

Introducción a la ciberseguridad

Cisco Tema 1

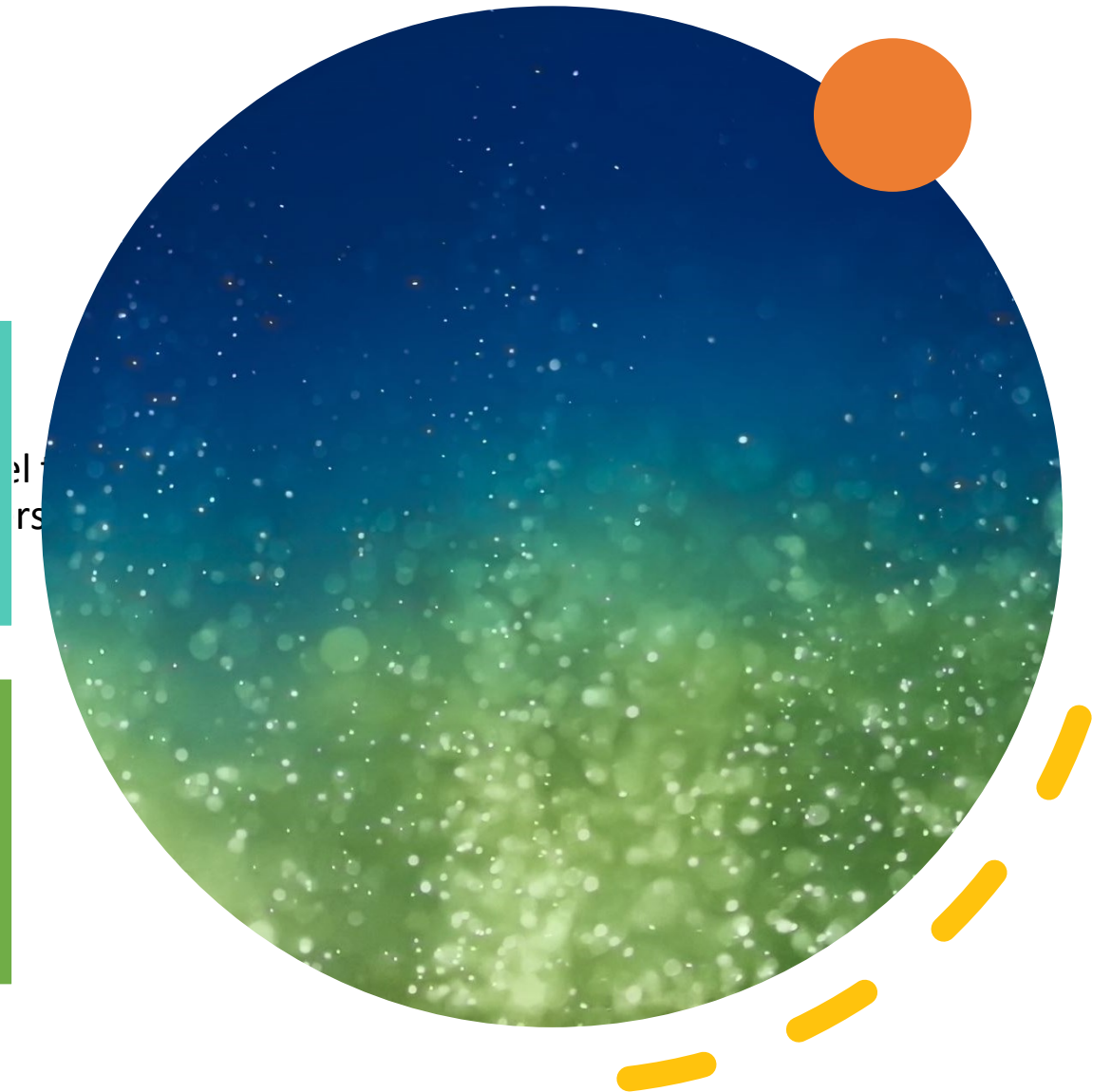
Descripción general del tema 1

Aprenderá los aspectos básicos de estar seguro en línea.

Aprenderá sobre los diferentes tipos de malware y ataques, y cómo las organizaciones se protegen contra ellos.

Explorará las opciones profesionales en ciberseguridad.

Al finalizar este curso, usted sabrá más acerca de la importancia de estar seguro en línea, de las consecuencias potenciales de los ciberataques y de las posibles opciones profesionales en ciberseguridad.



Tema 1: La necesidad de la ciberseguridad

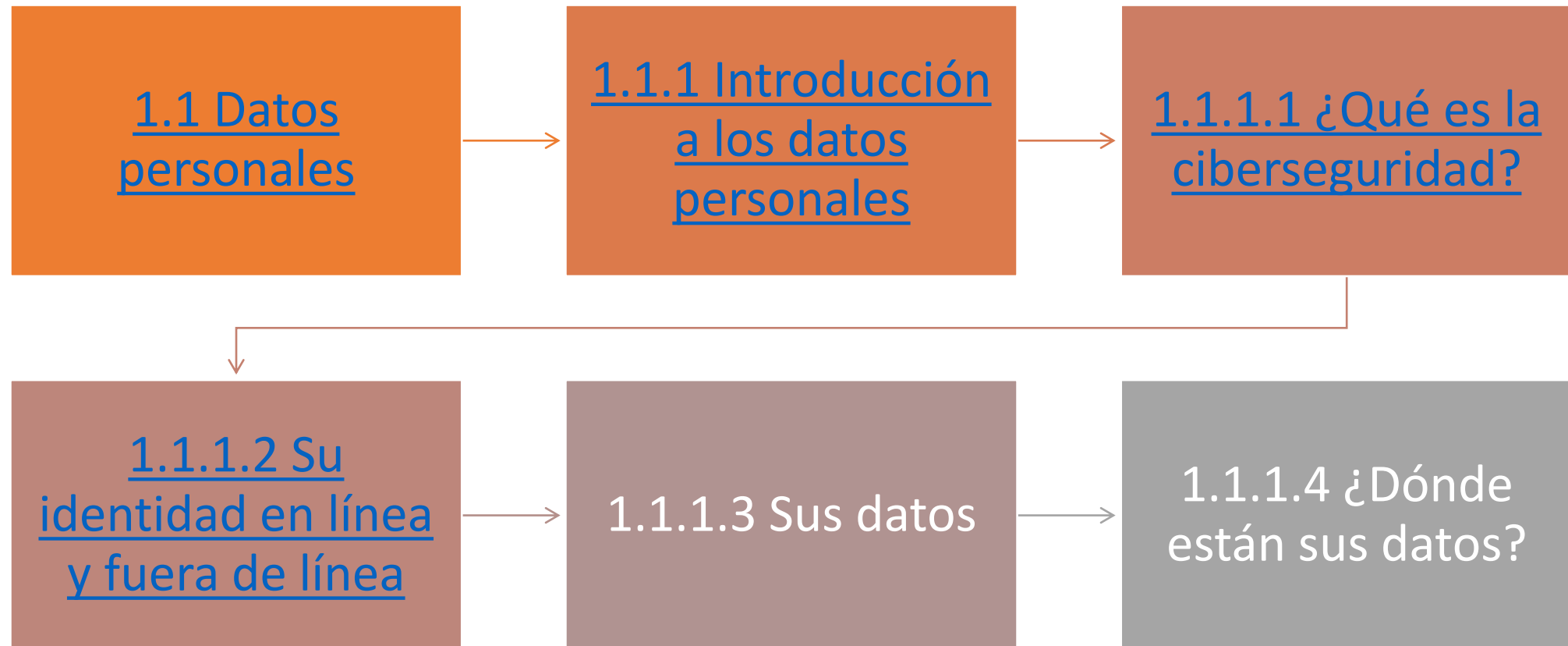
Qué es la ciberseguridad y por qué la demanda de profesionales de ciberseguridad está creciendo. Qué es su identidad y sus datos en línea, dónde se encuentra y por qué es de interés para los delincuentes cibernéticos.

Qué son los datos de una organización y por qué deben protegerse. Quiénes son los atacantes cibernéticos y lo que quieren. Los profesionales de la ciberseguridad deben tener las mismas habilidades que los atacantes cibernéticos, pero los profesionales de la ciberseguridad deben trabajar de acuerdo con la ley local, nacional e internacional. Los profesionales de ciberseguridad también deben usar sus habilidades con ética.

L

a guerra cibernética y por qué las naciones y los gobiernos necesitan profesionales de la ciberseguridad para proteger a sus ciudadanos y su infraestructura.

Tema 1 La necesidad de la ciberseguridad



¿Qué es la ciberseguridad?

- La red de información electrónica conectada se ha convertido en una parte integral de nuestra vida cotidiana. Todos los tipos de organizaciones, como instituciones médicas, financieras y educativas, utilizan esta red para funcionar de manera eficaz. Utilizan la red para recopilar, procesar, almacenar y compartir grandes cantidades de información digital. A medida que se recopila y se comparte más información digital, la protección de esta información se vuelve incluso más importante para nuestra seguridad nacional y estabilidad económica.



¿Qué es la ciberseguridad?

- La ciberseguridad es el esfuerzo constante por proteger estos sistemas de red y todos los datos contra el uso no autorizado o los daños. A nivel personal, debe proteger su identidad, sus datos y sus dispositivos informáticos. A nivel corporativo, es responsabilidad de todos proteger la reputación, los datos y los clientes de la organización. A nivel del estado, la seguridad nacional, y la seguridad y el bienestar de los ciudadanos están en juego.



Su identidad en línea y fuera de línea

A medida que pasa más tiempo en línea, su identidad, en línea y fuera de línea, puede afectar su vida. Su identidad fuera de línea es la persona con la que sus amigos y familiares interactúan a diario en el hogar, la escuela o el trabajo. Conocen su información personal, como su nombre, edad, o dónde vive. Su identidad en línea es quién es usted en el ciberespacio. Su identidad en línea es cómo se presenta ante otros en línea. Esta identidad en línea solo debería revelar una cantidad limitada de información sobre usted.

- Debe tener cuidado al elegir un nombre de usuario o alias para su identidad en línea. El nombre de usuario no debe contener información personal. Debe ser algo correcto y respetuoso. Este nombre de usuario no debe llevar a extraños a pensar que es un objetivo fácil para los delitos cibernéticos o la atención no deseada.



Sus datos

- Cualquier información sobre usted puede ser considerada como sus datos.
- Esta información personal puede identificarlo de manera única como persona.
- Estos datos incluyen las imágenes y los mensajes que intercambia con su familia y amigos en línea.
- Otra información, como su nombre, número de seguro social, la fecha y el lugar de nacimiento, o su apellido materno, es de su conocimiento y se utiliza para identificarlo.
- La información como la información médica, educativa, financiera y laboral, también se puede utilizar para identificarlo en línea.
- **Expediente médico**
 - Cada vez que asiste al consultorio del médico, más información se agrega a su historial médico.
 - La prescripción de su médico de cabecera se vuelve parte de su historial médico.
 - Su historial médico incluye su estado físico y mental, y otra información personal que puede no estar relacionada médicamente. Por ejemplo, si asistió a terapias durante la niñez cuando se produjeron cambios importantes en la familia, esto figurará en algún lugar de sus historias clínicas.
 - Su historia médica y su información personal, su historial médico también puede incluir información sobre su familia.
 - Los dispositivos médicos, como las pulseras deportivas, utilizan la plataforma de la nube para permitir la transferencia, el almacenamiento y la visualización inalámbrica de los datos clínicos, como el ritmo cardíaco, la presión arterial y el azúcar en la sangre. Estos dispositivos pueden generar una enorme cantidad de datos clínicos que pueden volverse parte de su historial clínico.

Sus datos

- **Historial educativo**
- A medida que avanza en su educación, la información sobre sus notas y puntajes en las evaluaciones, su asistencia, los cursos realizados, los reconocimientos y títulos adquiridos, así como cualquier informe disciplinario puede estar en su historial educativo.
- Este historial también puede incluir información de contacto, salud y su historial de inmunización, así como un historial de educación especial, incluidos los programas educativos individualizados.

Sus datos

- **Historial financiero y de empleo**
- Su historial financiero puede incluir información sobre sus ingresos y gastos.
- El historial de impuestos pueden incluir talones de cheques de pago, resúmenes de la tarjeta de crédito, su calificación crediticia y otra información bancaria.
- Su información de empleo puede incluir su empleo anterior y su rendimiento.



Sus datos



¿Dónde están
sus datos?



¿Dónde están sus datos?

Toda esta información es
sobre usted.

Existen distintas leyes que
protegen la privacidad y los
datos en su país.

Pero, ¿sabe dónde están sus
datos?

Cuando está en el
consultorio médico, la
conversación que tiene con
el médico se registra en su
expediente médico.

Para fines de facturación,
esta información se puede
compartir con la empresa
de seguros para garantizar la
facturación y la calidad
adecuadas.

Ahora, una parte de su
historial médico de la visita
también se encuentra en la
empresa de seguros.

¿Dónde están sus datos?

Las tarjetas de fidelidad de la tienda pueden ser una manera conveniente de ahorrar dinero en sus compras.

La tienda compila un perfil de sus compras y utiliza esa información para su propio uso.

El perfil muestra que un comprador compra cierta marca y sabor de crema dental regularmente.

La tienda utiliza esta información para identificar como objetivo al comprador con ofertas especiales del partner de marketing.

Con la tarjeta de fidelidad, la tienda y el partner de marketing tienen un perfil del comportamiento de compra de un cliente.

¿Dónde están sus datos?

Cuando comparte sus imágenes en línea con sus amigos, ¿sabe quién puede tener una copia de las imágenes?

Las copias de las imágenes están en sus propios dispositivos.

Sus amigos pueden tener copias de dichas imágenes descargadas en sus dispositivos.

Si las imágenes se comparten públicamente, es posible que desconocidos tengan copias de ellas también.

Podrían descargar dichas imágenes o realizar capturas de pantalla de dichas imágenes.

Debido a que las imágenes se publicaron en línea, también se guardan en servidores ubicados en distintas partes del mundo.

Ahora las imágenes ya no se encuentran solo en sus dispositivos informáticos.

Sus dispositivos informáticos

- Sus dispositivos informáticos no solo almacenan sus datos.
- Ahora estos dispositivos se han convertido en el portal a sus datos y generan información sobre usted.



Sus dispositivos informáticos

- A menos que haya seleccionado recibir los resúmenes en papel para todas sus cuentas, usted utiliza sus dispositivos informáticos para acceder a los datos.
- Si desea una copia digital del último resumen de la tarjeta de crédito, utiliza sus dispositivos informáticos para acceder a la página web del emisor de la tarjeta de crédito.
- Si desea pagar su factura de la tarjeta de crédito en línea, accede a la página web de su banco para transferir los fondos con sus dispositivos informáticos.



Sus dispositivos informáticos

- Además de permitirle acceder a su información, los dispositivos informáticos también pueden generar información sobre usted.
- Con toda esta información sobre usted disponible en línea, sus datos personales se han vuelto rentables para los hackers.



A person wearing a black leather glove is reaching out towards a laptop on a desk. The person is also wearing blue jeans. The background is a plain, light-colored wall.

Quieren su dinero

Si tiene algo de valor, los
delincuentes lo quieren.

Quieren su dinero

- Sus credenciales en línea son valiosas.
- Estas credenciales otorgan a los ladrones acceso a sus cuentas.
- Puede pensar que los kilómetros de viajero frecuente adquiridos no tienen valor para los delincuentes cibernéticos, pero deberá reconsiderar esta afirmación.
- Luego de que se hackearan aproximadamente 10 000 cuentas de American Airlines y United, los delincuentes cibernéticos reservaban vuelos gratuitos y mejoras con estas credenciales robadas.
- Aunque los kilómetros de viajero frecuente fueron devueltos a los clientes por las aerolíneas, esto demuestra el valor de las credenciales de inicio de sesión.
- Un delincuente también podría aprovechar sus relaciones.
- Pueden acceder a sus cuentas en línea y su reputación para engañarlo para que transfiera dinero a sus amigos o familiares.



Quieren su dinero

- El delincuente puede enviar mensajes que indiquen que su familia o amigos necesitan que usted les transfiera dinero para que puedan regresar del extranjero después de perder sus billeteras.
- Los delincuentes son muy imaginativos cuando intentan engañarlo para que se les otorgue dinero. No solo roban su dinero; también pueden robar su identidad y arruinarle la vida.



The background of the image is a dark green surface with a complex pattern of gold-colored circuit lines and circular nodes, resembling a printed circuit board. In the center, there is a large, light blue puzzle piece. This piece has a keyhole-shaped cutout at its top edge. The text is overlaid on this puzzle piece.

Quieren su identidad

Además de robar su dinero para obtener una ganancia monetaria a corto plazo, los delincuentes desean obtener ganancias a largo plazo robando su identidad.

Quieren su identidad

- A medida que aumentan los costos médicos, el robo de la identidad médica también aumenta.
- Los ladrones de identidad pueden robar su seguro médico y usar sus beneficios de salud para ellos mismos, y estos procedimientos médicos ahora están en sus registros médicos.
- Los procedimientos anuales de declaración de impuestos pueden variar de un país a otro; sin embargo, los delincuentes cibernéticos consideran esto como una oportunidad.
- Por ejemplo, la población española necesita presentar sus impuestos antes del 30 de Junio de cada año.



Quieren su identidad

- Hacienda empieza a devolver aquellas declaraciones que salieron negativas desde abril hasta julio.
- Un ladrón de identidad podría generar una declaración de impuestos falsa y recolectar la devolución.
- Los usuarios legítimos notarán cuando intenten hacer la declaración que alguien ya la ha hecho previamente.
- Con la identidad robada, también pueden abrir cuentas de tarjeta de crédito y acumular deudas en su nombre.
- Esto provocará daños en su calificación crediticia y hará que sea más difícil para usted obtener préstamos.
- Las credenciales personales también pueden permitir el acceso a datos corporativos y de gobierno.






Tipos de datos de la organización

Tipos de datos de la organización: Internet de las cosas y datos masivos

- Con el surgimiento de la Internet de las cosas (IoT), hay muchos más datos para administrar y asegurar.
- La IoT es una gran red de objetos físicos, como sensores y equipos, que se extiende más allá de la red de computadoras tradicional. Todas estas conexiones,
- Además del hecho de que hemos ampliado la capacidad y los servicios de almacenamiento a través de la nube y la virtualización, llevan al crecimiento exponencial de los datos.
- Estos datos han creado una nueva área de interés en la tecnología y los negocios denominada “datos masivos”.
- Con la velocidad, el volumen y la variedad de datos generados por la IoT y las operaciones diarias de la empresa, la confidencialidad, integridad y disponibilidad de estos datos son vitales para la supervivencia de la organización

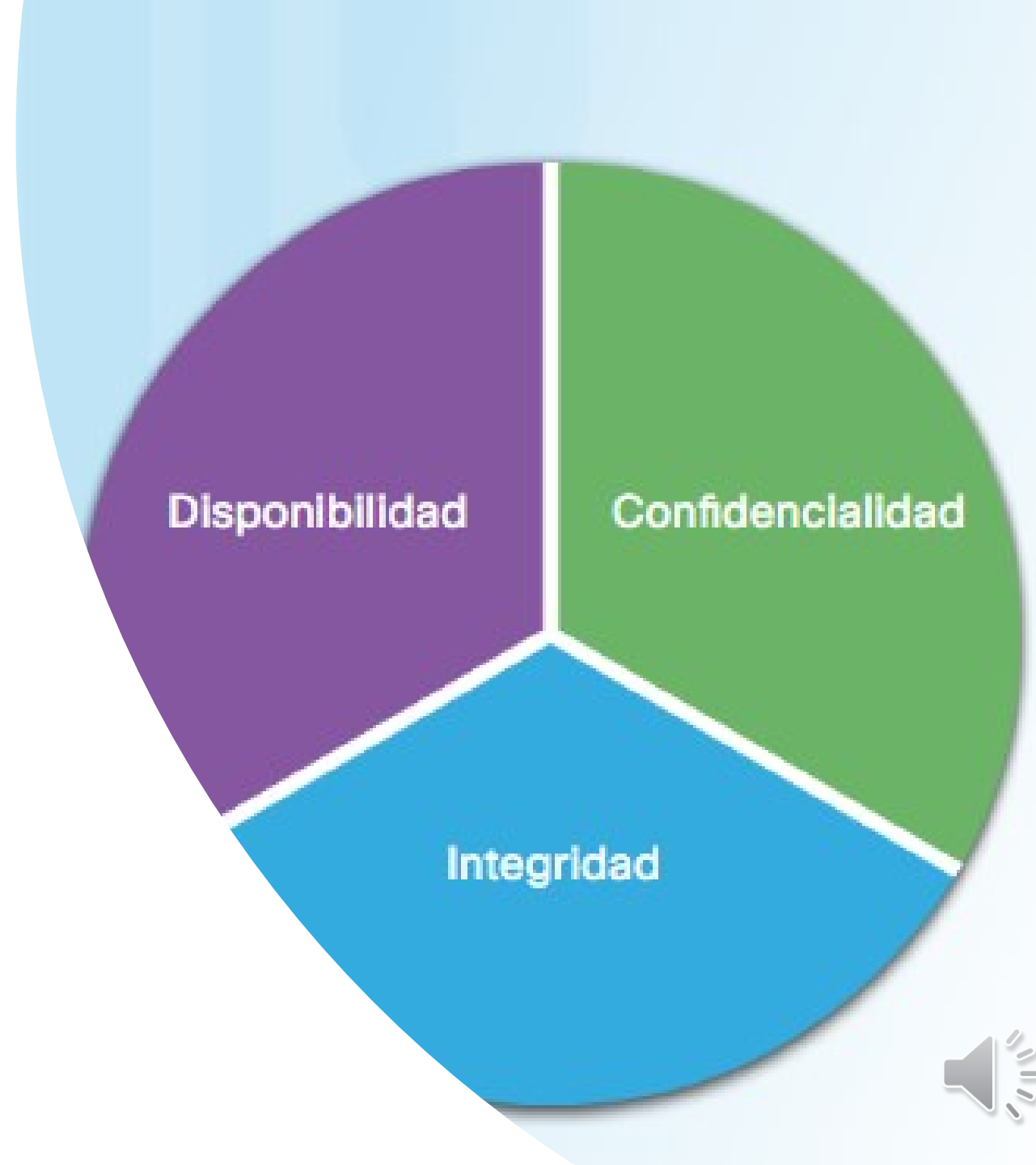




Tipos de datos de la organización: Datos tradicionales

- Los datos corporativos incluyen información del personal, propiedades intelectuales y datos financieros. La información del personal incluye el material de las postulaciones, la nómina, la carta de oferta, los acuerdos del empleado, y cualquier información utilizada para tomar decisiones de empleo.
- La propiedad intelectual, como patentes, marcas registradas y planes de nuevos productos, permite a una empresa obtener una ventaja económica sobre sus competidores.
- Esta propiedad intelectual se puede considerar un secreto comercial; perder esta información puede ser desastroso para el futuro de la empresa.
- Los datos financieros, como las declaraciones de ingresos, los balances y las declaraciones de flujo de caja de una empresa brindan información sobre el estado de la empresa.

CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD

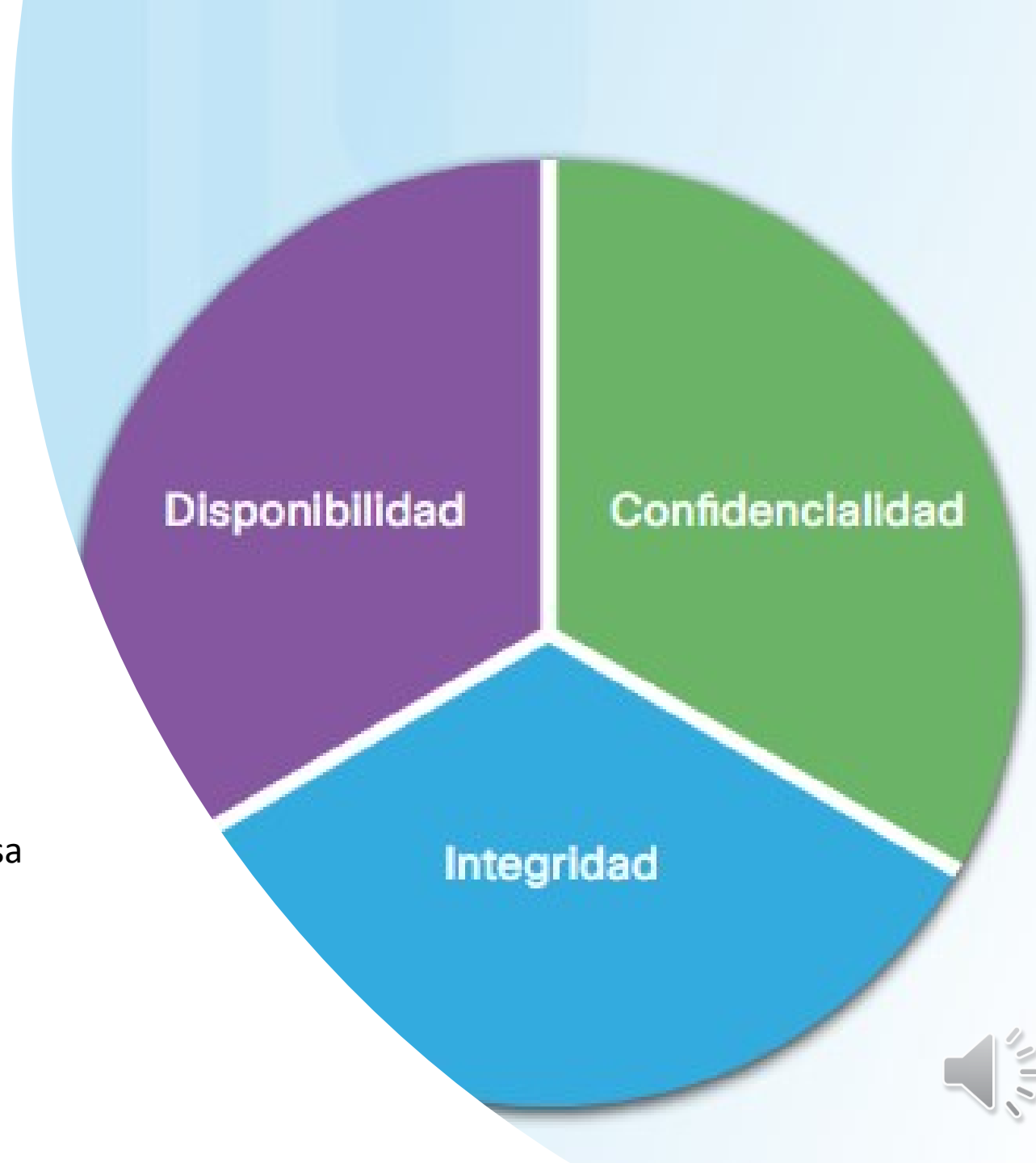


CONFIDENCIALIDAD

INTEGRIDAD

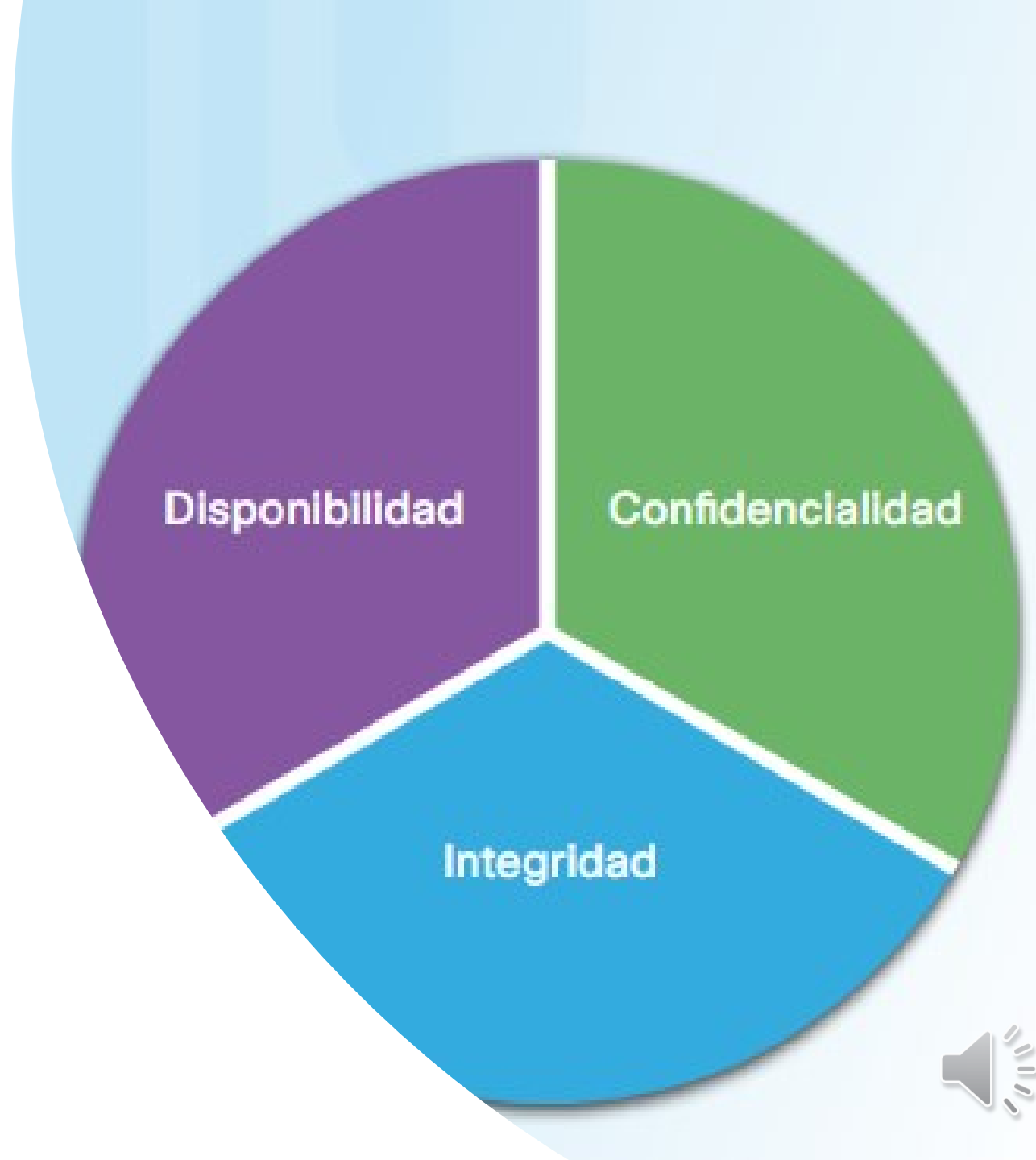
DISPONIBILIDAD

- La confidencialidad, integridad y disponibilidad, conocidas como la tríada CID, es una guía para la seguridad informática de una organización.
- La confidencialidad garantiza la privacidad de los datos mediante la restricción del acceso con el cifrado de la autenticación.
- La integridad garantiza que la información sea precisa y confiable.
- La disponibilidad garantiza que la información esté disponible a las personas autorizadas.



CONFIDENCIALIDAD

- Otro término para la confidencialidad sería privacidad.
- Las políticas de la empresa deben restringir el acceso a la información al personal autorizado y garantizar que solo las personas autorizadas verán estos datos.
 - Los datos se pueden dividir en secciones según el nivel de seguridad o sensibilidad de la información.
- Por ejemplo, un desarrollador Java no debe tener acceso a la información personal de todos los empleados.
- Además, los empleados deben recibir capacitación para comprender las mejores prácticas para resguardar datos confidenciales, para protegerse y proteger a la empresa contra ataques.



CONFIDENCIALIDAD

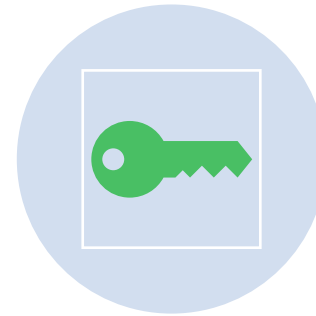
Entre los métodos para garantizar la confidencialidad se incluyen:



CIFRADO DE DATOS,



**NOMBRE DE USUARIO Y
CONTRASEÑA,**



**LA AUTENTICACIÓN DE DOS
FACTORES Y**



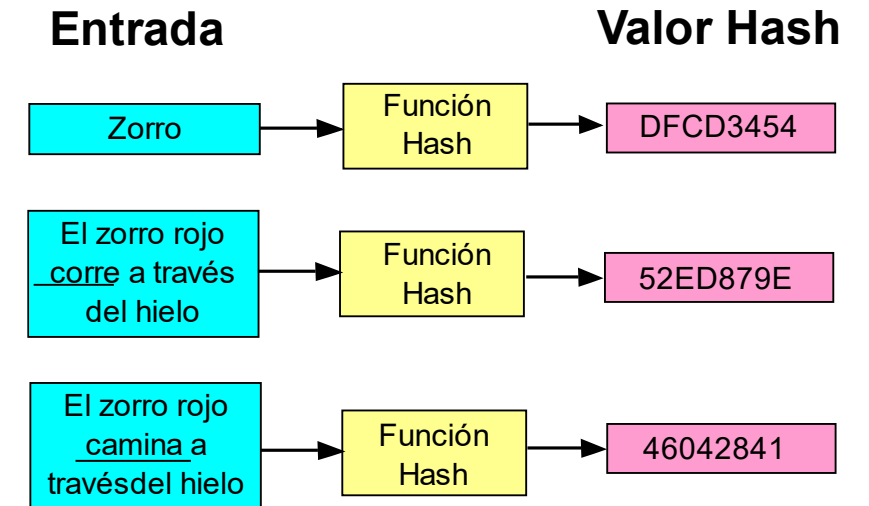
**LA MINIMIZACIÓN DE LA
EXPOSICIÓN DE LA
INFORMACIÓN CONFIDENCIAL.**

Integridad

- La integridad es **precisión, consistencia y confiabilidad de los datos durante su ciclo de vida**. Los datos deben permanecer inalterados durante la transferencia y no deben ser modificados por entidades no autorizadas.
- Los permisos de archivos y el control de acceso de usuarios pueden impedir el acceso no autorizado.
- El control de versión se puede utilizar para evitar **cambios accidentales** por parte de usuarios autorizados.
- Las copias de respaldo deben estar disponibles para restaurar los datos dañados, y **la suma de comprobación** del hash se puede utilizar para verificar la integridad de los datos durante la transferencia.

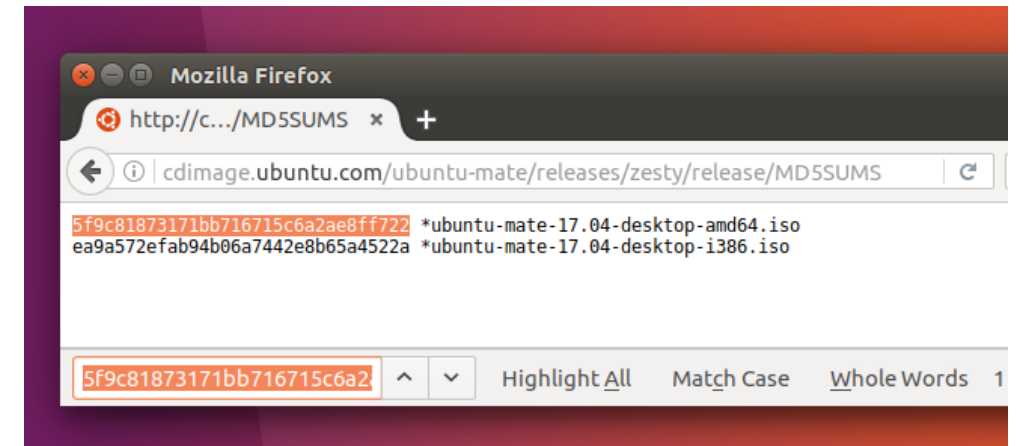
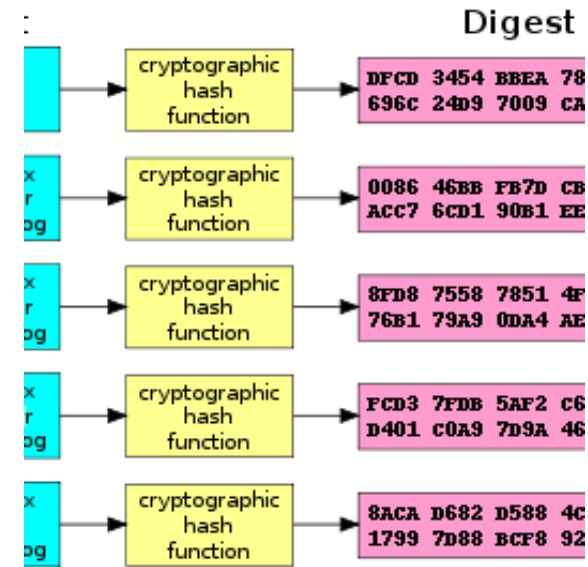
La suma de comprobación HASH o MD5

- La suma de comprobación se utiliza para verificar la integridad de los archivos, o cadenas de caracteres, luego de que se hayan transferido desde un dispositivo a otro a través de su red local o de Internet. Las sumas de comprobación se calculan con funciones de hash. Algunas de las sumas de comprobación comunes son MD5, SHA-1, SHA-256 y SHA-512. Una función de hash utiliza un algoritmo matemático para transformar los datos en un valor de longitud fija que representa los datos, tal como se muestra en la Figura 2. El valor de hash solo está allí para la comparación. Desde el valor de hash, los datos originales no se pueden recuperar directamente. Por ejemplo, si olvidó su contraseña, su contraseña no se puede recuperar desde el valor de hash. La contraseña se debe restablecer.



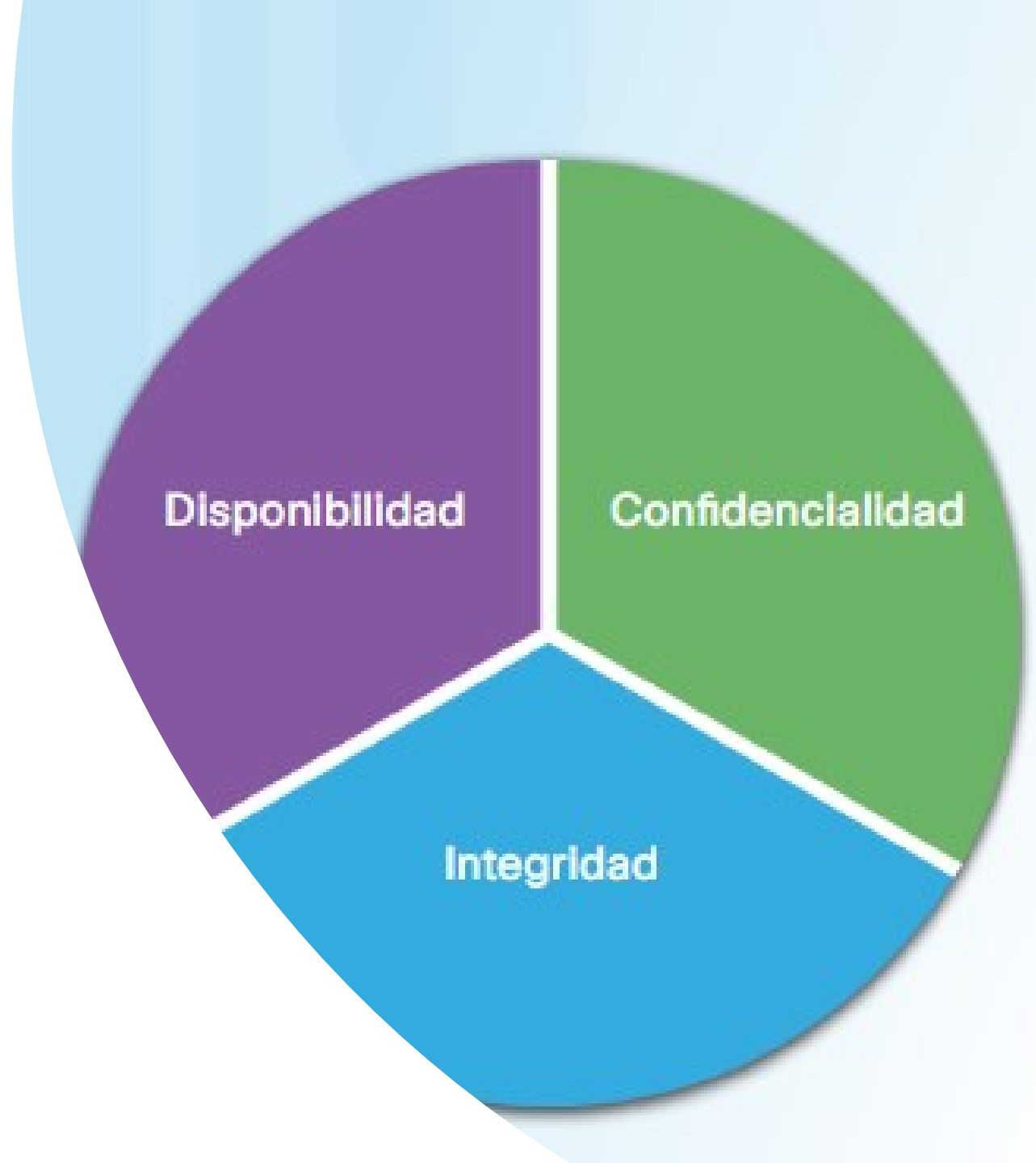
Ejemplo:HASH o MD5

- Luego de descargar un archivo, puede verificar su integridad comparando los valores de hash del origen con el que usted generó con cualquier calculadora de hash. Al comparar los valores de hash, puede asegurarse de que el archivo no se haya alterado ni dañado durante la transferencia.



Disponibilidad

- La confidencialidad, integridad y disponibilidad, conocidas como la tríada CID, es una guía para la seguridad informática de una organización.
- La confidencialidad garantiza la privacidad de los datos mediante la restricción del acceso con el cifrado de la autenticación.
- La integridad garantiza que la información sea precisa y confiable.
- La disponibilidad garantiza que la información esté disponible a las personas autorizadas.



Disponibilidad

- Mantener los equipos, realizar reparaciones de hardware, mantener los sistemas operativos y el software actualizados, así como crear respaldos, garantiza la disponibilidad de la red y los datos a los usuarios autorizados.
- Deben existir planes para recuperarse rápidamente ante desastres naturales o provocados por el hombre.
- Los equipos o software de seguridad, como los firewalls, lo protegen contra el tiempo de inactividad debido a los ataques, como la denegación de servicio (DoS).
- La denegación de servicio se produce cuando un atacante intenta agotar los recursos de manera tal que los servicios no estén disponibles para los usuarios.

Práctica de laboratorio 1

Práctica de laboratorio: Comparar datos con un hash

Objetivos

Use un programa de hash para comprobar la integridad de los datos.

Aspectos básicos/situación

- Es importante saber si los datos fueron dañados o manipulados. Para comprobar si los datos fueron cambiados o si permanecen igual, puede usarse un programa de hash. Un programa de hash realiza una función hash en datos o en un archivo, lo cual devuelve un valor (generalmente, mucho más corto). Hay varias funciones hash distintas, algunas muy simples y otras muy complejas. Cuando se ejecuta el mismo hash en los mismos datos, el valor devuelto es siempre el mismo. Si se implementa algún cambio en los datos, el valor hash devuelto será diferente.
- **Nota:** Necesitará privilegios de instalación y algunos conocimientos sobre el proceso para instalar programas de Windows.

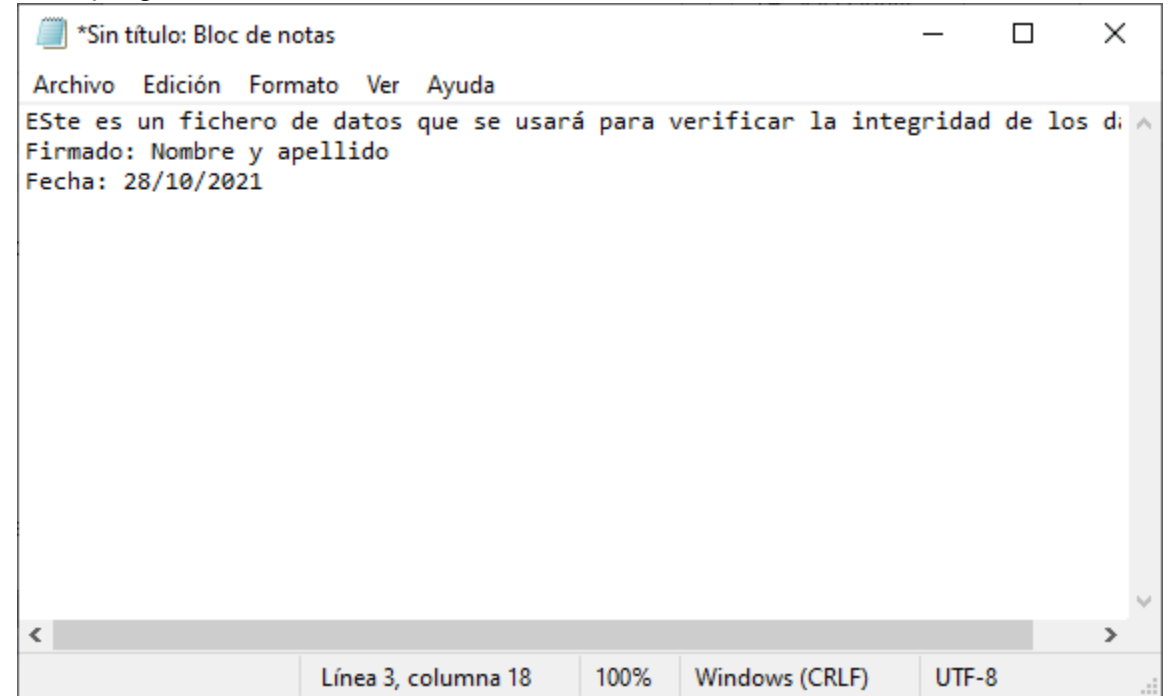
Recursos necesarios

- Computadora con acceso a Internet

Práctica de laboratorio 1

Paso 1: Crear un archivo de texto

- Busque en su equipo el programa Bloc de notas y ábralo.
- Escriba algún texto en el programa.

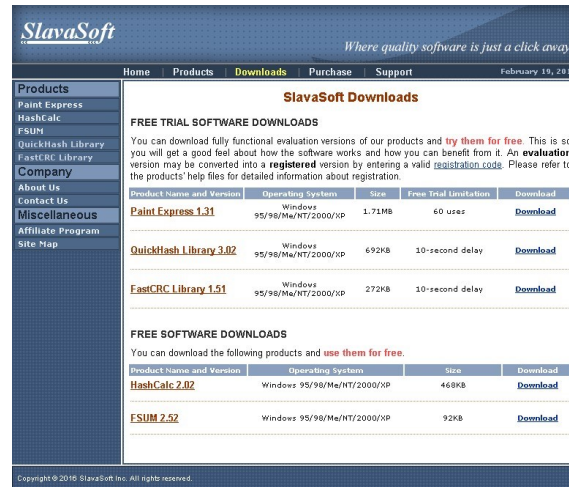


- Elija **Archivo > Guardar**.
- Navegue hasta **Escritorio**.
- Escriba **Hash** en el campo **Nombre de archivo:** nombreusuariodominio.txt (Pedroasir234) y haga clic en **Guardar**.

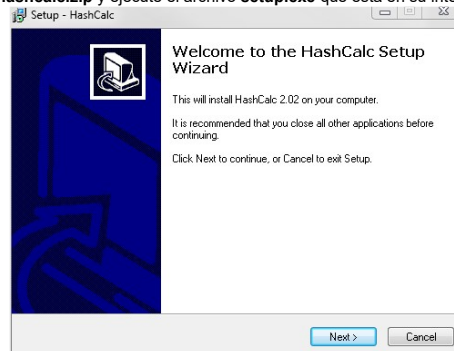
Práctica de laboratorio 1

Paso 2: Instalar HashCalc 1

- a. Abra un navegador web y vaya a <http://www.slavasoft.com/download.htm>.

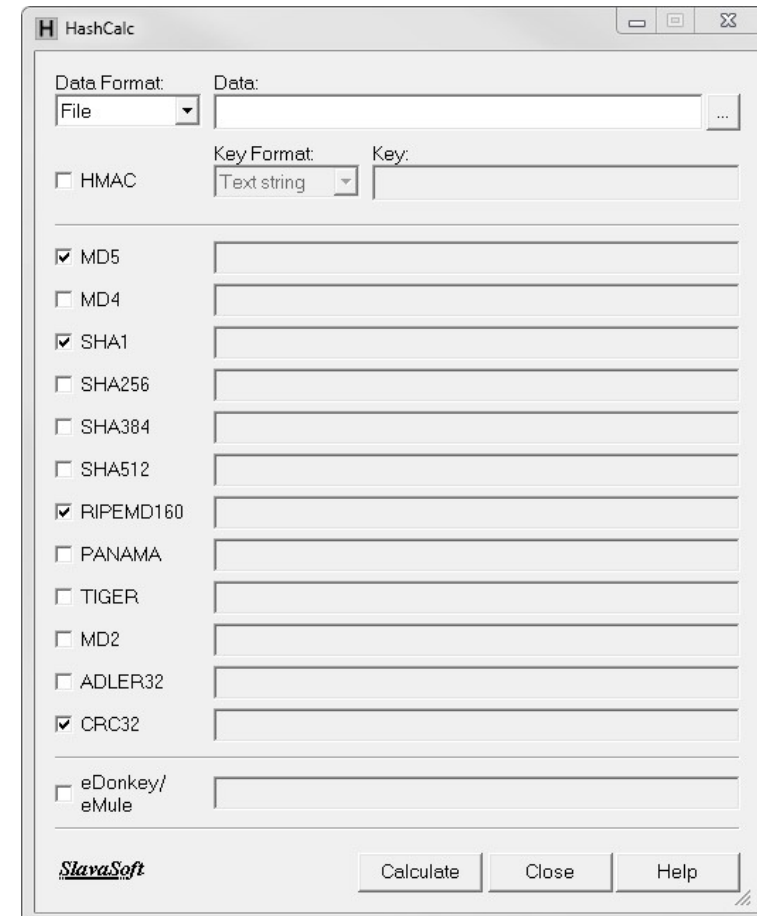


- b. Haga clic en **Descargar** en la fila **HashCalc 2.02**.
c. Abra el archivo **hashcalc.zip** y ejecute el archivo **setup.exe** que está en su interior.



- d. Siga el asistente de instalación para instalar HashCalc.
e. Haga clic en **Finalizar** en la última pantalla y cierre el archivo **README** si está abierto. Puede leer el archivo, si lo desea.
f. HashCalc ahora está instalado y en funcionamiento.

- a. Siga el asistente de instalación para instalar HashCalc.
b. Haga clic en **Finalizar** en la última pantalla y cierre el archivo **README** si está abierto. Puede leer el archivo, si lo desea.
c. HashCalc ahora está instalado y en funcionamiento.



Práctica de laboratorio 1

Paso 3: Calcular un hash del archivo Hash.txt

- a. Establezca los siguientes elementos en HashCalc:
 - 1) Formato de los datos: **Archivo**.
 - 2) Datos: haga clic en el botón ... que está junto al campo Datos, navegue hasta el Escritorio y elija el archivo **Hash.txt**.
 - 3) Quite la selección de **HMAC**.
 - 4) Quite la selección de todos los tipos de hash, excepto **MD5**.
 - b. Haga clic en el botón **Calcular**.
¿Cuál es el valor junto a **MD5**?
-

Paso 4: Haga un cambio en el archivo Hash.txt : Introduce la hora

- a. Navegue hasta el Escritorio y abra el archivo **Hash.txt**.
- b. Realice un cambio menor en el texto, como eliminar una letra, o agregar un espacio o un punto.
- c. Haga clic en **Archivo > Guardar** y cierre el **Bloc de notas**.

Paso 5: Calcule un nuevo hash del archivo Hash.txt

- a. Haga clic en el botón **Calcular** en HashCalc nuevamente.
¿Cuál es el valor junto a MD5?
-

¿El valor es diferente del valor registrado en el paso 3?

- b. Coloque una marca junto a todos los tipos de hash.
 - c. Haga clic en **Calcular**.
 - d. Fíjese cómo muchos de los tipos de hash crean un hash de longitud diferente. ¿Por qué?
-



<https://www.netacad.com/es/courses/cybersecurity>

- TAREAS 1 a 8

- TEST FINAL :

- <55%:0
- 55%-59%:1
- 60-64%:2
- 65%-69%:3
- 70%-74%:4
- 75%-79% :5
- 80% -84%:6
- 85%-89%:7
- 90%-94%:8
- 95%-99%:9
- 100%:10

- Entregar tareas 1, 2, 3 4 y 5
 - Miércoles 10 de Noviembre 8:30
- Entregar tareas 6, 7 y 8
 - Viernes 12 de Noviembre 12:30