Seguridad Informática

UNACHI – FAC- DE ECONOMÍA – LIC. GESTIÓN DE T. I.

Prof. Andrés Miranda Cerceño

Septiembre de 2024

¿Qué es la Seguridad Informática?

La Seguridad Informática es una especialidad o disciplina con la disponibilidad de proteger la estructura de los computadores y todos los dispositivos electrónicos.

Dentro de la Protección de la Seguridad Informática, podemos destacar algunos conceptos, tales como:

- ✓ Salvaguardar la **confidencialidad** de los datos.
- ✓ Preservar la **integridad** de los datos.
- ✓ Generar la **disponibilidad** de datos para usuarios autorizados.
- ✓ Proteger la **autenticidad** de la información.

Objetivos de la Seguridad Informática

Confidencialidad:

Los ciberdelincuentes cada día utilizan métodos y herramientas que son una amenaza para la información de las empresas Privadas o Públicas.
Todo profesional del área de Tecnología, que tiene a su cargo la creación, implementación o de mantener la estructura de seguridad informática, debe tener claro lo importante que TODO es Confidencial.

Integridad:

Todo profesional en el área de Tecnología de ciberseguridad o Seguridad Informática es necesario asegurar que bajo ninguna circunstancia se pueden modificar los datos .
Es Importante tener claro que los datos tengan una seguridad, que estén protegidos de un borrado, además de otras prácticas como las copias de seguridad.

Disponibilidad:

Solo los usuarios o las personas que tengan la autorización, pueden acceder a los sistemas, los datos o informaciones, en el momento que se necesiten o se soliciten.

Organismos de Normalización Internacionales

Las siglas ISO/IEC se refieren a los organismos de normalización internacionales. ISO es la Organización Internacional de Normalización, y IEC es la Comisión Electrotécnica Internacional.

Estos organismos establecen estándares y certifican empresas que cumplen con altos estándares de calidad en sus procesos

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

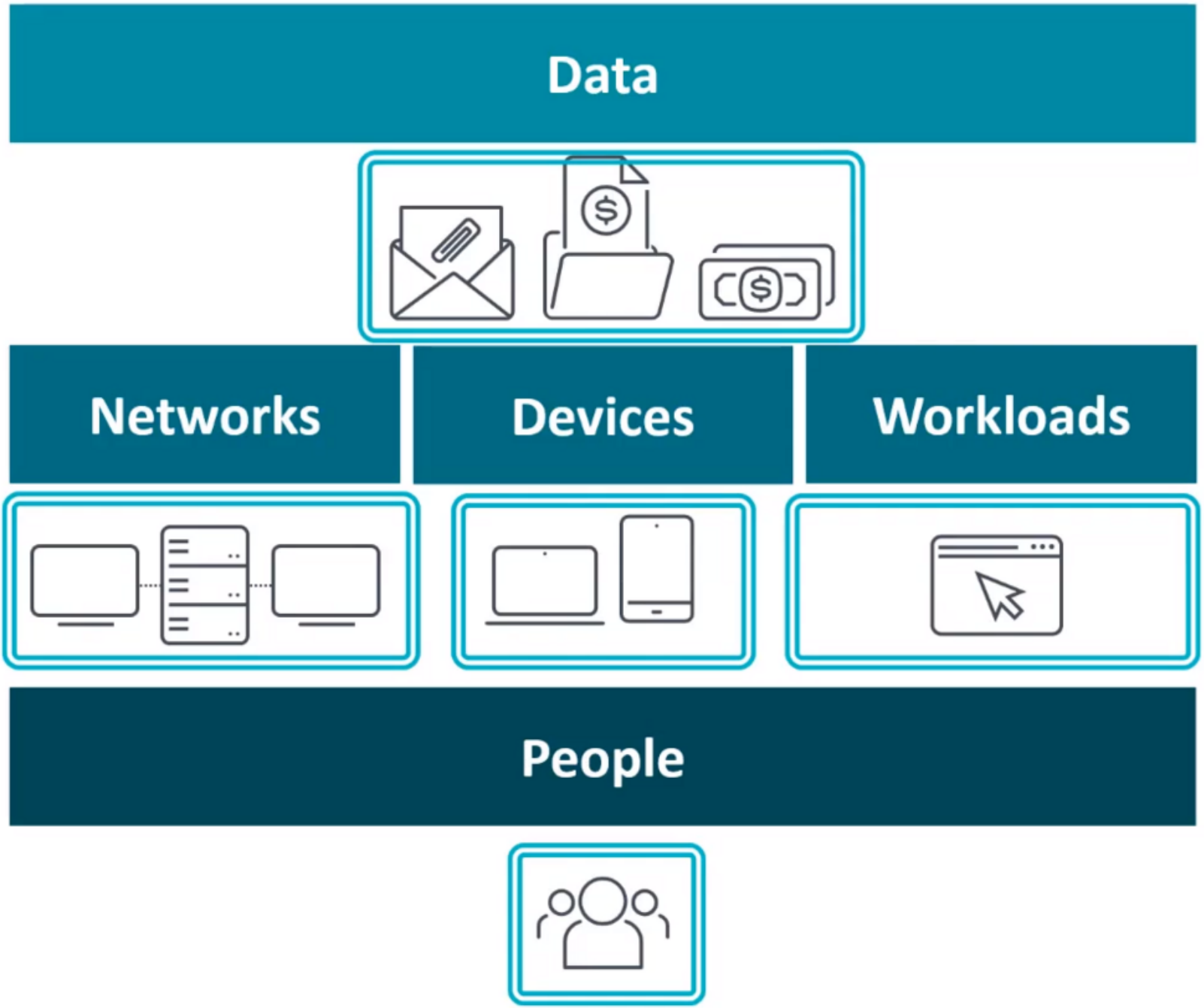
La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

¿Qué es Zero Trust?

Forrester creó este concepto en 2010 en contraste con el modelo de seguridad tradicional que se basa en la premisa de **"confiar pero verificar".**

Zero Trust, en cambio, establece que las organizaciones nunca deben confiar en una entidad ya sea interna o externa. En otras palabras, **"nunca confíes, verifica siempre".**

El modelo Zero Trust crea seguridad en torno a cada uno de los recursos y entidades clave de una organización: datos, redes, dispositivos, cargas de trabajo y personas.



- ✓ VISIBILITY
- ✓ POLICIES
- ✓ AUTOMATION

¿Qué debe hacer una organización para implementar el modelo de confianza cero?

Hay tres áreas centrales de capacidad que una organización debe desarrollar a medida que implementas el **modelo Zero Trust:**

1. Visibilidad: identifique los dispositivos y recursos que se deben supervisar y proteger. No es posible proteger un recurso que no conoce. Tener visibilidad de todos sus recursos y puntos de acceso es indispensable.

2. Políticas: Establezca controles que solo permitan que personas específicas tengan acceso a recursos específicos en condiciones específicas. En otras palabras, se requiere un nivel granular de controles de directiva.

3. Automatización: Automatice los procesos para garantizar la correcta aplicación de las políticas y permitir que la organización se adapte rápidamente a cualquier desviación de los procedimientos estándar.

Basándose en las capacidades fundamentales descritas aquí, podemos definir Zero Trust como un modelo de seguridad que construye defensas alrededor de cada una de las siguientes entidades**: datos, redes, dispositivos, cargas de trabajo y personas.**

¿Cómo funciona una arquitectura de confianza cero o seguridad Zero Trust?

La **Implementación de Confianza Cero** implica requerir una verificación de identidad estricta para cada persona o dispositivo que intente acceder a la red o aplicación. Esta verificación se aplica independientemente de si el dispositivo o usuario ya está dentro del perímetro de la red.

La Superficie de Protección

La protección comienza identificando su superficie de protección, que se basa en datos, aplicaciones, activos o servicios, comúnmente referidos por el acrónimo **DAAS:**

- ✓ **Datos**: ¿Qué datos tiene que proteger?
- ✓ **Aplicaciones**: ¿Qué aplicaciones tienen información confidencial?
- ✓ **Activos**: ¿Cuáles son sus activos más sensibles?
- ✓ **Servicios**: ¿Qué servicios puede vulnerar un actor malicioso en un intento de interrumpir el funcionamiento normal de TI?

Establecer esta superficie de protección, le ayuda a perfeccionar exactamente lo que debe protegerse.

Una política de confianza cero o modelo Zero Trust, implica regular el tráfico relacionado con los datos y componentes críticos mediante la formación de microperímetros.

En el borde de un microperímetro, una red de confianza cero emplea una **Puerta de Enlace de Segmentación**, que monitorea la entrada de personas y datos. Aplica medidas de seguridad diseñadas para examinar exhaustivamente a los usuarios y datos antes de otorgar acceso utilizando un firewall de Capa 7 y el método Kipling.

Una regla de **Capa 7** implica inspeccionar la carga útil de paquetes para ver si coinciden con los tipos de tráfico conocidos.

Si un paquete contiene datos que no cumplen con los parámetros de la regla de **Capa 7**, el acceso se bloquea.

El método de Kipling cuestiona la validez del intento de participación haciendo seis preguntas sobre la participación y quién está tratando de ingresar: **¿Quién? ¿Qué? ¿Cuándo? ¿Dónde? ¿Por qué? ¿Cómo?** Si la respuesta a cualquiera de las

¿Qué es un escritorio como servicio (DaaS)?

Desktop-as-a-Service (DaaS) es una forma de ofrecer entornos completos de escritorios virtuales a los usuarios, incluidos sistemas operativos, aplicaciones, archivos y preferencias de usuario desde la nube. Los escritorios se ejecutan en **Virtual Machines** alojadas en una infraestructura de computación, almacenamiento y red administrada por el proveedor de la nube.

Los usuarios pueden acceder a su entorno de escritorio desde una amplia variedad de dispositivos, incluidos PC, computadoras portátiles, tabletas y algunos smartphones.

Muchas organizaciones buscan una alternativa al modelo tradicional de despliegue de escritorio, en el que los administradores de TI instalan un sistema operativo y aplicaciones en cada dispositivo de los empleados.

Con ese modelo, los administradores suelen gastar demasiado tiempo y dinero instalando software, administrando actualizaciones e intentando proteger los dispositivos.

DaaS versus infraestructura de escritorio virtual

Al igual que las ofertas de DaaS, las soluciones de infraestructura de escritorio virtual (VDI) ofrecen escritorios a dispositivos desde un centro de datos centralizado.

Con el modelo DaaS, la infraestructura de **cómputo, almacenamiento y red** son gestionadas por un proveedor de la nube.

La organización que proporciona escritorios a sus empleados puede administrar el **sistema operativo de escritorio, las aplicaciones, el software antivirus** y cualquier otra tarea relacionada con el escritorio, o trabajar con un proveedor de servicios de escritorio administrado por terceros.