PCA
Alfabetización para todos, futuro para Corrientes

GOBIERNO PROVINCIAL
CORRIENTES somos todos!
MINISTERIO DE EDUCACIÓN

Programa:
"LEER y COMPRENDER para RESOLVER y APRENDER"

PROPUESTAS DE ACTIVIDADES DE COMPRENSIÓN LECTORA, ORALIDAD Y MATEMÁTICA
6° AÑO DEL NIVEL SECUNDARIO

ESPECIALIDAD INFORMÁTICA PROFESIONAL Y PERSONAL
MODALIDAD TÉCNICO PROFESIONAL

CORRIENTES 2024

DIRECCIÓN DE PLANEAMIENTO E INVESTIGACIÓN EDUCATIVA

AUTORIDADES

CORRIENTES
Ministerio de Educación

Dr. Gustavo Adolfo Valdés
Gobernador de Corrientes

Lic. Práxedes Ytatí López
Ministra de Educación

Dr. Julio César de la Cruz Navias
Subsecretario de Gestión Educativa

Dra. Pabla Muzzachiodi
Secretaria General

Prof. Sergio Gutiérrez
Director General de la Dirección de Nivel Secundario

Lic. Julio Fernando Simonit
Director de Planeamiento e Investigación Educativa

Prof. Sergio Paniagua
Director de la modalidad de Educación Técnico Profesional

COMISIONES DE TRABAJO AD HOC EN EL MARCO DEL PLAN DE COMPROMISO POR LA ALFABETIZACIÓN

Prof. Gloria Espinoza
Coordinadora Área de Lengua
Dirección de Planeamiento e Investigación Educativa

Prof. Luz Meza
Coordinadora Área Matemática
Dirección de Planeamiento e Investigación Educativa

Lic. Marcela Arévalo
Diseño Gráfico

ÍNDICE

COMPRENSIÓN LECTORA Y ORALIDAD

RESOLUCIÓN DE PROBLEMAS – MATEMÁTICA

Programa:
"LEER y COMPRENDER
para RESOLVER y APRENDER"

PROPUESTAS DE ACTIVIDADES DE COMPRENSIÓN LECTORA, ORALIDAD Y MATEMÁTICA 6° AÑO DEL NIVEL SECUNDARIO

ESPECIALIDAD INFORMÁTICA PROFESIONAL Y PERSONAL
MODALIDAD TÉCNICO PROFESIONAL

PROPUESTA 1

Seguridad Informática

Antes de la lectura

1. Reflexiona sobre el título "Seguridad de la Información" y registra tus ideas en un padlet interactivo.

2. Expresa tus expectativas y conocimientos previos sobre este tema en relación con el entorno laboral y tecnológico.

Durante la lectura

1. Lee el siguiente texto.

¿A qué se llama Seguridad de la información?

Se denomina seguridad de la información al conjunto de prácticas destinadas a preservar la integridad, la disponibilidad y la confidencialidad de la información con independencia de su soporte y desde el punto de vista de procesos. La visión de la seguridad de la información se integra a las distintas funciones de una organización para incluir las prácticas recomendadas, tanto en los procesos de la organización como en sus servicios. Por esta razón, se debe tener conocimiento de la misión y funciones de la organización, así como de las prácticas y estándares de la seguridad de la información para poder integrarlas de manera completa.

La Gestión de la seguridad de la información incluye el diseño e implementación de planes de prevención desde los distintos procesos (clasificación de la información, gestión de accesos, de vulnerabilidades y amenazas, evaluación de riesgos, etc.) que se relacionan dentro de la organización, la gestión de los recursos necesarios para dichas actividades, y la consideración de un análisis de riesgos que permita balancear objetivos de seguridad con recursos disponibles y la exposición a las amenazas con mayor probabilidad de afectar a la organización.

Adicionalmente, en el contexto de una organización pública o privada, la asignación de responsabilidades debe ser clara para una correcta rendición de cuentas, tanto para la gestión operativa como para las posibles consecuencias administrativas o judiciales ante incidentes. En este sentido, los procedimientos de mayor relevancia deberán estar documentados para evidenciar los análisis y la aprobación de las autoridades.

¿Es lo mismo seguridad de la información que seguridad informática?

La seguridad informática es una disciplina técnica que contempla las medidas de seguridad aplicadas en el ámbito de la tecnología informática y de telecomunicaciones, ya sea el desarrollo de sistemas de información, los protocolos de comunicación, aplicaciones móviles, las infraestructuras, las bases de datos, la virtualización, las "nubes", las redes, los dispositivos que incluyen un circuito integrado, etc. De manera genérica, comprende la seguridad del software, del hardware, de las redes y de sus interacciones.

En ciertos contextos se utilizan de manera indistinta. Sin embargo, es mejor entender las diferencias, describir las funciones y alcances de la manera más precisa posible. Por otro lado, en general, cuando se menciona seguridad de la información se incluye a la seguridad informática. En este contexto, resulta relevante asegurarse que los alcances de los términos que se utilizan sean los correctos.

En grandes líneas, las personas expertas en seguridad informática tienen conocimientos y habilidades en técnicas en desarrollo seguro, técnicas de hacking, aseguramiento de redes, administración de sistemas, configuraciones seguras (hardening) o análisis de malware, por mencionar las más requeridas.

En el caso de la seguridad de la información, el conocimiento y habilidades están dados por el campo de implementación de buenas prácticas para la gestión de la seguridad de manera transversal e integral en una organización, es decir, los distintos estándares y procesos, la definición de planes, normas y procedimientos y su implementación, así como su vinculación con la gestión de los riesgos de las tecnologías de la información.

La implementación de medidas técnicas de seguridad para el software, el hardware y las redes constituyen actividades básicas que se estructurarán y organizarán en función de los procesos y sus actividades. En el mismo sentido, los procesos deben administrarse de manera continua, para adecuarse a los cambios.

Las organizaciones cambian cuando incorporan o rotan sus empleados, cuando adquieren o actualizan el equipamiento informático, cuando se desarrollan nuevos sistemas de información o aplicaciones y todo tipo de redes, así como cuando se materializan cambios en las funciones o en los productos. Por estos motivos se deben realizar los mantenimientos y actualizaciones necesarias de manera planificada, diseñar y establecer planes de respuesta ante incidentes y participar en el diseño e implementación de los planes de resiliencia.

Para las organizaciones que adoptan el modelo de gestión de servicios de Tecnologías de la Información o TI (ITIL1 o ISO/IEC 20000), tanto de manera interna como en los servicios que brindan a la ciudadanía, los aspectos de seguridad forman parte del ciclo de vida de dichos servicios, desde su diseño hasta su finalización. Además, la implementación de seguridad debe incorporarse en los niveles de operación, gestión y hasta en la dirección.

Extraído de: Pallero, M. y Heguiabehere, J. M. (2023). Seguridad de la información y ciberseguridad. Informe técnico. Ministerio de Ciencia, Tecnología e Innovación. https://fundacionsadosky.org.ar/wp-content/uploads/2023/12/Seguridad-de-la-informacion-y-ciberseguridad.pdf

2. Realiza una segunda lectura y responde:

a. ¿Qué se entiende por seguridad de la información según el texto proporcionado?

b. ¿Cuáles son los pilares considerados fundamentales de la seguridad? Explica brevemente cada uno de ellos.
c. ¿Qué implica la gestión de la seguridad de la información en una organización?
d. ¿Por qué es importante documentar los procedimientos de relevancia en el ámbito de la seguridad de la información?
e. ¿Cuál es la diferencia principal entre seguridad de la información y seguridad informática?
f. Menciona al menos tres habilidades específicas que requiere un especialista en seguridad informática, según lo desarrollado en el texto.
g. Considerando la importancia de la seguridad de la información y la seguridad informática en el contexto actual, ¿cómo crees que las organizaciones deberían abordar estos aspectos de forma más proactiva e integral para garantizar la protección de los datos y la operatividad de sus servicios?

Después de la lectura

1. Elabora una infografía en Canva en la que integres los conceptos claves sobre la seguridad de la información.

2. Comparte con la clase tu presentación.

PROPUESTA 2

Inteligencia artificial. IA. Hitos

Antes de la lectura

1. Piensa y responde en tu carpeta:

a. ¿Qué significa la palabra “hito”? ¿Qué sinónimos puedes mencionar?
b. ¿Conoces otros juegos en los que los jugadores compiten contra una máquina en lugar de hacerlo con otra persona de manera presencial?
c. ¿Cómo funcionan estas plataformas de juegos?

Durante la lectura

1. Realiza una lectura silenciosa del siguiente texto.

Tres hitos de la inteligencia artificial: Turing, Deep Blue y AlphaGo

En esta nota, exploramos la evolución de las inteligencias artificiales desde los días de Turing, pasando por Deep Blue hasta el triunfo de AlphaGo y cómo estos hitos transformaron nuestra mirada de la relación entre humanos y máquinas.

La historia de la inteligencia artificial (IA) es un viaje fascinante que abarca desde los primeros experimentos hasta los algoritmos más recientes.

El desafío de Turing

En 1950, **Alan Turing,** matemático, filósofo y criptógrafo, propuso una prueba para detectar si una máquina podía pensar como un humano. Este famoso "Desafío de Turing" consistía en un juego de imitación en el que un interrogador debía averiguar quién era una máquina y quién era una persona solo mediante preguntas escritas. Si el interrogador no podía distinguir a la máquina de la persona, se consideraba que la máquina había pasado la prueba. Las contribuciones de Turing sentaron las bases para la investigación moderna en IA.

Desde la década de 1950 hasta nuestros días, la IA avanzó enormemente gracias al desarrollo de la computación, la programación y el aprendizaje automático (machine learning). La capacidad de los sistemas automáticos para aprender por sí mismos a partir de entrenamientos con datos masivos y experiencias fue fundamental para su progreso.

Deep Blue: los límites del ajedrez

En 1997, **Deep Blue**, la supercomputadora de IBM, derrotó al campeón mundial de ajedrez: el ruso **Garry Kasparov.** Deep Blue utilizó una combinación de altísima capacidad de cómputo y algoritmos de búsqueda para evaluar millones de posiciones por segundo. Aunque algunos argumentan que no fue una verdadera IA, la victoria de Deep Blue marcó un hito importante en la relación entre humanos y máquinas.

AlphaGo: la nueva frontera

En 2016, **AlphaGo,** una inteligencia artificial desarrollada por DeepMind de Google, venció al surcoreano **Lee Sedol,** uno de los mejores jugadores de go en el mundo. El go es un juego milenario de origen chino. A diferencia del ajedrez, el go tiene un espacio de búsqueda mucho más amplio, lo que hace que la victoria de AlphaGo sea aún más impresionante.

AlphaGo utilizó redes neuronales y técnicas de aprendizaje profundo para evaluar posiciones y tomar decisiones estratégicas. Su capacidad para aprender de sus propios errores y mejorar la estrategia con cada partida demostró la versatilidad de esta inteligencia artificial.

La evolución de la IA, desde Deep Blue hasta AlphaGo, nos muestra que cuando se trata de lógica y potencia de cálculo, las inteligencias artificiales pueden superar a los humanos. Pero cuando se trata de sentido común, emociones y ambigüedades, las IA fallan. Si de algo estamos seguros es que la relación entre humanos y máquinas continuará evolucionando en formas sorprendentes.

Fuente:
https://www.educ.ar/recursos/159083/tres-hitos-de-la-inteligencia-artificial-turing-deep-blue-y-

2. A medida que avanzas en la lectura, resuelve las siguientes actividades:

a. Describe qué está haciendo el joven en la imagen.
b. Elabora un campo semántico de términos que se relacionen con el título del texto.
c. Crea una línea del tiempo con la historia de la inteligencia artificial, incluyendo fechas, autores destacados y hechos relevantes. Puedes recurrir al cuadernillo *Técnicas de estudio y estrategias para el aprendizaje* del Ministerio de Educación (págs. 33 a 35).

Después de la lectura

1. Marca con una **X** la opción correcta.

¿Cuál fue el principal objetivo del "desafío de Turing"?

- ☐ **a)** Demostrar que las máquinas pueden pensar de forma creativa.
- ☐ **b)** Crear una máquina capaz de sentir emociones.
- ☐ **c)** Determinar si una máquina puede engañar a un humano haciéndose pasar por otro.

¿Qué característica de AlphaGo la diferenció de Deep Blue?

- ☐ **a)** Una mayor capacidad de cálculo.
- ☐ **b)** La habilidad de aprender y adaptarse a través del aprendizaje profundo.
- ☐ **c)** Un diseño físico más avanzado.

¿Cuál de las siguientes afirmaciones es CORRECTA sobre la evolución de la IA?

- ☐ **a)** La IA ha demostrado ser superior a los humanos en todas las tareas.
- ☐ **b)** La IA aún no ha alcanzado el nivel de inteligencia humana.
- ☐ **c)** La IA solo es capaz de realizar tareas repetitivas.

2. Indica al margen de cada afirmación si son VERDADERAS o FALSAS:

- ☐ Deep Blue derrotó a Garry Kasparov en una partida de ajedrez.
- ☐ AlphaGo utiliza redes neuronales para tomar decisiones.
- ☐ Alan Turing propuso un test para determinar si una máquina puede pensar.
- ☐ El go es un juego más simple que el ajedrez.
- ☐ Deep Blue y AlphaGo utilizan la misma tecnología.
- ☐ El aprendizaje automático ha sido clave en el desarrollo de la IA.
- ☐ La IA actual puede comprender completamente el lenguaje humano.
- ☐ El desafío de Turing sigue siendo el estándar más utilizado para medir la inteligencia de una máquina.

PROPUESTA 3

Ciberseguridad

Antes de la lectura

1. ¿Con qué frecuencia utilizas las redes sociales? ¿Cuáles son las que más usas?

2. Lee el título y responde: ¿Qué es la ciberseguridad? Escribe al menos 3 ideas que expliquen este concepto.

3. Redacta tres (3) preguntas que crees que podrás contestar luego de leer el texto.

Durante la lectura

1. Lee silenciosa y detenidamente el siguiente texto.

¿A qué se llama ciberseguridad?

En las últimas décadas, los impactos de los incidentes de seguridad de la información se han expandido desde las organizaciones a las sociedades y a los países. Estos impactos a nivel país tienen mayor alcance, en tanto se abordan aspectos de la seguridad en los servicios esenciales y sus infraestructuras críticas, el comercio internacional o las atribuciones de los ataques que se originan en un país y afectan a civiles de otros países o a sus infraestructuras, los espionajes industriales y entre países.

Estas nuevas ramificaciones merecen análisis multidisciplinar. Además, las consecuencias afectan desde derechos fundamentales como la libertad de expresión, la privacidad, la protección de datos personales hasta la defensa nacional. En el contexto de los problemas que afectan a la ciudadanía se adopta el uso del término "ciberseguridad", no existiendo aún una definición con consenso internacional. Adicionalmente, para el público en general, varios términos se usan de manera indistinta. Se debe tener en cuenta que para diferentes ámbitos puede tener definiciones distintas.

En este sentido, las normas ISO han adoptado para ciberseguridad una definición en la ISO/IEC 27100 en el año 2020 comentada a continuación:

Ciberseguridad: Resguardo* de las personas, la sociedad, las organizaciones y las naciones de los ciberriesgos, entendiendo por ciberriesgo** como el efecto de la incertidumbre sobre los objetivos establecidos.

Adicionalmente en la definición se incluyen las siguientes tres aclaraciones:

· 1ero. Cuando se refiere a *Resguardo significa mantener el ciberriesgo en un nivel tolerable.

· 2do. ** El ciberriesgo puede expresarse como efecto de la incertidumbre de una entidad en el ciberespacio.

· 3ero. El ciberriesgo está asociado con la posibilidad de que las amenazas exploten las vulnerabilidades en el ciberespacio y, por lo tanto, causen daño a las entidades. Por otro lado, define Ciberespacio como el entorno digital interconectado de redes, servicios, sistemas, personas, procesos, organizaciones y lo que reside en el entorno digital o lo atraviesa.

Es importante que la terminología sea clara y coherente desde los aspectos organizacionales y a nivel país, dado que en general la regulación suele basarse en estas definiciones, y ante disputas legales, las interpretaciones pueden ser críticas. Una consideración relevante de la definición de ciberseguridad de ISO/IEC 27100 y en algunas otras que suelen utilizarse, es que parecen excluir el entorno físico asociado al entorno digital, mientras que se encuentran presentes en las buenas prácticas de seguridad de la información así como es evidente en la práctica profesional la importancia de proteger el espacio físico

asociado, que alcanza a la provisión de los servicios básicos, el cableados, y la información en otros soportes asociado a los servicios digitales. Cabe mencionar que Argentina cuenta con la Resolución Nro. 1523/2019 en la queque se ha adoptado un glosario de ciberseguridad que, de acuerdo con su texto, se actualizará de acuerdo con la evolución tecnológica. En el contexto de las organizaciones, no ya a nivel de Estados, el término de ciberseguridad se utiliza también para englobar a la seguridad informáticas, la seguridad de la información, también aspectos legales relacionados y la gestión de los riesgos de tecnologías como una categoría, aunque muchas veces, como se ha mencionado, se la nombre como sinónimo de seguridad informática.

Volviendo al ámbito nacional, la ciberseguridad está presente en las relaciones internacionales, por un lado, cuando se interviene para promover la protección de servicios e infraestructuras civiles de ataques originados en el extranjero (por individuos o grupos) como para la protección de personas, infraestructuras y organizaciones de ataques de Estados extranjeros.

En ambos contextos se puede apreciar que la protección del entorno físico es inherente a la protección de servicios digitales y de la información, la seguridad de la infraestructura que les da soporte, así como la de los elementos físicos que interactúan o almacenan algún tipo de información necesaria (discos rígidos externos, dispositivos USB, código QR en papel, etc.) para el funcionamiento de algún servicio digital. De esta manera, la protección del entorno físico asociado al ámbito que procesa información como pueden ser los puertos de conexión de un dispositivo, el cableado por el que circulan los datos, o su soporte de almacenamiento son también parte del ambiente en la ciberseguridad.

Extraído de: Pallero, M. y Heguiabehere, J. M. (2023). Seguridad de la información y ciberseguridad. Informe técnico. Ministerio de Ciencia, Tecnología e Innovación. https://fundacionsadosky.org.ar/wp-content/uploads/2023/12/Seguridad-de-la-informacion-y-ciberseguridad.pdf

2. Subraya con un color las ideas del texto que consideres más importantes.

3. Escribe una nota marginal al lado de cada párrafo con la idea central.

4. Según el texto, ¿cuáles son las nuevas ramificaciones que merecen análisis multidisciplinar?

5. Redacta definiciones para los términos “ciberacoso”, “ciberriesgo” y “ciberespacio”.

Después de la lectura

1. Marca con una **X** la respuesta correcta:

¿Qué es la ciberseguridad según la norma ISO/IEC 27100?

- ☐ **a)** La protección de la información en el entorno físico.
- ☐ **b)** El resguardo de las personas, la sociedad, las organizaciones y las naciones de los ciberriesgo.

- ☐ **c)** La seguridad informática y la gestión de riesgos.
- ☐ **d)** La protección de infraestructuras críticas y defensa nacional.

¿A qué se define como el entorno digital interconectado de redes, servicios, sistemas, personas, procesos, organizaciones y lo que reside en el entorno digital o lo atraviesa?

- ☐ **a)** Al ciberespacio.
- ☐ **b)** A la ciberseguridad.
- ☐ **c)** A la seguridad informática.
- ☐ **d)** A la gestión de riesgos.

¿Por qué es importante considerar el entorno físico asociado al entorno digital en la ciberseguridad?

- ☐ **a)** Porque no tiene relación con la seguridad digital.
- ☐ **b)** Porque es necesario proteger los dispositivos y cableados.
- ☐ **c)** Porque solo se enfoca en la seguridad informática.
- ☐ **d)** Porque no es relevante para la protección de la información.

¿Qué sugiere el texto sobre la importancia de la ciberseguridad en las relaciones internacionales?

- ☐ **a)** Que no es relevante para las relaciones internacionales.
- ☐ **b)** Que solo se enfoca en la protección de la información.
- ☐ **c)** Que es crucial para proteger servicios e infraestructuras civiles de ataques extranjeros.
- ☐ **d)** Que solo se aplica a la seguridad informática.

2. Reflexiona sobre cómo la ciberseguridad afecta tu vida diaria, y redacta un breve texto explicativo.

a) ¿Cómo proteges tu información personal en las redes sociales?
b) ¿Qué riesgos cibernéticos has enfrentado o conoces?

3. ¡Los técnicos en informática también concientizan!

a) Utiliza tu red social (si es que tienes una: Facebook, Instagram o estado de WhatsApp) o hazlo en un folleto escrito para concientizar sobre el ciberacoso o ciberriesgos.
b) Escribe una frase reflexiva sobre “la ciberseguridad” y comparte con tus seguidores y/o grupos.

PROPUESTA 4

Las cookies

Antes de la lectura

1. Describe brevemente lo que observas en la imagen que se presenta a continuación.

2. Responde:

a) ¿Qué son las cookies?
b) ¿En qué idioma está escrito y qué significado tiene?
c) ¿Qué relación tienen las cookies con la informática?

Durante la lectura

1. Lee silenciosamente el siguiente texto.

2. Escribe al margen de cada párrafo una breve nota que resuma la idea central.

Qué son las cookies, para qué sirven y cómo funcionan

Las cookies son una herramienta de recopilación de datos que permite que los navegadores y los sitios intercambien información de los visitantes. Su finalidad es dar una mejor experiencia al usuario.

Las cookies son archivos temporales que un sitio web almacena en tu navegador con el fin de recordar tus interacciones en el sitio y mejorar tus visitas en el futuro. Gracias a las cookies, las páginas pueden acceder a información sobre tu actividad en línea.

No importa si navegas desde una computadora de escritorio, tu celular, un buscador independiente o una aplicación: las cookies permiten que los sitios reconozcan a los usuarios. La información que se comparte es muy valiosa para mejorar el marketing en línea.

¿Para qué sirven las cookies?

La principal funcionalidad de las cookies es reconocer usuarios. Al habilitarlas, una persona puede regresar a una tienda en línea y continuar con la compra que dejó en el carrito o mantener actualizado un historial de búsqueda dentro del sitio. También sirven para almacenar información que normalmente se pide en distintos formularios de registro o de compras (nombre, ubicación, edad, números de cuenta, etc.) y es necesaria para aprender los comportamientos de los usuarios. Esto también facilita que otras empresas muestren publicidad personalizada
.

Si tu web tiene cookies podrás:

- Guardar los artículos de compra en el carrito hasta que tus clientes logren finalizar el proceso.
- Recordar los datos de tus visitantes para evitar que tengan que llenarlos cada vez que regresen.
- Registrar las preferencias de las personas que interactúan con tu sitio, por ejemplo: idioma, ubicación o moneda con la que prefieren pagar.
- Personalizar el contenido que se muestra a las personas, desde artículos de blog que pueden interesarles hasta novedades de tus productos, según lo que han comprado o visto anteriormente (o lo que pertenece a la misma categoría o colección).
- Brindar una mejor experiencia de usuario, pues ayudan a que una página que ya se visitó se cargue con mayor rapidez.

¿Cómo funcionan las cookies?

Básicamente así: cuando ingresas a una página por primera vez, una cookie se descarga y se aloja en tu navegador. Si regresas, el sitio buscará una cookie que tenga su nombre. Al encontrarla podrá facilitar la navegación ya que te ha reconocido, adaptando la información que aparece en tu pantalla de acuerdo con tus interacciones anteriores en el sitio.

Esa es la razón por la que, cuando realizas una búsqueda en Google que ya habías hecho días antes, verás que los enlaces en los que hiciste clic la primera vez aparecen en distinto color. Esto te permite distinguir los sitios a los que habías ingresado antes de aquellos donde no lo hiciste.

Tipos de cookies

A grandes rasgos podemos categorizar las cookies de acuerdo con su origen, temporalidad o función. Revisemos las características de cada uno de estos tipos.

Tipos de cookies por origen

Una pregunta fundamental a la hora de hablar de cookies consiste en saber quién las genera y con qué fin. Es por ello que podemos hablar de dos grandes tipos de cookies dependiendo de su origen: las propias y las de terceros.

- **Propias:** son aquellas generadas directamente por el sitio web. Estas cookies se descargan en el equipo del visitante y son gestionadas para mejorar la experiencia de navegación del usuario en el futuro dentro de sus páginas.
- **De terceros:** son aquellas que no son generadas por el sitio que es visitado, sino que tienen origen en servidores externos. Es el caso de algunas plataformas de redes sociales que utilizan las cookies para rastrear la actividad en línea de los internautas y utilizarla para publicitar servicios y productos específicos.

Tipos de cookies por temporalidad

Por otro lado, existen diferentes tipos de cookies dependiendo de la tarea que desempeñan dentro del sistema. Podemos afirmar que existen dos grandes tipos de cookies según su tiempo de vida: temporales y permanentes.

- **Temporales:** son cookies que solamente desempeñan su función durante el tiempo de navegación del visitante. Esto significa que al abandonar el sitio desaparecen estos archivos y solo están diseñados para mantener la información al visitar diferentes páginas del sitio o al refrescarlas.
- **Permanentes:** las cookies permanentes se distinguen por tener un tiempo de vida mucho más largo. Esto significa que los archivos permanecerán indefinidamente en el equipo del visitante y estarán siempre disponibles para el momento en que vuelva a visitar el sitio.

Es importante mencionar que todas las cookies tienen una fecha de expiración, ya que al actualizar el software de una página se puede perder la capacidad de encontrar a la cookie. Sin embargo, el archivo sí puede permanecer en el equipo indefinidamente, aunque ya no tengan ninguna función.

Tipos de cookies por función

Por último, podemos categorizar a las cookies dependiendo de la función que desempeñan. No todas están diseñadas para resguardar información, sino que forman parte de procesos más completos, según el uso que quiera darles el propietario. Algunas de ellas son:

- **De análisis:** permiten conocer el rendimiento de un sitio al recopilar la información de lo que los visitantes hacen en él. Estos datos ayudan a dimensionar los enlaces con más clics, las llamadas a la acción más exitosas, por mencionar algunos.
- **De preferencias:** hacen posible que se guarde la personalización de un usuario al visitar un sitio: idioma, ubicación desde donde se ingresa, por ejemplo.

- **De marketing:** ayudan a crear perfiles analizando los comportamientos de los visitantes, como la navegación en otras páginas o las búsquedas que realizan. Además, permiten gestionar los anuncios con mayor éxito, pues muestran los más adecuados a quien tiene más probabilidades de interesarse en tu contenido (según edad, sexo, ubicación, preferencias).

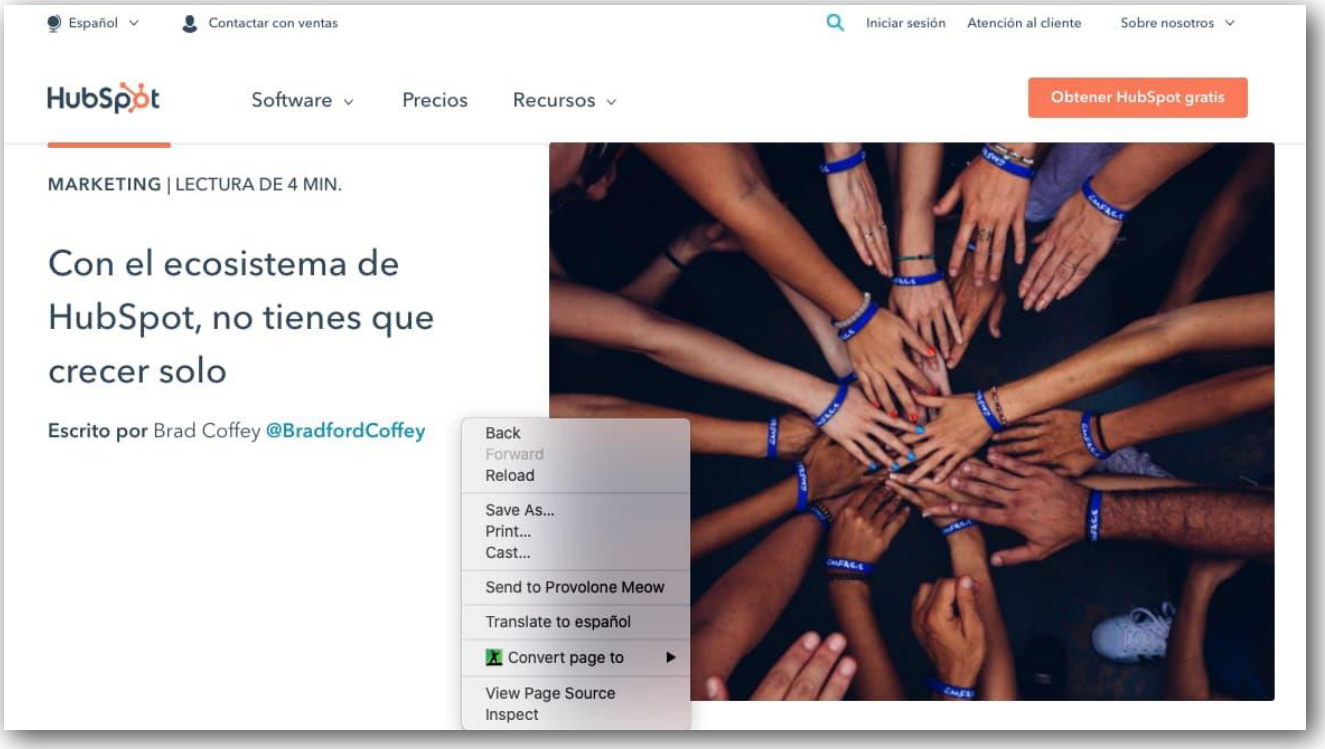
- **Técnicas:** son las que no se pueden borrar de los navegadores porque optimizan el funcionamiento de la web (cuando realizas una compra, compartes contenido en redes sociales) y permiten que un sitio gestione el tráfico que recibe.

Podría decirse que todos los sitios tienen cookies debido a que existen procesos que requieren que los visitantes se registren, aunque sea únicamente con su correo electrónico (como para hacer comentarios en publicaciones, realizar compras o descargar contenido gratuito). Si, por ejemplo, usas Google Analytics para medir el desempeño de tu sitio o implementas el píxel de Facebook para dar seguimiento a tus conversiones que ocurren desde la plataforma, ya tienes cookies.

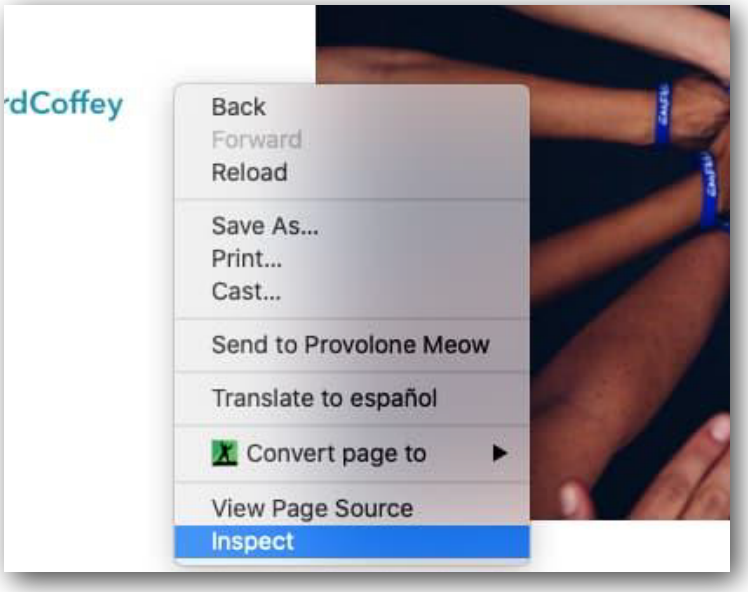
¿Cómo ver las cookies en tu sitio web? Paso por paso

Ver las cookies en tu sitio es muy sencillo. Revisemos paso a paso la mejor forma de hacerlo:

1. Haz clic derecho en cualquier lugar de una de tus páginas y verás que se despliega un menú:



2. Elige «Inspeccionar» o «Inspect», en inglés:



3. Verás que el sitio se divide en dos: del lado izquierdo verás el sitio tal y como lo ve cualquier visitante, y del lado derecho verás el código que está tras bambalinas. Busca el menú de «Application» y haz clic en él:

4. Ahora busca «Cookies» en el nuevo menú que acaba de desplegarse y ya puedes ver las que hay en esa página:

Extraído de: Casarotto, C. (3 de junio de 2022). *¿Qué son las cookies y cuál es su finalidad en los sitios web?* Rockcontent blog. https://rockcontent.com/es/blog/cookies/

Después de la lectura

1. Define en tres ideas cuál es el tema principal del texto.

2. Explica brevemente cómo funcionan las cookies y cuál es su importancia.

3. Desarrolla, mediante captura de pantalla utilizando tu PC o celular, los pasos explicados en el texto para visualizar las cookies del siguiente sitio web: https://sima.mec.gob.ar/

Actividades de extensión

1. Busca información sobre los algoritmos de Google y sus funciones.

2. Menciona al menos tres ejemplos de algoritmos utilizados en internet.

3. Elabora un mapa conceptual con la información que has encontrado. Recuerda citar las fuentes consultadas. Puedes recurrir al cuadernillo Técnicas de estudios y estrategias para el aprendizaje del Ministerio de Educación (págs. 25-27) https://bit.ly/mectecnicasdeestudio

PROPUESTA 5

¿Qué es la IA?

Antes de la lectura

1. ¿Qué es la inteligencia artificial (IA)?

2. En la actualidad, ¿en qué situaciones se puede usar la IA?

3. Define en tres ideas qué es el Chat GPT y qué funciones tiene. ¿Lo sueles usar? ¿Para qué o en qué situaciones?

Durante la lectura

1. Lee atentamente el siguiente texto:

¿Qué es la IA?

Definir la IA no es fácil, ya que el concepto de inteligencia per se no es del todo preciso. En términos coloquiales, IA se usa cuando una máquina es capaz de imitar las funciones cognitivas propias de la mente humana, como: creatividad, sensibilidad, aprendizaje, entendimiento, percepción del ambiente y uso del lenguaje. Un subcampo de la IA que ha ganado auge en años recientes es el aprendizaje computacional (machine learning), donde un sistema aprende a ejecutar tareas, ya sea a partir de ejemplos o mediante prueba y error.

Los modelos llamados redes neuronales están inspirados en una forma simplificada del funcionamiento de las neuronas. En la actualidad, las redes neuronales profundas (con gran número de células bajo un orden jerárquico), han sido muy exitosas en tareas de alta complejidad, como la identificación de objetos en imágenes y el reconocimiento del habla humana.

Una propiedad muy importante de cualquier sistema inteligente es su transparencia, es decir, qué tan fácil es interrogarlo sobre su propio funcionamiento. Por ejemplo, si un vehículo autónomo no reconoce a un peatón y sufre un percance, un modelo transparente puede ser interrogado para averiguar por qué falló. Las redes neuronales, en cambio, no son transparentes, son modelos tipo caja negra, en las que conocemos la información recibida y las respuestas, pero no la forma como se llega a la solución; es decir, no existen las técnicas adecuadas para descifrar los patrones de aprendizaje a partir de los datos. Otra propiedad importante de un modelo es su honestidad, esto es, qué tan confiables son

sus predicciones. Por ejemplo, un sistema inteligente para diagnosticar cáncer debe discernir entre tejido benigno y maligno y ser capaz, también, de indicarnos cuál es la probabilidad de acierto. Así, podremos distinguir las muestras que tienen una alta probabilidad de ser malignas sobre aquellas donde no hay certeza alguna.

Una clase diferente son los modelos gráficos probabilísticos, que representan explícitamente las relaciones entre las diferentes variables de un problema. A diferencia de las redes neuronales, en este caso existe un registro de cada decisión tomada que puede consultarse y revisarse permitiendo interrogar al modelo sobre las decisiones y medir la confiabilidad de sus predicciones.

Una aplicación exitosa de los modelos gráficos probabilísticos es el diagnóstico de enfermedades. Por ejemplo, para determinar si un paciente tiene malaria, el modelo toma en cuenta la relación entre variables, como los síntomas del paciente (cansancio, vómito, dolor de cabeza, etc.), los viajes que realizó recientemente (en particular si estuvo en alguna región de alto riesgo) y los resultados de estudios médicos; asigna un grado de importancia a cada variable y permite a los analistas determinar cuáles factores son cruciales al tomar una decisión.

Los modelos gráficos probabilísticos presentan ventajas, pero también algunas desventajas. Cuentan con características deseables, como transparencia y honestidad, pero aún no han alcanzado el desempeño logrado por los modelos de redes neuronales en tareas de gran complejidad. Existe una compensación entre el desempeño de la tecnología actual y las características que son deseables para poder implementarla en la sociedad.

Fuente:https://www.foroconsultivo.org.mx/INCyTU/documentos/Completa/INCYTU_18-012.pdf

2. Responde:

a. ¿Cómo se define a la inteligencia artificial según el texto?

b. ¿Qué es el aprendizaje computacional y cómo se diferencia de las redes neuronales?

Después de la lectura

1. Explica la importancia de la transparencia en un sistema inteligente. Para ello, realiza un esquema con los datos que te aportó el texto. Puedes guiarte con el cuadernillo *Técnicas de estudio y estrategias para el aprendizaje* del Ministerio de Educación de Corrientes, (pág. 33). https://bit.ly/mectecnicasdeestudio

2. Escribe un breve párrafo reflexionando sobre cómo la inteligencia artificial puede afectar tu vida diaria. Considera tanto los beneficios como los posibles riesgos. Fundamenta tu opinión.

PROPUESTA 6

Seguridad informática

Antes de la lectura

1. Organizados en grupos de 5 o 6 estudiantes, dialoguen sobre:

a. ¿Qué cambios observan como usuarios digitales en sus tareas y obligaciones cotidianas, ya sea en la escuela, en las redes, grupos o en otros dispositivos que utilizan?
b. Registren sus conclusiones para luego compartirlas con los otros grupos.
c. Elaboren conclusiones finales que resuman las intervenciones de todos los grupos y transcríbanlas en sus carpetas.

2. ¿Cómo protegen sus datos personales al ingresar a un dispositivo digital?

Durante la lectura

1. Lee en voz alta, con entonación, el siguiente texto. Se sugiere una lectura a coro, primero lee un párrafo y luego continúa tu compañero, así hasta que lean todos los estudiantes del aula.

Seguridad Informática

La seguridad informática ha surgido como una necesidad, debido a los intensos cambios en el sector productivo, la educación e, inclusive, la manera en cómo vive la sociedad mundial gracias a la transformación digital.

Por este motivo, la información se ha convertido en uno de los activos principales de las empresas e individuos y, para mantener sus datos resguardados, deben invertir en este tipo de seguridad.

Este novedoso método para blindar los datos se encarga de prevenir y detectar el uso no autorizado de un sistema informático. Implica la protección contra intrusos que pretendan utilizar las herramientas y/o datos empresariales maliciosamente o con intención de lucro ilegítimo.

¿Qué es la informática?

Antes de irnos con la seguridad informática, primeramente, es indispensable conocer el siguiente concepto: la informática.

Esta es la rama de la Ingeniería que se basa en el estudio del hardware, redes de datos y los softwares que son requeridos para automatizar la información.

- **Hardware:** Es la parte física del ordenador, tablet, laptops, smartphones, etcétera. Están formados internamente por componentes electrónicos que permiten su funcionamiento.

- **Software:** Son los programas, reglas informáticas, etcétera, que permiten ejecutar las innumerables tareas que puede hacer una computadora.

Seguridad informática: su concepto

La seguridad informática se encarga de eludir y localizar el uso indebido de un sistema informático con la finalidad de resguardar la integridad y privacidad de los datos almacenados. Esta seguridad no se limita, ya que, puede ser particular —individuos con su propio sistema— o empresarial.

Las medidas de seguridad que abarca pueden ser: antivirus, firewalls u otras medidas que dependen del usuario como, por ejemplo, la activación o desactivación de algunas de las funciones del software como el Java, ActiveX, para asegurar el uso de la computadora, los recursos de red o del Internet.

La seguridad informática busca la preservación de la confidencialidad, integridad y disponibilidad de la información. Debido a que la información corporativa es uno de los activos más importantes que maneja toda empresa, se encargan de invertir en un sistema de gestión que busque garantizar su protección.

Pero, ¿qué es un sistema de gestión? Es la forma en la que una organización maneja su gestión interna con la finalidad de cumplir sus metas u objetivos.

Principios de la seguridad informática

Las áreas principales de la información que cubren son 4: Integridad: Se trata de la autorización de algunos usuarios en particular para el manejo y modificación de datos cuando se considere necesario.

Confidencialidad: únicamente los usuarios autorizados tienen acceso a los distintos tipos de recursos, datos e información, logrando filtrar y robustecer el sistema de seguridad informática.

Disponibilidad: los datos deben estar disponibles para el momento en que sean necesitados. Es la capacidad de permanecer accesible en el sitio, momento y en la forma que los usuarios autorizados lo necesiten.

Autenticación: se basa en la certeza de la información que manejamos. Es indispensable contar con software y un hardware con perfecta disponibilidad, de esta forma, estaremos reduciendo los tiempos muertos y evitaremos pérdidas económicas, daños físicos y, en el peor de los casos, una posible amenaza que atente contra la vida humana.

Tipos de amenazas

Dentro de las amenazas, podemos señalar 3 tipos:

1. Amenazas humanas

Un gran número de ataques informáticos son de naturaleza humana que por motus propio, o por error, pueden lograr ocasionar daños severos. Podemos encontrar:

I. Ataques pasivos: pretenden sustraer la información, pero, sin llegar a modificarla. Pueden ser:

Usuario con conocimientos básicos: los cuales ingresan a los dispositivos sin tener una mala intención, utilizando tácticas simples.

Hackers: son profesionales que emplean sus habilidades informáticas para encontrar defectos y vulnerabilidades. Comúnmente, no son peligrosos, pero mientras menos expuesto estés, mejor.

II. Ataques activos: manipulan la información para su propio beneficio o para dañar dolosamente. Por ejemplo:

Exempleados: Que aprovechan sus conocimientos del sistema para vulnerar la seguridad.

Crackers: Son profesionales informáticos. Aprovechan sus conocimientos para manipular los sistemas y dañarlos.

¿Qué semejanzas y diferencias hay entre un cracker y un hacker?

La principal diferencia entre cracker y hacker se puede observar a través de los siguientes puntos: los hackers son personas que usan su conocimiento para un buen propósito y no dañan los datos, mientras que un cracker es alguien que irrumpe en el sistema con un propósito malicioso y daña los datos intencionalmente.

2. Amenazas lógicas

Existen dos tipos de softwares que pueden dañar un sistema informático:

Vulnerabilidades del software: Son posibles errores en el sistema operativo que ponen en riesgo la seguridad del dispositivo si llega a ser encontrado por un atacante.

Software malicioso: Existen programas con objetivos malignos, como, por ejemplo, los virus, gusanos o troyanos.

3. Amenazas físicas

Se originan por causas principales tales como:

Fallo del dispositivo: Ante un agente externo como una caída del sistema eléctrico o por un desperfecto físico del dispositivo.

Accidentes: Que pueden ocurrir por un sinnúmero de razones. Catástrofes naturales: Como terremotos, tormentas, etcétera.

6 tipos de amenazas informáticas

La criminalidad cibernética es un problema real, por este motivo, debemos conocer los peligros que acechan la integridad de los datos sensibles para garantizar la estabilidad jurídico-operativa de nuestra organización o de nuestro propio dispositivo.

Estos son algunos de los más importantes:

1. Phishing: se vale de técnicas de la ingeniería social, donde el "phisher" se hace pasar por una persona o empresa de confianza, por lo general por correo electrónico, redes sociales, entre otros, para sustraer información personal y financiera de manera ilegítima.

2. Malware o "malicious software": engloba todo programa o código informático cuyo objetivo es causar daño cibernético.

3. Spam: son mensajes no solicitados, mayormente en términos publicitarios, que son enviados de forma masiva sin autorización ni solicitud alguna para perjudicar de alguna manera al receptor.

4. **Spyware o troyano:** es un programa espía — un tipo de malware— ingresa en un ordenador y recopila información de la computadora, para luego transmitirla a un ente externo sin el consentimiento del usuario.

5. **Virus informático:** es un software que su finalidad es alterar el normal funcionamiento de cualquier dispositivo informático sin permiso del usuario.

6. **Pharming:** es un tipo de ciberataque que consiste en convencer al usuario de ingresar a un sitio web malicioso redireccionándolo con una URL (unidad remota lógica). Una vez dentro, los cibercriminales buscan que el usuario brinde información privada.

Estos son algunos de los más destacados actualmente, debemos seguir este tema de cerca ya que la tecnología avanza a pasos agigantados y los ciberataques no se quedan atrás. La seguridad informática es un aspecto muy importante que cualquier empresa debe dedicar tiempo, esfuerzos y recursos. Los datos sensibles de tu organización son tus nuevos activos. ¡Protégelos!

Fuente:
https://wwwsi.frsn.utn.edu.ar/tecnicas3/presentaciones/Seguridad%20informatica.pdf

3. Subraya las ideas principales de cada párrafo y luego elabora una síntesis del texto. Puedes utilizar el cuadernillo Técnicas de estudio y estrategias para el aprendizaje del Ministerio de Educación de Corrientes (págs. 20). https://bit.ly/mectecnicasdeestudio

Después de la lectura

1. Explica las diferencias y similitudes entre un hackers y un crackers.

2. Elabora un esquema de los contenidos del texto. Puedes guiarte con el cuadernillo mencionado en la actividad anterior, (págs. 20-23). https://bit.ly/mectecnicasdeestudio

3. Subraya las ideas principales de cada párrafo y luego elabora una síntesis del texto. Puedes utilizar el cuadernillo Técnicas de estudio y estrategias para el aprendizaje del Ministerio de Educación de Corrientes (págs. 20- 23). https://bit.ly/mectecnicasdeestudio

Actividades de extensión

Por un error de tipeo las características de estas amenazas aparecen desordenadas. Sugiere la alternativa correcta.

Criminalidad cibernética					
Phishing	**Spam**	**Malware**	**Virus informático**	**Spyware o troyano**	**Pharming**
espía programa	daño programa o informático que código causa cibernético	ingresar malicioso lógica) remota convence al a un sitio web a con usuario una URL (unidad	mensajes mayormente solicitados, no publicitarios en términos	software dispositivo altera normal que funcionamiento de un el	correo una persona sociales, sustrae o empresa, financiera por electrónico, redes entre otros, información personal y

PROPUESTA 7

Área ocupacional

Antes de la lectura

1. Explica con tus palabras el significado del título del texto que se presenta a continuación.

2. Menciona todas las áreas ocupacionales que conozcas donde puede desempeñarse un técnico en Informática Profesional y Personal.

Durante la lectura

1. Lee de manera silenciosa e individualmente el siguiente texto.

I.1.2. Área ocupacional: El técnico en Informática Profesional y Personal puede desempeñarse en un área ocupacional que incluye, fundamentalmente, actividades de apoyo y asistencia al usuario de informática, quien muchas veces no está en condiciones de aprovechar efectiva y eficientemente los recursos que tiene a su disposición.

Esta asistencia puede formar parte de un servicio externo o constituir una función interna de la organización en la que se desempeñe el usuario.

El perfil previsto se recorta dentro de un área denominada genéricamente “informática”, pero que requiere una delimitación más precisa. Se ha realizado una clasificación "ad hoc" de los grupos de aplicaciones informáticas, con énfasis puesto en diferenciar el perfil de profesionalidad y el posible efecto en la empleabilidad.

- Informática organizacional, empresaria, estratégica o de "misión crítica".
- Informática personal, profesional, educativa, táctica o departamental.
- Informática dedicada a propósitos específicos.
- Informática oculta en otros productos.
- Informática del hogar, lúdica, recreacional.

La atención se centra en dos de grupos de aplicaciones: la informática del hogar y la informática profesional y personal, abarcativa de usuarios individuales, actúen o no en relación de dependencia, y usuarios colectivos de aplicaciones orientadas al sector, departamento o unidad en la que actúan, ya sea dentro de organizaciones grandes, PyMEs o establecimientos educativos.

Estas aplicaciones se basan en productos o servicios informáticos formados por un equipo computador básico más componentes adicionales - “hardware”, “software”, redes de comunicación, proveedores de contenido- que definen su configuración final, presentación y comercialización. Las tendencias señalan que este equipo básico será el que sustituya o reemplace a la computadora personal (PC) actual y una gran parte de los programas, servicios y contenidos estarán distribuidos dentro de redes.

El diseño y desarrollo, la producción y el armado, la distribución y la comercialización de los equipos básicos, sus componentes y adicionales son realizados por empresas dedicadas que utilizan especialistas con una sólida formación universitaria y profundos conocimientos tecnológicos, requeridos para enfrentar la complejidad de los productos y servicios informáticos.

En el otro extremo de la cadena se encuentra el usuario final, a quien se le demanda conocer, en mayor o menor grado, el funcionamiento de los componentes necesarios para el desarrollo de sus tareas y que no dispone del tiempo o la vocación para dominar los conocimientos indispensables para alcanzar una efectiva y eficiente utilización de sus recursos informáticos. Esta brecha entre ambos tipos de conocimientos y agentes se cubre con una actividad denominada Apoyo o Atención al Usuario (helpdesk).

Este rol de apoyo y asesoramiento suele estar desempeñado por personas con formaciones profesionales diversas, con o sin títulos de enseñanza media o superior, pero sobre todo con una gran dosis de autoaprendizaje. La creciente heterogeneidad de los productos y servicios, de los usuarios y de los campos de aplicación de la informática (personal, profesional y del hogar) delimitan un área ocupacional específica a ser cubierta por un perfil profesional formado sistemáticamente al efecto.

Este técnico podrá ejercer su actividad profesional en los siguientes ámbitos de desempeño:

- Dentro de la misma organización - institución, empresa o entidad - que el usuario. Como apoyo directo dentro de la misma unidad operativa que éste o como apoyo organizacional, formando parte de una unidad específica dedicada a la asistencia en toda la organización.

- Otro ámbito está integrado por las personas o empresas que desempeñan las funciones descriptas en el punto anterior en forma externa ("tercerización"), siendo el apoyo o asistencia provista en forma central o distribuida, pero desde fuera.

- La contratación directa, por abono mensual o bajo llamada, del técnico es frecuente en los casos de las organizaciones pequeñas, los profesionales independientes y los usuarios hogareños. Esto abre la posibilidad de un autoempleo o pequeño emprendimiento.

- Las empresas proveedoras de servicios integrados, según análisis de tendencias de mercado, prestarán el servicio de asistencia a sus usuarios; esto indica un área adicional de desempeño del técnico.

En las consultas efectuadas no se detectaron variaciones regionales significativas. La más importante corresponde a la mayor o menor modernidad de los equipos, componentes y sistemas utilizados; pero esta diferencia, generada por la mayor o menor inversión, está presente en todas las regiones y aún dentro de ellas. Es de esperar que las relaciones laborales y humanas del Técnico en Informática Profesional y Personal con su entorno se desarrollen dentro de las siguientes pautas:

- La mayor parte del accionar de este técnico se realiza en forma individual, en relación uno a uno con el usuario, con gran autonomía e independencia.

- Puede formar parte de un grupo de técnicos dedicados a tareas de apoyo, pero son escasos los momentos en que interactúan entre sí. Puede colaborar en tareas de diagnóstico, de medición de comportamientos, o en intercambio de experiencias y estadísticas de fallas.

- Los superiores jerárquicos pueden tener distintas formaciones, ya que normalmente realizan una supervisión más administrativa y de desempeño que técnica.

En caso de acceder a formación universitaria o superior, puede pasar a desempeñarse en posiciones más cercanas al diseño, desarrollo, mantenimiento funcional e integral, e implementación de productos y servicios informáticos.

Fuente: ***Perfil Profesional del TTP en Informática Profesional y Personal según Resolución del CFCyE N.° 68/98. Ministerio de Cultura y Educación • INET.***

2. Nombra y describe en qué ámbitos ocupacionales se desempeña un técnico en Informática Profesional y Personal.

3. Vuelve a leer el texto y realiza una síntesis del área ocupacional específica a ser cubierta por un perfil técnico en Informática Profesional y Personal formado sistemáticamente para tales efectos.

4. Elabora un cuadro comparativo de diferencias entre la informática organizacional y la informática personal. Puedes guiarte con el cuadernillo mencionado en la actividad anterior, (págs. 48-49). https://bit.ly/mectecnicasdeestudio

Después de la lectura

1. Diseña un plan de asistencia técnica para una pequeña empresa, considerando los ámbitos de desempeño del técnico en Informática Profesional y Personal.

2. Reflexiona sobre la importancia del técnico en Informática Profesional y Personal en la sociedad actual. Fundamenta tu opinión.

Bibliografía

Casarotto, C. (3 de junio de 2022). *¿Qué son las cookies y cuál es su finalidad en los sitios web?* Rockcontent blog. https://rockcontent.com/es/blog/cookies/

Herrero, M. E. (2016). *Técnicas de estudio y estrategias de aprendizaje: herramientas para el éxito académico.* Editorial Bonum.

https://www.educ.ar/recursos/159083/tres-hitos-de-la-inteligencia-artificial-turing-deep-blue-y-

https://www.foroconsultivo.org.mx/INCyTU/documentos/Completa/INCYTU_18-012.pdf

https://www.inet.edu.ar/

https://wwwsi.frsn.utn.edu.ar/tecnicas3/presentaciones/Seguridad%20informatica.pdf

Marina, J. A. (2011). *Aprender a estudiar.* Editorial Ariel.

Ministerio de Educación de Corrientes (2023). *Técnicas de estudio y estrategias para el aprendizaje.*

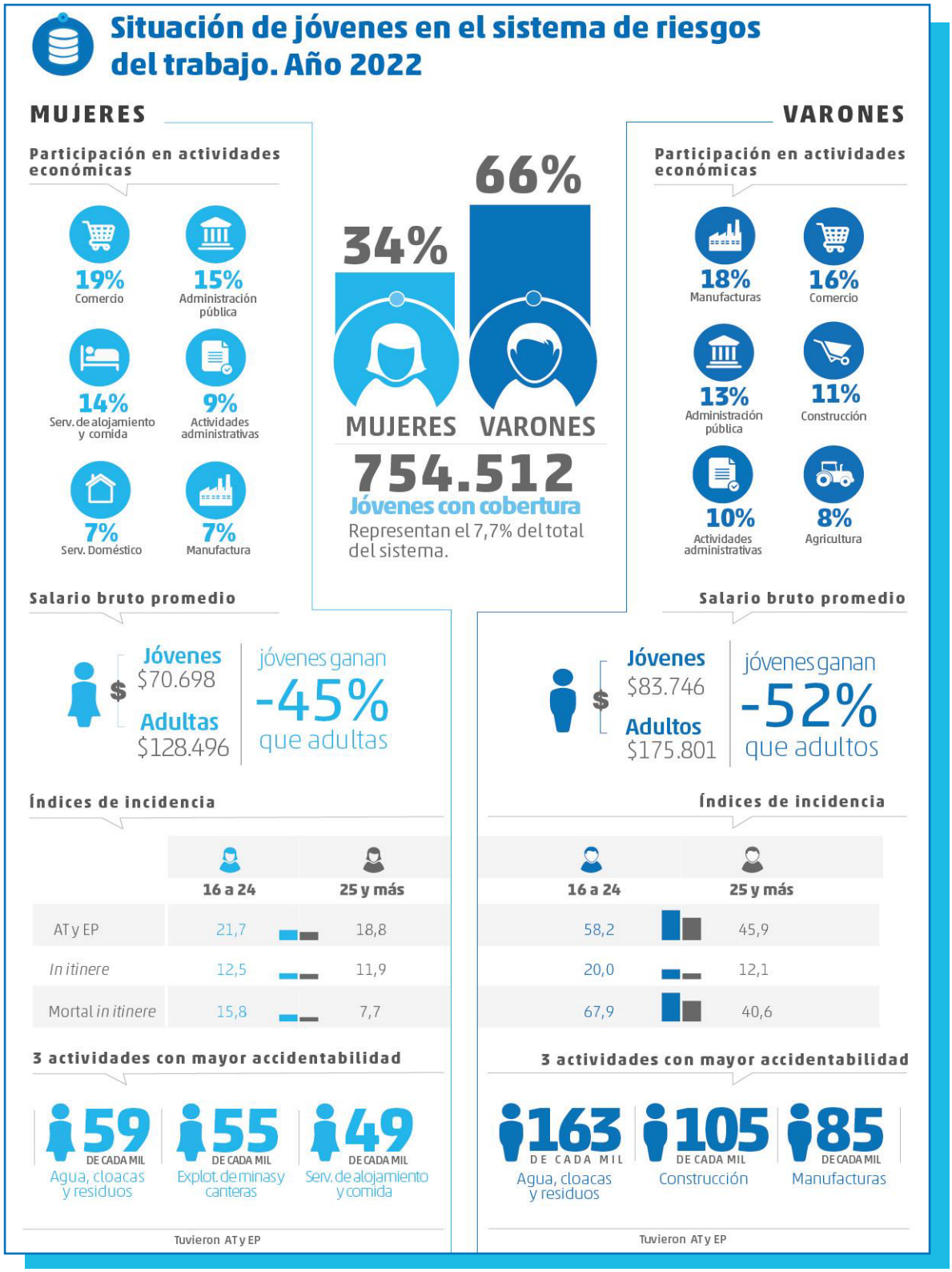
Pallero, M. y Heguiabehere, J. M. (2023). *Seguridad de la información y ciberseguridad*. Informe técnico. Ministerio de Ciencia, Tecnología e Innovación. https://fundacionsadosky.org.ar/wp-content/uploads/2023/12/Seguridad-de-la-informacion-y-ciberseguridad.pdf

Rodríguez, M. L. (2013). *Estrategias de aprendizaje y técnicas de estudio: Guía práctica para mejorar el rendimiento académico.* Editorial Paidós.

PROPUESTA 1

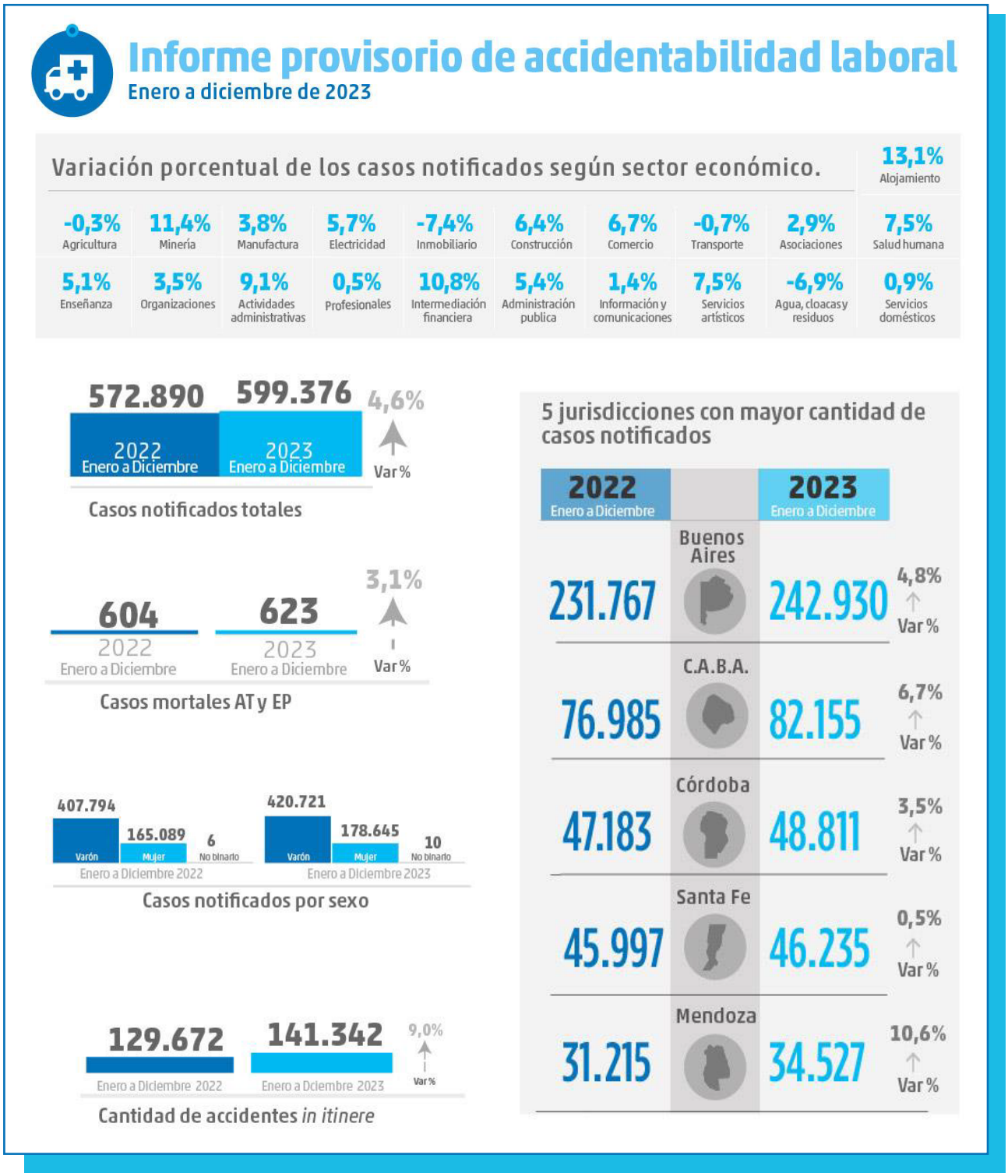
Estadística y probabilidad

1. A partir del análisis de la siguiente infografía, responde:



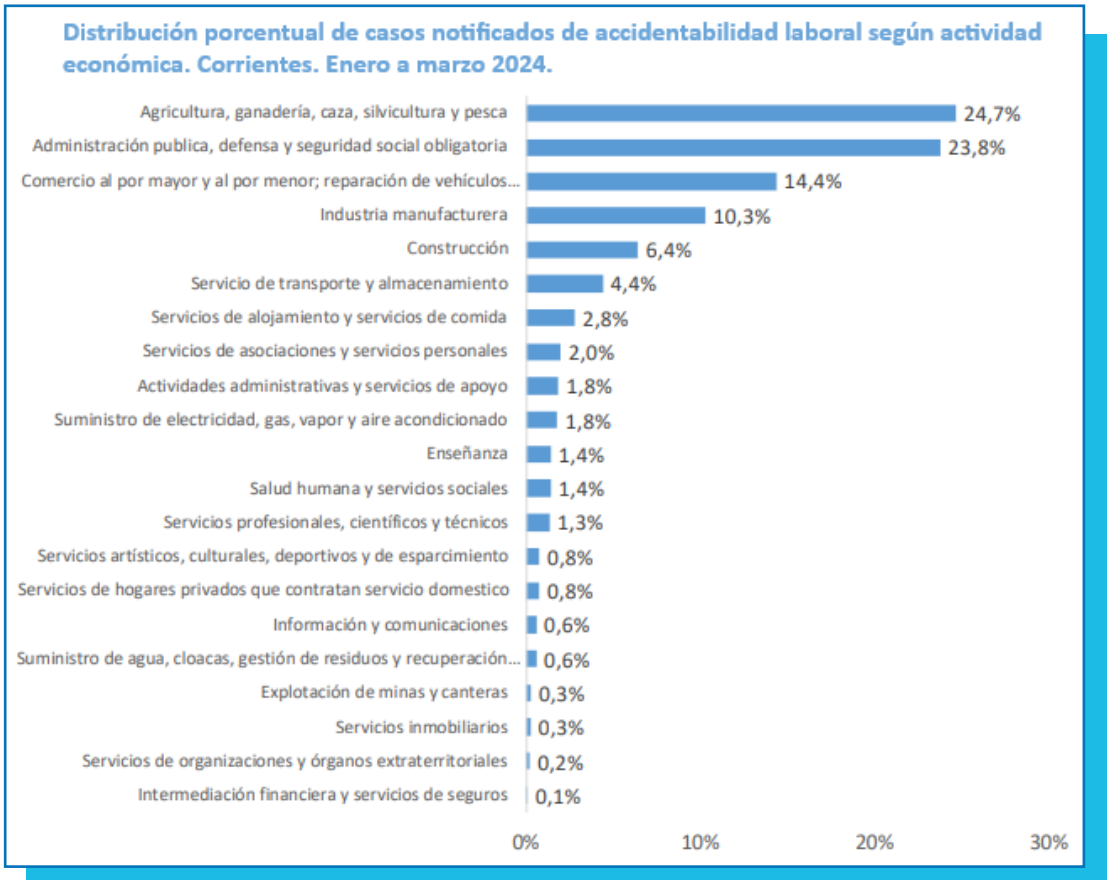
a. ¿Cuáles son las variables que se estudian? ¿De qué tipo son?
b. ¿Es posible determinar cuál es la población objeto de estudio? ¿Por qué?
c. ¿Qué preguntas se pueden responder a partir de la información brindada? Escribe un mínimo de cinco preguntas.

2. A partir del análisis de la siguiente infografía, contesta:



a. ¿Cuáles son las variables que se estudian? ¿De qué tipo son?
b. ¿Se puede determinar cuál es la población que se estudia? ¿Por qué?
c. ¿Qué preguntas es posible plantear a partir de la información presentada? Escribe un mínimo de cinco preguntas.

3. A partir de la información que ofrece el gráfico, resuelve las consignas que se proponen a continuación.



Fuente: Informe provisorio de accidentabilidad laboral en Corrientes (1.574 casos notificados). Superintendencia de Riesgo de Trabajo.

a. Describe la información que brinda el gráfico.
b. ¿Cuál es la variable en estudio? ¿De qué tipo es?
c. A partir del gráfico, confecciona una tabla de frecuencias.
d. Teniendo en cuenta la información obtenida, ¿qué interpretación de los datos puedes hacer? Justifica tu respuesta.

4. Elabora una infografía que presente los datos analizados en la actividad anterior. (Sugerencia para el diseño de la infografía: https://www.canva.com/)

5. Teniendo en cuenta las actividades resueltas, responde:

a. ¿Cuáles son las variables estadísticas que se pusieron en juego en cada uno de los problemas?
b. ¿De qué manera se pueden organizar los datos obtenidos para que su lectura e interpretación resulte accesible?

c. A partir de los distintos registros que se utilizaron en estas actividades para representar la información recolectada, ¿hay alguna representación que te haya resultado más adecuada que otra? ¿Por qué?

PROPUESTA 2 — Interpretación y estimación por intervalos

1. Una fábrica produce dardos con diámetros que tienen un desvío estándar σ= 0,25mm. De un lote grande, se seleccionó una muestra aleatoria simple de 40 dardos, y se obtuvo un promedio de 3,09 mm en sus diámetros.

a. Obtén un intervalo de confianza de aproximadamente el 95% para la media de los diámetros de todos los dardos producidos de la misma forma.
b. Realiza lo mismo que en el punto anterior, pero con una confianza aproximada del 99.7%
c. ¿De qué tamaño debe ser la muestra para que la longitud del intervalo de confianza del 95% sea 0,1 mm?

2. ¿Cómo afecta un aumento del nivel de confianza del 95% al 99,7% al **intervalo de confianza** de una proporción? Selecciona una respuesta y justifica tu elección.

a. Aumenta la longitud del intervalo en 4,7%.
b. Reduce la longitud del intervalo en 4,7%.
c. Aumenta la longitud del intervalo en 50%
d. Reduce la longitud del intervalo en 50%.
e. No puede saberse sin conocer el tamaño de la muestra.

3. Se prueban 49 autos de un nuevo modelo y se registran los litros de nafta consumidos en un recorrido de 100 km, obteniéndose una media muestral, x=6,8 litros y un desvío estándar muestral, s=1,4 litros. Selecciona el intervalo de aproximadamente 95% de confianza para la cantidad media de litros de nafta consumida por ese tipo de vehículo en 100 km. Justifica tu respuesta.

a. [5,4; 8,2] **b.** [6,6; 7,0] **c.** [6,4; 7,2] **d.** [6,2; 7,4]

4. Se sabe que el 82 % de los alumnos del último año de las escuelas secundarias planean seguir estudios superiores. Supongamos que se selecciona una muestra aleatoria simple de alumnos del último año de dichas escuelas y se obtiene un intervalo de confianza en base a la proporción que manifiesta tener interés en continuar sus estudios. Selecciona la opción correcta y justifica tu elección:

a. El centro del intervalo de confianza es 0,82.
b. El intervalo de confianza contiene el valor 0,82.
c. Un intervalo de confianza del 99,7% contiene el valor 0,82.

5. ¿Cómo varía la longitud del intervalo de confianza si se duplica el tamaño de la muestra, manteniendo constantes las demás condiciones? Justifica tu respuesta.

a. Se duplica la longitud.
b. La longitud se reduce a la mitad.
c. La longitud se multiplica por 1,414.
d. La longitud se divide por 1,414.
e. No se puede saber.

6. Una encuesta reveló que el porcentaje de personas a las que no le gusta planificar sus vacaciones con más de un mes de anticipación es 68% con un margen de error del ± 5%. ¿Qué significa el ± 5%? Selecciona la opción correcta y justifica tu elección.

a. Se encuestó al 5 % de la población.
b. En la muestra, el porcentaje de personas a las que no les gusta planificar sus vacaciones con más de un mes de anticipación se encontró entre 63% y 73%.
c. En la población, el porcentaje de personas a las que no les gusta planificar sus vacaciones con más de un mes de anticipación está entre 63% y 73%.
d. Se encuestó entre 63% y 73% de la población.
e. Sería raro que en la población el porcentaje de personas a las que no le gusta planificar sus vacaciones con más de un mes de anticipación esté fuera del intervalo de 63% a 73%.

7. En un estudio sobre hábitos de vida saludable en adultos, se encuestó a 300 hombres y 400 mujeres de 30 años. Los resultados mostraron que el 65% de los hombres realizaban actividad física de forma habitual (3- 4 veces por semana) y el 48% de las mujeres hacían actividad física de forma habitual (3- 4 veces por semana).

Estima la diferencia en la proporción de personas que realizan actividad física entre hombres y mujeres en esta población:

a. 17% ± 0,38 %
b. 17% ± 7,48 %
c. 55,6 % ± 7,48 %
d. 56,5 % ± 0,74 %
e. 56,5 % ± 0,38 %

8. Se realizó un muestreo aleatorio simple, de un embarque de 50.000 piezas delicadas, registrándose 16 piezas dañadas de un total de 220 observadas. Obtén un intervalo del 95% de confianza para estimar la verdadera proporción y, a partir de él, la cantidad de piezas dañadas.

Bibliografía

Kelmansky, D. (2009). *Estadística para todos. Estrategias de pensamiento y herramientas para la solución de problemas*. Artes gráficas Rioplatense S. A. https://www.inet.edu.ar/wp-content/uploads/2023/06/Estadistica-para-todos.pdf

Ministerio de Educación de Corrientes. *Diseño curricular Jurisdiccional. Matemática. Ciclo Superior del nivel secundario de la modalidad de Educación Técnico Profesional*.

Superintendencia de Riesgo de Trabajo (Junio de 2024). Informe provisorio de accidentabilidad laboral. *Accidentabilidad por jurisdicción*. Corrientes. https://www.srt.gob.ar/estadisticas/datos-provisorios/provincia/2021/1er%20TRIMESTRE%202024%20-%20Corrientes.pdf

Superintendencia de Riesgo de Trabajo. (s. f.). *Infografías SRT*. Ministerio de Capital Humano. https://www.srt.gob.ar/estadisticas/infografias_srt.php

CORRIENTES

Ministerio de Educación