



**Consultor
Industrial**



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR



ENERO DE 2023

SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

EJES TEMÁTICOS.

1. MANEJO DE RECURSOS DEL COMPUTADOR.



2. CONFIGURACIONES DE COMPUTADORES.



3. CIBERSEGURIDAD BÁSICA.



4. ALGUNOS TIPS INFORMÁTICOS.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS
DEL COMPUTADOR

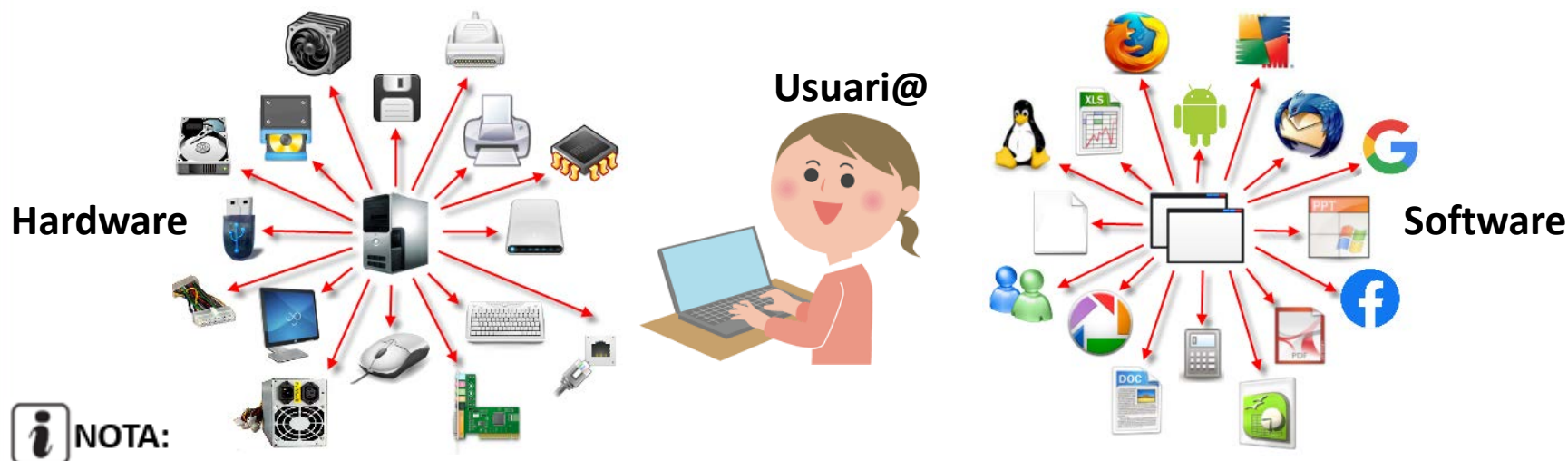


SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Funcionamiento de un computador:

El computador, es un sistema compuesto por distintos elementos físicos llamados hardware que se relacionan a través de instrucciones conocidas como software, estas instrucciones son enviadas por el usuario que interactúa entre hardware y software por medio de un lenguaje binario.



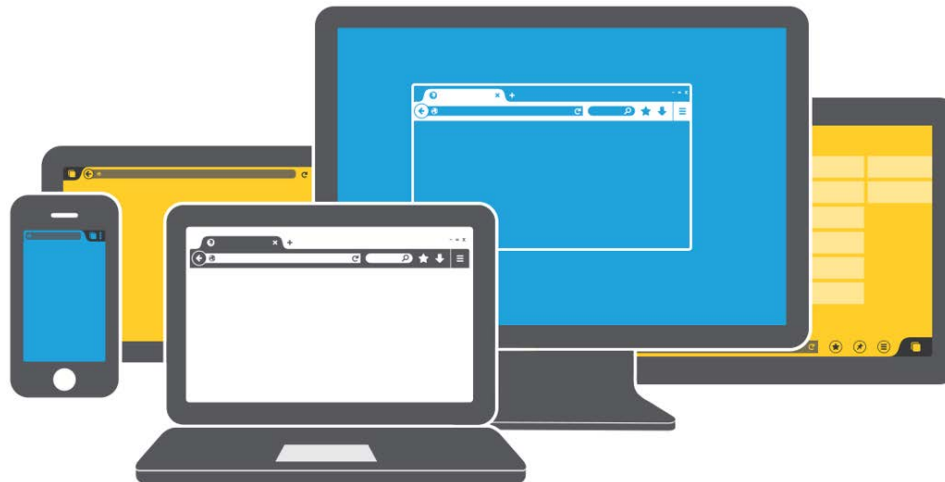
La información circula mediante pulsos eléctricos por medio de soportes como pistas o filamentos de cobre o fibra óptica (buses).

SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Conexión del usuario (interfaz):

La conexión se logra por medio de la interfaz del usuario (GUI = Graphical user interface), es el medio visual que combina una serie de controles y elementos que permiten la comunicación e interacción del usuario con el dispositivo electrónico. La interfaz es la que permite la interacción del sistema operativo con los programas, aplicaciones y diferentes recursos.



La interfaz debe ser sencilla de utilizar, fácil de comprender y de aprender.

SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Arquitectura del computador:

La arquitectura del computador es el conjunto de técnicas que permiten construir máquinas lógicas generales programables en forma práctica.



NOTA:

Técnicamente la "arquitectura" del computador es distinta a la "organización" de este.

SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Configuración de un computador:

Ir a configuración > Sistema > Acerca de



El equipo está supervisado y protegido.

[Ver detalles en Seguridad de Windows](#)

Especificaciones del dispositivo

Nombre del dispositivo	████████████████████
Procesador	Intel(R) Core(TM) i3-6006U CPU @ 2.00GHz 1.99 GHz
RAM instalada	12,0 GB (11,9 GB utilizable)
Id. del dispositivo	██
Id. del producto	████████████████████
Tipo de sistema	Sistema operativo de 64 bits, procesador x64
Lápiz y entrada táctil	La entrada táctil o manuscrita no está disponible para esta pantalla

Copiar

Cambiar el nombre de este equipo

Especificaciones de Windows

Edición	Windows 10 Pro for Workstations
Versión	21H2
Se instaló el	04-01-2021
Compilación del SO	██████████
Experiencia	Windows Feature Experience Pack ██████████

SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Importancia de las licencias originales:

El uso de software legal, garantiza el funcionamiento correcto del producto sin ninguna anomalía, permitiendo también que el usuario acceda a características adicionales.

Beneficios:

- Actualización del software con soporte directo del fabricante.
- Más seguridad ante malware u otras amenazas.
- Mejor funcionamiento del computador.
- Respaldo de información ante posibles pérdidas y otras amenazas.



BENEFICIOS



LICENCIA ORIGINAL

VS



LICENCIA PIRATA



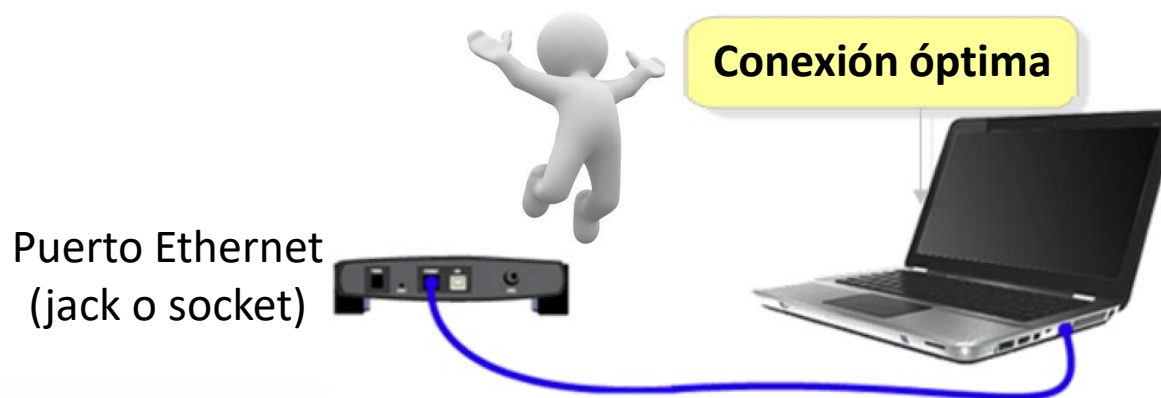
SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Transmisión de datos:

El “bit”, es la unidad que se aplica para medir la velocidad de transmisión de datos entre dos puertos o aparatos. Esta se mide en bits transmitidos por segundo (bps).

Abreviatura	Múltiplo	Descripción	Cantidad
1 Kbit/s	10^3	Kilobit por segundo	1.000 bits por segundo
1 Mbps/s	10^6	Megabit por segundo	1.000 kilobit por segundo
1 Gbp/s	10^9	Gigabit por segundo	1.000 megabit por segundo



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Conexión eficiente a internet en video conferencias:

- Considere la conectividad por cable de red.
- Cuando utilice la plataforma Zoom, configure la resolución de la cámara.
- Apague el audio cuando no intervenga.
- Si requiere grabar, utilice la opción disponible en la nube.
- Cierre las aplicaciones que no utilice.
- Comparta la pantalla solo si es necesario.
- Instale el router cerca de los dispositivos.
- Cambie a 5 GHz dentro de lo factible.



La frecuencia inalámbrica de 5 GHz proporciona mayores velocidades de datos a distancias más cortas y suele ser mucho menos ocupada que la frecuencia inalámbrica de 2.4 GHz. Si es factible, considere el cambio de router a 5 GHz para obtener un aumento de velocidad de corto alcance.

SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Navegación por Google:

- Deshabilite la opción de "recordar contraseñas".
- Cierra siempre sus sesiones al salir.
- Elimine regularmente el historial de navegación, cookies y archivos temporales.



Activación de navegación segura por Google Chrome:

Haga clic en "Configuración".

Haga clic en Privacidad y seguridad.

Seleccione el nivel de "Navegación segura" que quiera utilizar.



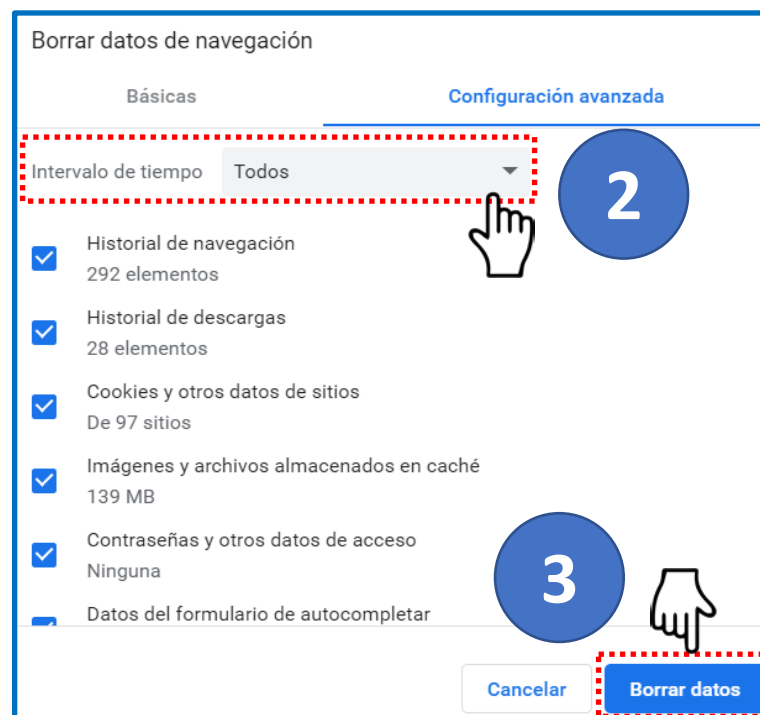
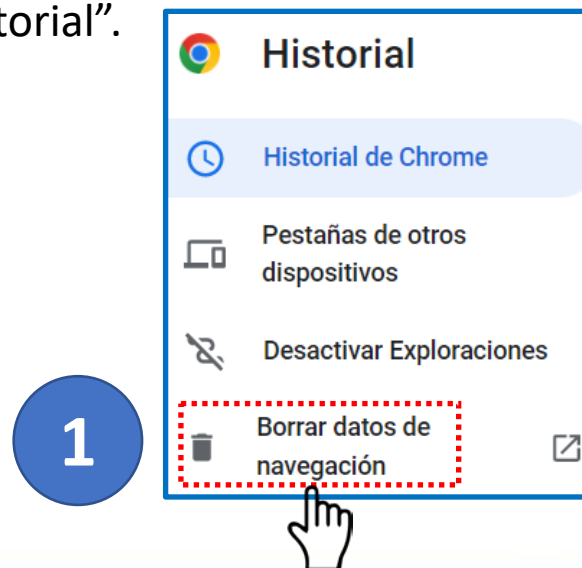
SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Limpieza de historial de Google Chrome:

Borrar el historial del navegador sirve, básicamente, para proteger su privacidad sobre todo si accede a Internet de forma puntual en un computador que no sea el suyo.

Para borrar el historial de Google Chrome:
En la esquina superior derecha, haz clic en Más. ⋮
Haga clic en “Historial”.

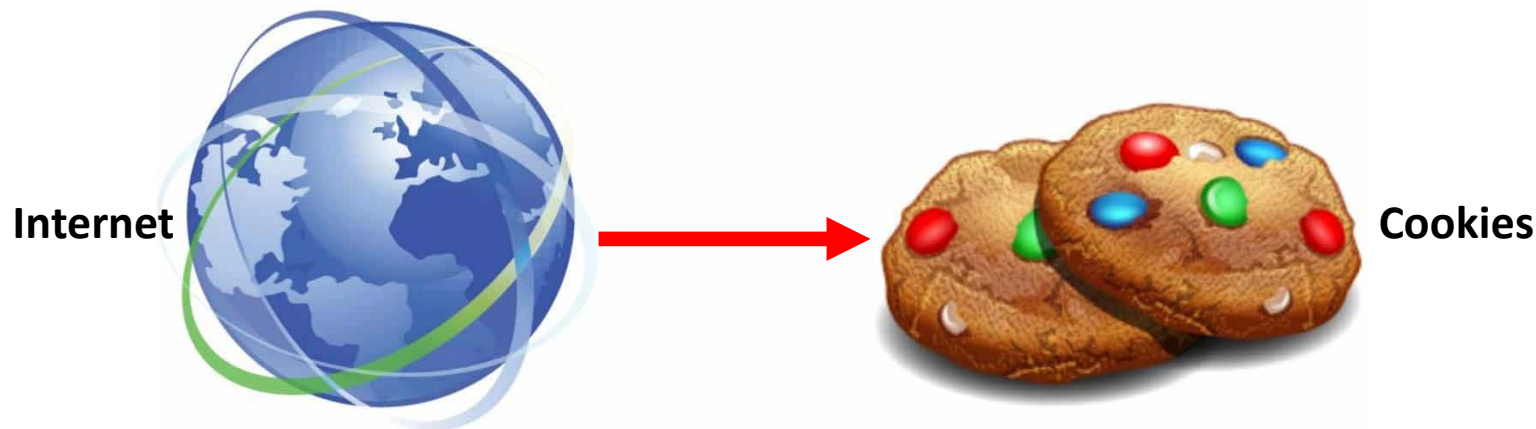


SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Cookies, ¿Qué son? y ¿para qué sirven?

Las cookies son pequeños fragmentos de texto que los sitios web que visita envían al navegador. Permiten que los sitios web recuerden información sobre su visita, lo que permite mayor facilidad para volver a visitar los sitios con más utilidad.



¿Qué pasa si acepto el uso de cookies?

Al aceptar las cookies está permitiendo que ese sitio tome sus datos como el idioma de su navegador y los intereses en función de la ubicación y el usuario (IP).

SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

¿Para qué sirven las cookies?

- Recuerda su “Login” y “Password” en aquellos sitios web que las utilizan
- Muestran avisos publicitarios online acorde a sus preferencias.
- Recuerda sus opciones elegidas en un sitio web.
- Permite compartir en sus redes sociales.
- Si está en una tienda online y cerró la página involuntariamente, puede regresar y se mantendrá todo lo que haya incluido en su carro de compras.
- Facilita su navegación web al recordar datos y ajustes importantes.
- Agiliza los procesos que se presentan al momento de acceder a un sitio web.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Cookies y seguridad:

- Los archivos cookies permiten conseguir numerosas estadísticas a los desarrolladores.
- Las cookies usan un formato de texto plano, pero no compilan códigos, por lo tanto no se pueden ejecutar de forma automática.
- Las cookies si se pueden emplear con una finalidad maliciosa, debido a su capacidad por guardar información sobre preferencias e historial de navegación del usuario.
- Las cookies se pueden utilizar para actuar como spyware (robo de datos).
- La seguridad de los sitios web es la “clave”.



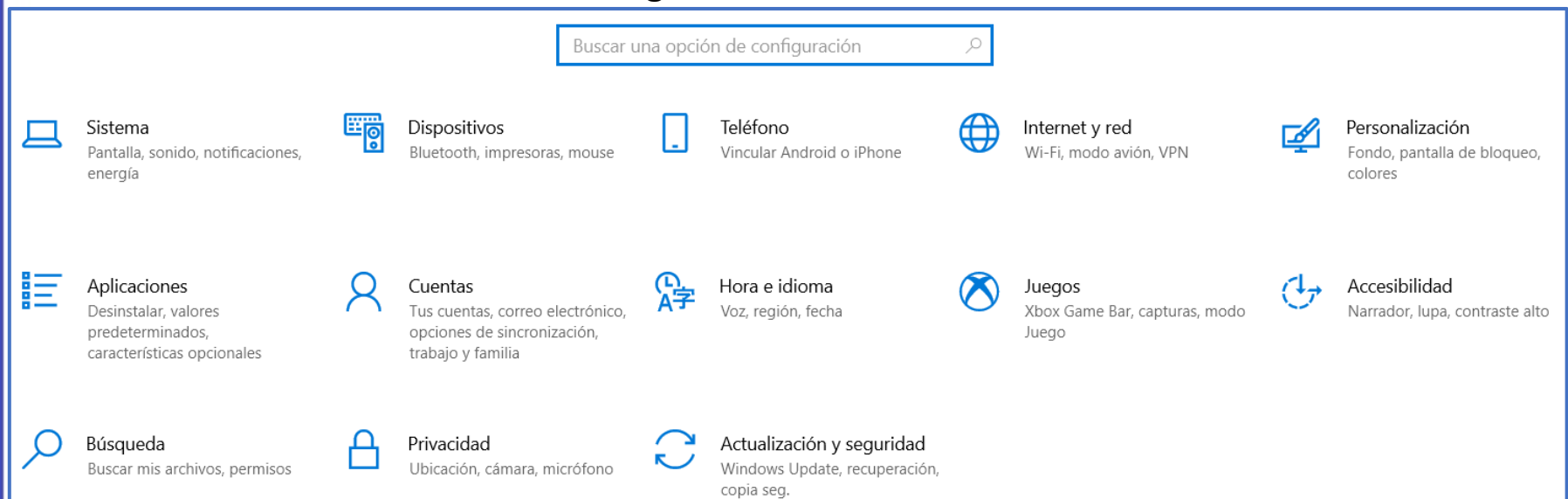
CAMBIO DE EJE TEMÁTICO



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CONFIGURACIONES DE COMPUTADORES.

Configuración de Windows

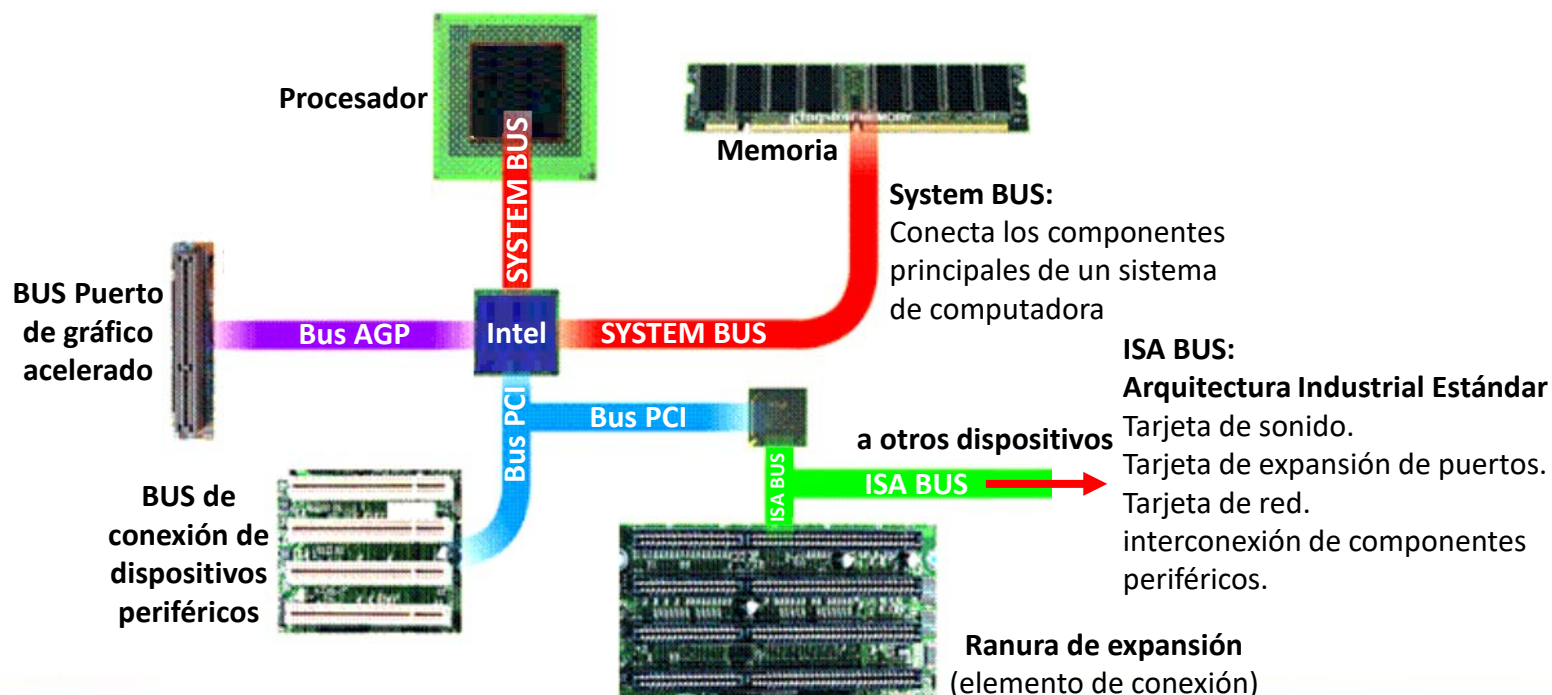


SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Los buses del computador:

Los computadores utilizan buses para enviar y recibir instrucciones e información entre sus partes como la memoria, el micro procesador, el disco duro y todos los elementos periféricos como impresoras, pendrive o celulares.

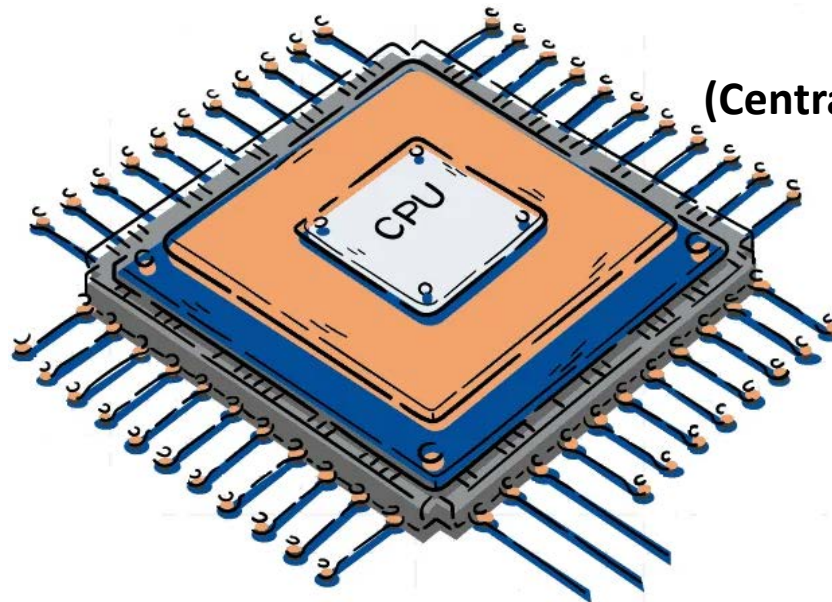


SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

CPU del computador:

Unidad Central de Procesamiento (UCP = CPU), es el cerebro del computador, cuya función es realizar los cálculos, ejecutar las diferentes aplicaciones y coordinar el uso de los diferentes dispositivos.



CPU
(Central Processing Unit)



NOTA:

La velocidad se mide en MHz (instrucciones de procesamiento por segundo).

SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CONFIGURACIONES DE COMPUTADORES.

Procesadores de computadores.

El procesador es el componente más importante de la CPU; permite todo el funcionamiento del sistema, siendo el encargado de dirigir todas las tareas del equipo y de ejecutar el código de los diferentes programas, muchas veces con la ayuda conjunta del resto de componentes y periféricos.

El procesador está formado por:

- ☐ Un conjunto de registros que almacenan datos.
- ☐ Una unidad aritmético-lógica que realiza operaciones.
- ☐ Una unidad de control que coordinar todos los componentes.
- ☐ Un reloj interno que determina la velocidad de trabajo.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CONFIGURACIONES DE COMPUTADORES.



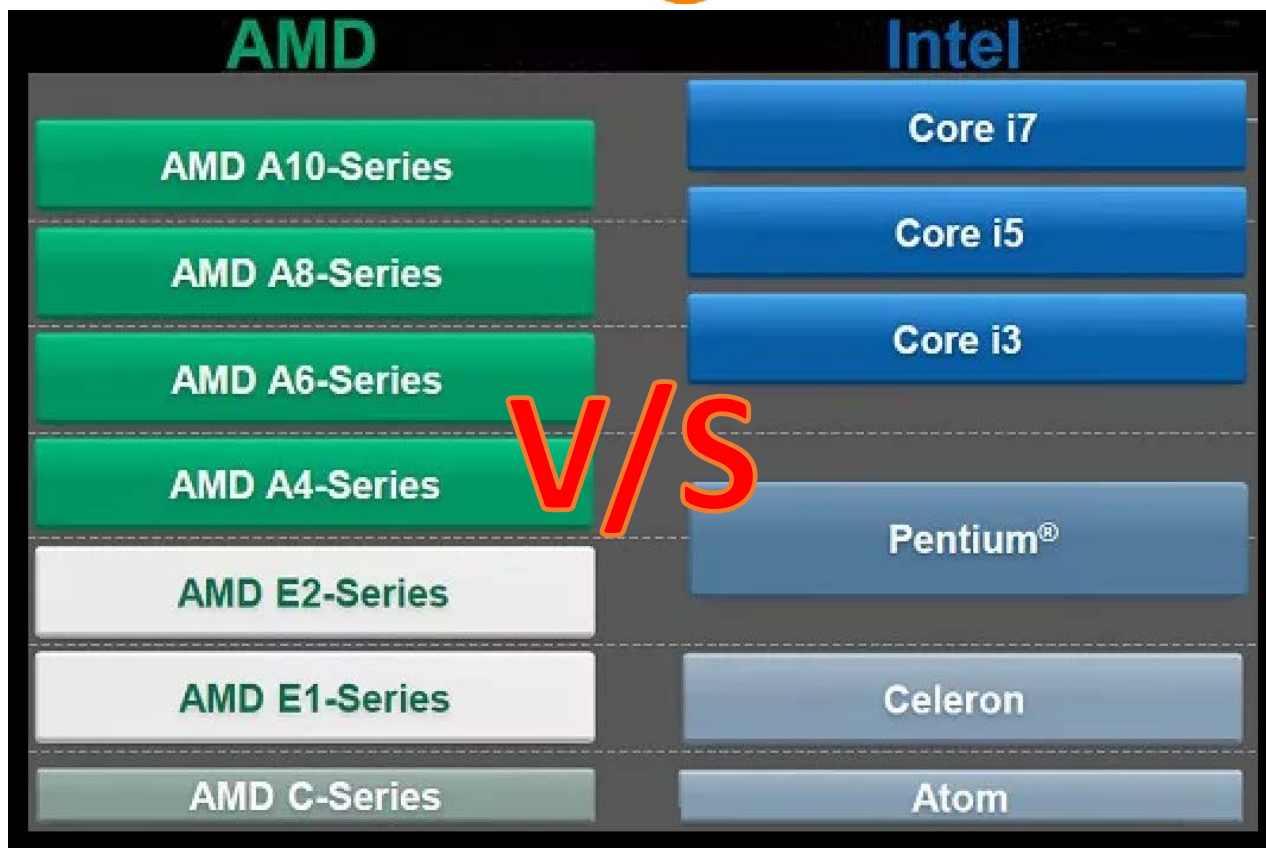
Diferencias entre procesadores de computadores.

Intel suele tener más potencia y mejor rendimiento.

AMD ofrece un buen rendimiento a un precio más económico.



Las diferencias no son tan fáciles poder determinar debido a que algunos procesadores AMD son tan buenos como los Intel.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Memoria RAM (Random Access Memory = Memoria de acceso aleatorio):

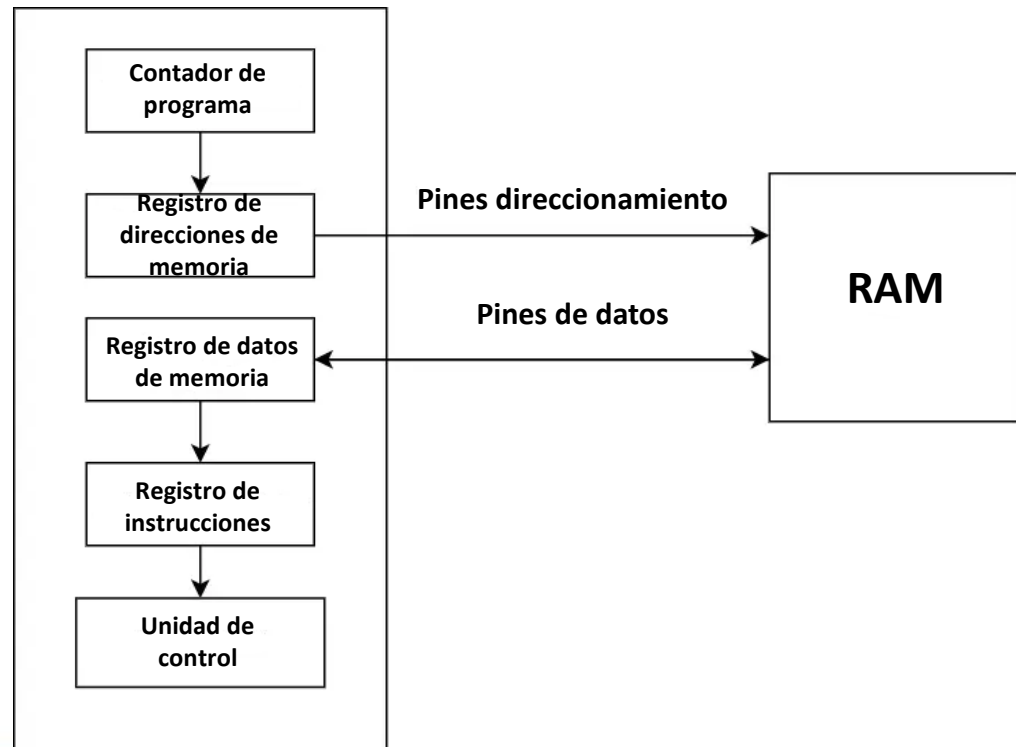
La memoria RAM es volátil, debido a que pierde la información cuando deja de recibir energía. Anexo a esta memoria se encuentra la memoria ROM, es lectura de datos la cual no puede editar o modificar éstos.

Comunicación entre la CPU y la memoria RAM.



NOTA:

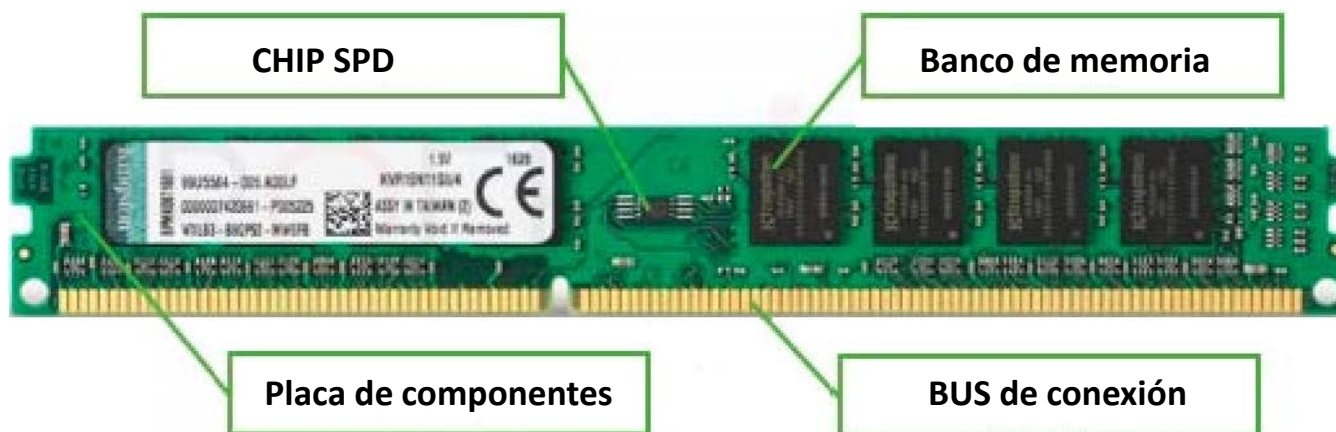
El procesador requiere un espacio para el almacenamiento de los datos, estos lugares son la memoria RAM y el disco duro.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

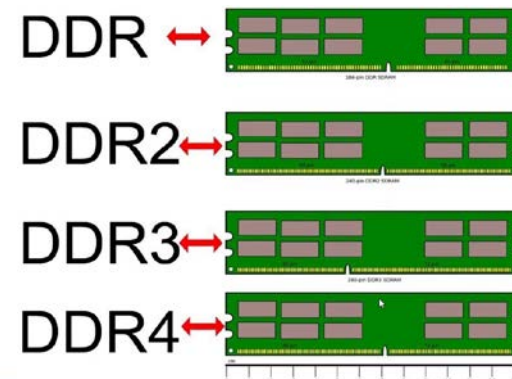
MANEJO DE RECURSOS DEL COMPUTADOR.

Memoria RAM (Random Access Memory = memoria de acceso aleatorio):



NOTA:

CHIP SPD (Serial Presence Detect) Proceso estandarizado de acceso automático a información de un módulo en la memoria RAM. Se encarga de almacenar los datos relativos al módulo de la memoria RAM. Estos datos son el tamaño de la memoria, el tiempo de acceso, velocidad y el tipo de memoria.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Disco duro del computador:

Es el componente (hardware) donde se almacena todo el contenido digital, como el sistema operativo, programas, aplicaciones, documentos, imágenes, música, vídeos, etc.

Tipos (más utilizados):

- Disco duro mecánico (HDD = Hard Drive Disk).
- Disco duro sólido (SSD = Solid State Drive).

HDD
(Hard Drive Disk)



SSD
(Solid State Drive)



Toda la información se almacena en forma de BIT (unidad mínima de información)..

SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

MANEJO DE RECURSOS DEL COMPUTADOR.

Placas del computador:

Para el trabajo integrado, los computadores utilizan la placa de red, la cual está relacionada con la placa madre que es el circuito que permite vincular todas las piezas, partes y componente.

Placa de red:

Tarjeta de red, adaptador de red, adaptador LAN, interfaz de red física, network interface card o network interface controller (NIC) (tarjeta de interfaz de red), su función es la conexión a la red informática y a internet.



Placa madre:

Placa base, tarjeta madre, placa principal, motherboard o mainboard, es una tarjeta de circuito impreso en la que se conectan y comunican los componentes del computador (columna vertebral).



CAMBIO DE EJE TEMÁTICO



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

Generalidades de la ciberseguridad.



¿Qué es la ciberseguridad?

La ciberseguridad (*) o seguridad digital, es la práctica de proteger su información digital, dispositivos y activos. Esto incluye información personal, cuentas, archivos, fotos y dinero.

¿Cuál es el objetivo principal de la ciberseguridad?

Proteger a los usuarios de ataques y amenazas.



Tipos de ataques:

- Ataques activos (afectan a los sistemas).
- Ataques pasivos (buscan obtener información).



(*) Ciberseguridad:

Disciplina creada el año 1.988 por la Association for Computing Machinery (ACM), sociedad científica y educativa en el campo de la computación.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

Claves para una navegación segura por internet:



- Utilice el sentido común.
- Utilice programas con licencia y antivirus.
- Utilice contraseñas difíciles de descifrar.
- Evite utilizar siempre la misma contraseña.
- No abra enlaces que lleguen a su correo electrónico.
- No descargue archivos de dudosa procedencia.
- No utilice redes públicas.
- No entregue sus claves de sesión a nadie.
- Nunca guarde sus claves en los navegadores.
- No guarde fotos de su cedula de identidad ni de sus tarjetas en su teléfono móvil.
- Recuerde que sus claves son solo suyas, no comparta mediante chats ni almacene en "Notas" de su teléfono móvil.



Opera



Google Chrome



Safari



Mozilla Firefox



Internet Explorer



Microsoft Edge

SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

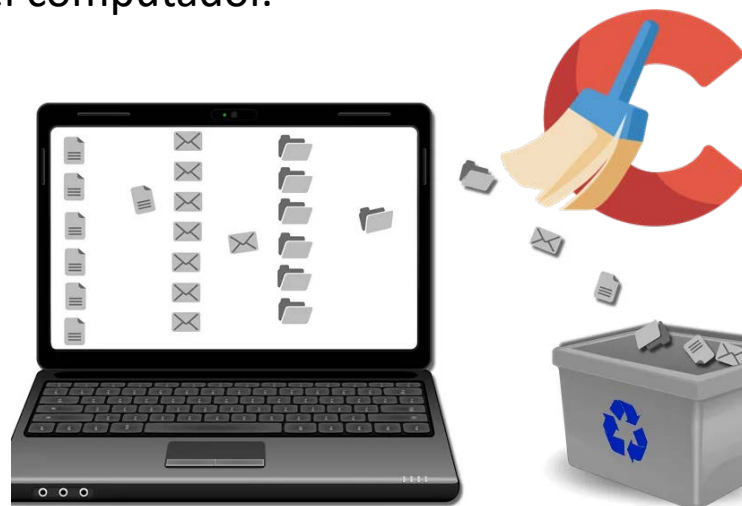
Claves para una navegación segura por internet:

Limpie adecuadamente su computador:

Ccleaner es una aplicación gratuita para sistemas Windows, que sirve para realizar una limpieza y puesta a punto del Sistema Operativo del computador.

Consideraciones:

- Limpieza a fondo del computador de una forma sencilla de archivos basura y configuraciones obsoletas.
- Más espacio efectivo en el disco duro.
- Evita que el computador se ralentice.
- Optimiza el funcionamiento del computador.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

Malware:

Malware o “malicious software” (software malicioso) es un software diseñado y creado para causar daño a un dispositivo o a su usuario.

Consideraciones:

- En general causan los daños una vez que entran en su sistema.
- Este daño se puede manifestar de muchas formas, a menudo implica robo de datos del computador del usuario, encriptar los datos o simplemente eliminar.
- Pueden ser en la práctica una molestia hasta ser destructivos.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

Tipos de Malware.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

Tipos de Malware.

Ransomware:

Es la forma de malware más hostil y directa. Los otros tipos de malware operan invisibles, Ransomware anuncia su presencia de inmediato y exige un pago a cambio de devolver el acceso a sus dispositivos o archivos.

Consideraciones:

- Más difícil de observar y trabaja con discreción en segundo plano (en la mayoría de los casos).
- Opera por simple malevolencia y borra datos importantes en equipos afectados.
- No busca ni cometer fraude ni robar nada, y la única recompensa del hacker es la frustración y los contratiempos que sufren las víctimas.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

Tipos de Malware.

Spyware:

Diseñados para recopilar datos del computador y usuario.

Consideraciones:

- Se infiltra en el equipo del usuario, monitoreando sus actividades.
- Se instala en el computador del usuario directamente o mediante explotación de agujeros de seguridad (fallo de un programa informático) permitiendo el robo de información.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

Tipos de Malware.

Adware:

El trabajo del Adware es crear ingresos para el desarrollador sometiendo a la víctima a publicidad no deseada.

Consideraciones:

- Algunos tipos comunes de adware, son los juegos gratuitos y las barras de herramientas para el navegador.
- Recopilan datos personales de la víctima y después los emplean para personalizar los anuncios que muestran.
- Aunque la mayoría se instalan de forma legal, igualmente es molesto para el usuario.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

Tipos de Malware.

Gusanos:

Los gusanos están diseñados con un objetivo de proliferar y dañar los equipos.

Consideraciones:

- Un gusano infecta un equipo y después se replica y se extiende a otros adicionales, permaneciendo activo en todas las máquinas.
- Algunos gusanos actúan como mensajeros para instalar malwares adicionales.
- Otros, solo se extienden y no causan daño intencionadamente a las máquinas anfitrionas, aunque siguen atestando las redes con sus demandas de ancho de banda.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

Tipos de Malware.

Troyanos:

Los antiguos poetas griegos hablaban de los guerreros atenienses que se escondieron en un gigantesco caballo de madera para luego salir del interior, una vez que los troyanos lo arrastraron tras las murallas de la ciudad.

Consideraciones:

- Un caballo de Troya es un vehículo que oculta a los atacantes.
- El malware troyano se infiltra en el dispositivo de una víctima presentándose como software legítimo.
- Una vez instalado, el troyano se activa y, en ocasiones, llega incluso a descargar malwares adicionales.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

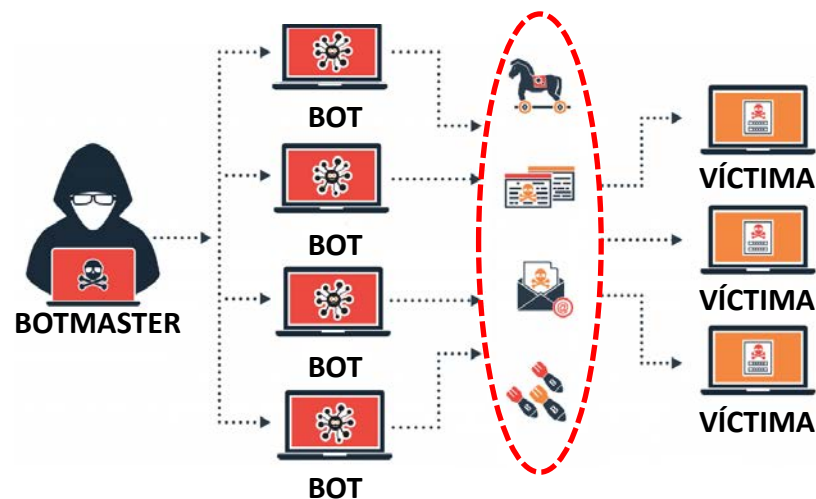
Tipos de Malware.

Redes de robots.

Una red de robots no es un tipo de malware, sino una red de equipos o de código informático que puede desarrollar o ejecutar malware.

Consideraciones:

- Los atacantes infectan un grupo de equipos con software malicioso conocido como “robots” (o “bots”), capaz de recibir órdenes desde su controlador.
- Posteriormente, los equipos forman una red que proporciona al controlador acceso a una capacidad de procesamiento sustancial.
- La capacidad se puede emplear para coordinar ataques, enviar spam, robar datos y crear anuncios falsos en su navegador.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

¿Cómo eliminar un malware?

La mejor manera de eliminar malware, es con los softwares antivirus. Estas herramientas escanean su sistema, detectan el malware y lo eliminan. Todo automático. Además de esto, previenen la futura instalación de malwares en su dispositivo.

Consideraciones:

- Algunas herramientas antimalware gratuitas pueden ser útiles, pero esta no es una solución definitiva.
- Los antimalware gratuitos, se concentran en eliminar el malware que ya está instalado en su dispositivo, en lugar de prevenir que un nuevo malware se instale.
- Los antimalware gratuitos, más que prevenir la infección, en ocasiones la podrían aumentar.

Sugerencia para equipos con licencia



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

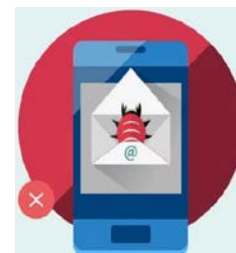
CIBERSEGURIDAD BÁSICA.

Métodos para robar su identidad en internet:

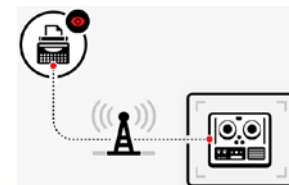
Spam: Mensaje de correo electrónico enviado a varios destinatarios, debe cumplir varios aspectos: ser enviado de forma masiva, ser un mensaje no solicitado por el usuario y tener contenido engañoso (habitualmente de tipo publicitario).



Spim: Es un caso específico de spam a través del cual se envían mensajes instantáneos a celular cuyo contenido puede incluir spyware, registradores de pulsaciones, vínculos a sitios (phishing), invitaciones para suscripciones a servicios o promociones falsas; el objetivo es tomar el control de la lista de contactos para suplantar la identidad del afectado.



Keylogger (registradores de pulsaciones): Es una forma de software espía que guarda los caracteres que fueron pulsados cuando un usuario navega en la web, visita sitios de comercio electrónico o en la banca electrónica.

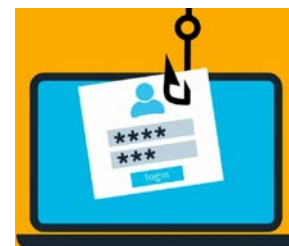


SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

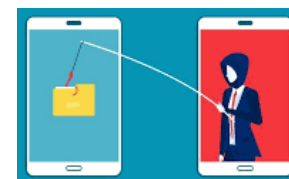
CIBERSEGURIDAD BÁSICA.

Métodos para robar su identidad en internet:

Phishing (suplantación de identidad): El término proviene de fishing (pesca). Los atacantes, conocidos como phishers, simulan ser empresas legítimas y tienen la finalidad de obtener información confidencial a través del empleo de spam, sitios web falsos, mensajes de correo electrónico y mensajes instantáneos.



Smishing (fraude por mensaje de texto): El atacante usa un atractivo mensaje de SMS a un teléfono móvil para convencer al destinatario que haga clic en un enlace para descargar programas malintencionados.



Pharming: Consiste en redirigir a un usuario que navega en una página web a una página diseñada para robar información. A diferencia del phishing, el Pharming es programado para atacar al equipo de la víctima y redireccionar la navegación a servidores plagados con aspecto similar.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

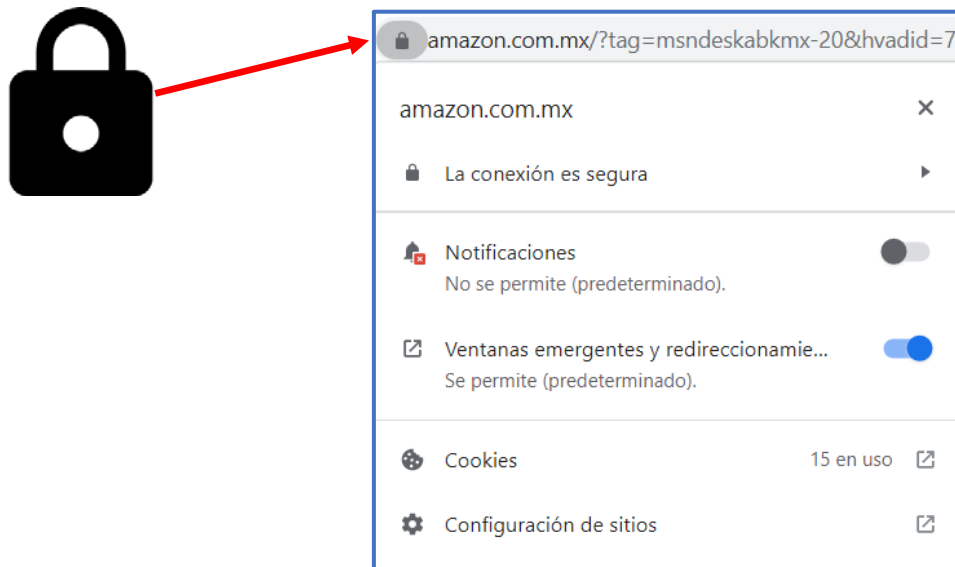
CIBERSEGURIDAD BÁSICA.

¿Cómo puedo saber si una página web es segura?

Google Chrome lo alertará si no puede visitar el sitio de forma segura o privada.

Cuando abra una página, para comprobar la seguridad de un sitio, a la izquierda de la dirección web, busque el candado de seguridad “seguro”.

Para ver los permisos y los datos del sitio, seleccione el ícono.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

Seguridad en las compras por internet:

En el año 2021, el valor de las ventas alcanzó los 492 mil millones de dólares. Se estima que para el año 2025 el comercio electrónico alcance ventas por más de 1.2 mil millones de dólares con un crecimiento anual del 26% promedio.

Consideraciones:

- Busque de forma segura, escriba la URL en la barra de direcciones.



- Cierre “siempre” las sesiones al salir de una página web.



- No utilice redes públicas o poco seguras.



- No comparta con nadie las claves de sus tarjetas (débito / crédito).



- Diseñe un solo computador para compras y actividades bancarias en línea.



- Use una dirección de correo electrónico dedicada (si es posible).



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

CIBERSEGURIDAD BÁSICA.

Consideraciones básicas para la protección de equipos y dispositivos:

- No abra correos electrónicos o archivos adjuntos de personas desconocidas.
- Proteja todos sus dispositivos con PIN o contraseña.
- Utilice contraseñas fuertes e indescifrables.
- Utilice contraseñas seguras y diferentes para cada cuenta.
- Actualice el sistema operativo y softwares cada vez que sea factible.
- Encripte y firme sus correos electrónicos digitalmente.
- Utilice la autenticación de dos pasos (2FA = Two factor authentication).
- Piense dos veces antes de clicar un link.
- Realice regularmente copias de seguridad en dispositivos o en la nube.
- Evite conexiones en redes públicas.
- Presta atención a sus publicaciones en sus redes sociales.



LAS CONTRASEÑAS, SON COMO SU ROPA INTERIOR.
NO LA DEBE COMPARTIR CON NADIE 😊



CAMBIO DE EJE TEMÁTICO

CIBERSEGURIDAD BÁSICA

ALGUNOS TIPS INFORMÁTICOS



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

ALGUNOS TIPS INFORMÁTICOS.



- Piense qué realmente necesita del programa, por ejemplo, el dato que necesita extraer.



- Cree su propio esquema de trabajo. Trabajar de esta forma, permite agilizar los procesos de desarrollo, asegurando buenas prácticas y la gestión del conocimiento.



- Comparta con su familia, amigos y compañeros de trabajo los datos útiles; la gestión del conocimiento es la clave para mejorar las competencias informáticas.

Tips

SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

ALGUNOS TIPS INFORMÁTICOS.

PIRÁMIDE DE NECESIDADES DIGITALES:




SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

ALGUNOS TIPS INFORMÁTICOS.



TIPS BÁSICOS:


Para:	Tips
<p>Prolongar la vida útil del notebook</p> 	No trabaje con el equipo sobre la cama.
	Evite golpes del computador especialmente si está encendido.
	No mueva el equipo si tiene instalado un disco mecánico (HDD).
	Realice un mantenimiento anual del notebook con personas idóneas (limpieza de componentes, ventilador, etc.).
	No coma cerca del computador, evitará derrames de líquidos y sustancias.
	Evite utilizar el notebook con su mascota muy cerca.
	Formatee el computador en casos necesarios (cuando se ralentice).
	Realice una limpieza periódica de archivos basura del computador.

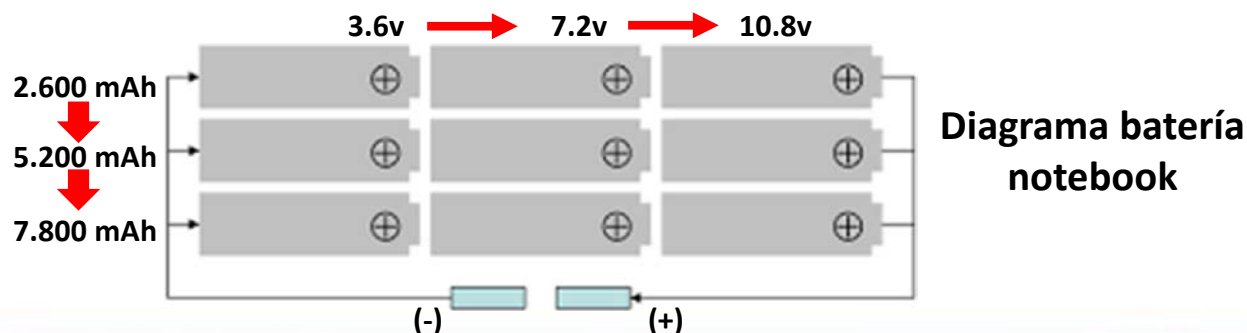
SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

ALGUNOS TIPS INFORMÁTICOS.



TIPS BÁSICOS:

Tip para:	Considerar
<p>Prolongar la vida útil de la batería del notebook</p> 	Si trabaja conectado a la corriente, retire la batería si es factible. En caso de equipos nuevos con batería integrada no es necesario.
	Evite dejar el notebook cerca de las fuentes de calor.
	Los altos voltajes degradan la duración de la batería.
	En caso de oscilaciones de voltaje, trabaje con la batería.
	Active el modo de energía.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR:

ALGUNOS TIPS INFORMÁTICOS.



TIPS BÁSICOS:

La vida útil de la batería de un notebook, se mide en ciclos de carga; cuanto menor sea la descarga (bajo DoD), mayor duración tendrá. Si es factible, evite las descargas completas y cargue con más frecuencia.

Considere: El ciclo de carga entre el 25% - 85%, proporciona una vida útil mayor.

Temperatura	100% de carga
0° C	94% (después de 1 año)
25° C	80% (después de 1 año)
40° C	65% (después de 1 año)
60° C	60% (después de 3 meses)



Profundidad de descarga	Ciclos de descarga
100% DoD	300 - 500
50% DoD	1.200 – 1.500
25% DoD	2.000 – 2.500
10% DoD	3.750 – 4.700

DOD (Depth of Discharge = profundidad de descarga):

Es la cantidad o grado de agotamiento de una batería. Esto significa que si la batería se agota por completo, la profundidad de descarga es del 100%.



SEGURIDAD INFORMÁTICA Y MANEJO DE RECURSOS DEL COMPUTADOR

ENERO DE 2023