Nota. Adaptado de: <https://3dbay.io/image/reports>

Figura 9

Sistema de protección de datos

Sistema de Protección de Datos Personales, lo conforman:



Nota. Ordóñez, V. (2021, 23 mayo). *Ley Orgánica de Protección de Datos Personales pasó al registro oficial*. Política | Noticias | El Universo. <https://www.eluniverso.com/noticias/politica/al-registro-oficial-ley-organica-de-proteccion-de-datos-personales-nota/>

A continuación, se detalla los componentes del Sistema de Protección de Datos.

1. **Titular:** Persona natural cuyos datos son objeto de tratamiento.
2. **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, autoridad pública u otro organismo que, solo o conjuntamente con otros, decide sobre la finalidad y el tratamiento de datos personales.
3. **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, autoridad pública u otro organismo que, solo o conjuntamente con otros, trata datos personales en nombre y por cuenta del responsable del tratamiento de datos personales.
4. **Destinatario:** Persona natural o jurídica que ha recibido datos personales.
5. **Autoridad de Protección de Datos Personales:** Autoridad independiente encargada de supervisar la aplicación de la ley, reglamentos y resoluciones que emita, con el fin de proteger los derechos y libertades fundamentales de las personas naturales en relación con el tratamiento de sus datos personales.
6. **Entidades certificadoras:** Entidades reconocidas por la Autoridad de Protección de Datos Personales que podrán, de manera no exclusiva, proporcionar certificaciones en materia de protección de datos personales.
7. **Delegado de protección de datos personales:** Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar por el cumplimiento normativo al respecto y cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta

y la entidad responsable del tratamiento de datos.

La fuente de esta información es la Ley Orgánica de Protección de Datos del 26 de mayo de 2021.

¿Qué derechos tengo para proteger mis datos personales?

En la Ley de Protección de Datos, el artículo 12, que se refiere al derecho a la información, tiene como objetivo comunicar al titular de los datos personales su derecho a ser notificado de manera acorde con los principios de lealtad y transparencia, por cualquier medio. Este artículo consta de 17 literales; puedes consultarlos en la ley. A continuación, mencionamos algunos de ellos:

- Sobre los fines del tratamiento.
- Consecuencias para el titular de la entrega o negativa de los datos personales.
- Tipos de tratamiento.
- Tiempos de conservación de la información.
- Otras finalidades y tratamientos ulteriores.
- Conocer la identidad del responsable del tratamiento de datos personales.
- Posibilidad de revocar el consentimiento.
- Dónde y cómo presentar sus reclamos ante el responsable del tratamiento de datos y la Autoridad de Protección de Datos Personales.
- Entre otros.

RETO 1: Investigación: Uso de la Inteligencia Artificial: ¿Solución o problema?

Descripción:

El primer reto de la asignatura tiene como objetivo principal motivar a los estudiantes a aplicar las mejores prácticas en la obtención de información de fuentes académicas confiables. En este desafío, los estudiantes realizarán una investigación exhaustiva sobre los aspectos positivos y negativos del uso de la inteligencia artificial (IA) en los ámbitos académico, social y familiar.

Los estudiantes deberán llevar a cabo una búsqueda de artículos científicos que respondan a las siguientes preguntas:

1. ¿Cómo se relaciona la inteligencia artificial con nuestro entorno familiar, académico y social?
2. ¿Qué ventajas y desventajas tiene su uso en estos ámbitos?

Para validar su investigación, los estudiantes deberán incluir datos estadísticos encontrados en los artículos científicos. Además, deberán escribir al menos tres conclusiones basadas en su investigación. Se recomienda utilizar bases de datos bibliográficas como IEEE, Springer, Scopus, WoS y Google Académico para la consulta de artículos.

Objetivo de Aprendizaje:

- Aplicar las buenas prácticas estudiadas en la asignatura sobre la validación de fuentes de información.

Resultados de Aprendizaje:

- Aplicar las buenas prácticas para el uso efectivo de las tecnologías de la información y la comunicación en sus actividades académicas.

Criterios de Evaluación:

- El trabajo entregado evidencia el cumplimiento de lo solicitado y hace uso de datos estadísticos (15 puntos).
- Validez de las conclusiones presentadas (15 puntos).
- Calidad de las fuentes bibliográficas (10 puntos).
- Redacción de calidad y sin faltas ortográficas (10 puntos).

Entregable:

Los estudiantes deberán subir un documento PDF al aula virtual de la universidad. Este documento

debe contener los siguientes apartados:

- Título
- Nombre del estudiante
- Introducción
- Desarrollo de la investigación
- Conclusiones
- Referencias bibliográficas en norma APA 7

REFERENCIAS

Biblioguias: Gestión de datos de investigación: Protección de los datos. (s. f.). <https://biblioguias.cepal.org/c.php?g=495473&p=4398118>

Colaboradores de Wikipedia. (2023, 2 de diciembre). Protección de datos personales. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Protecci%C3%B3n_de_datos_personales

Comisión Europea. (s. f.). https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_es

Ley Orgánica de Protección de Datos (26 de mayo de 2021). Quinto Suplemento N° 459 - Registro Oficial.

GLOSARIO

Netiqueta: Conjunto de reglas que facilita y regula la interacción de los usuarios en línea. Estas normas son esenciales para mantener un ambiente de comunicación respetuoso y productivo en contextos como chats, mensajería instantánea, correos electrónicos, blogs y foros. La netiqueta incluye pautas como ser cordial, respetar las opiniones ajenas, no utilizar mayúsculas (ya que se interpretan como gritos) y asegurarse de que el contenido compartido sea relevante y veraz.

Identidad digital: Imagen que una persona u organización proyecta en Internet, formada por un conjunto de datos personales, imágenes, noticias, comentarios, gustos o aficiones publicadas en línea. También se refiere a un estándar que permite confirmar la identidad de un usuario en línea. La identidad digital es crucial para la forma en que interactuamos a través de los medios digitales y para la gestión de la privacidad de nuestros datos.

Huella digital: Conjunto de datos que un usuario deja al utilizar dispositivos y navegar por sitios



web, aplicaciones, foros o archivos en Internet, de forma activa o pasiva. Estos datos son rastreados por software de seguimiento en línea y constituyen la base de la identidad digital del usuario. La huella digital incluye información sobre las páginas visitadas, las búsquedas realizadas, las interacciones en redes sociales y otros rastros de actividad en línea. Cuidar la huella digital es importante, ya que puede influir en la percepción de empleadores, agencias gubernamentales y otras entidades sobre el usuario.



La excelencia no se improvisa

síguenos

