Universidad Nacional
Federico Villarreal

FACULTAD DE INGENIERÍA
ELECTRÓNICA E INFORMÁTICA

INGENIERIA DE SISTEMAS DE INFORMACIÓN

Docente: Ing. Alejandro Rea

Lima Perú Junio 2025

Sesión 12

Tipos de ciberseguridad

Para entender mejor en qué consiste la ciberseguridad y cómo se implementa, veamos cuáles son sus principales áreas operativas.

Ciberseguridad de la infraestructura crítica

Garantiza el funcionamiento de los principales sistemas y redes de los países, tales como las redes de carreteras, servicios públicos, agua potable o energía eléctrica.

Seguridad en la red

Se enfoca en la protección de redes informáticas a través de soluciones como cortafuegos, detección de intrusiones, cifrados, controles de acceso, etc.

Seguridad en la nube

Resguarda toda la información que es almacenada y compartida en la nube, evitando la pérdida de datos, robo de credenciales, entre otras acciones perjudiciales.

Seguridad de IoT

Los dispositivos que funcionan a través de Internet son propensos a sufrir ataques cibernéticos, por lo que requieren sistemas de seguridad como autenticación o encriptación.

Seguridad de los datos

Asegura que el intercambio de datos entre un usuario a otro se realice de forma segura, a través de soluciones como el cifrado, restricciones de acceso o copias de seguridad.

Seguridad de las aplicaciones

Es un tipo de ciberseguridad que detecta y corrige elementos vulnerables en el código de una aplicación, evitando que puedan ser explotados por hackers y programas maliciosos.

Seguridad de los puntos de conexión

Mitiga todos los riesgos involucrados al momento de ingresar a la red de una organización de forma remota. Puede clasificarse como un componente de la seguridad de la red.

Planificación de la recuperación de desastres y continuidad del negocio

Establece una serie de políticas y procedimientos para responder a un ciberataque de forma inmediata, sin comprometer el funcionamiento de una empresa.

Educación del usuario final

Se centra en la capacitación del personal de una organización para que puedan detectar cualquier indicio de amenaza y reaccionar a tiempo.

Últimas innovaciones tecnológicas en ***ciberseguridad***

¿Qué aportan las tecnologías modernas de ciberseguridad?

La ingeniería en ciberseguridad ha permitido desarrollar herramientas que facilitan la protección de datos para las organizaciones. Estos son algunos ejemplos.

Confianza cero

Este principio establece que, por defecto, ninguna aplicación ni usuario es confiable, incluso si forman parte de una organización. En base a ello, se realizan controles de acceso y supervisión de aplicaciones.

Análisis del comportamiento

Monitorea las actividades de transferencia o intercambio de información, a fin de detectar comportamientos sospechosos y tomar las medidas necesarias.

Sistema de detección de intrusiones

Son herramientas que se utilizan para identificar amenazas de ciberataques, a través de sistemas modernos como machine learning y estrategias como el análisis de datos.

Cifrado en la nube

Consiste en aplicar códigos de seguridad en los datos antes de subirlos a la nube, impidiendo el acceso de personas no autorizadas.

Conclusión

En resumen, la **ciberseguridad** es esencial en un mundo digitalizado donde las amenazas son cada vez más sofisticadas. Ya sea a nivel individual o organizacional, comprender y aplicar medidas de **ciberseguridad** no solo protege la información sensible, sino que también asegura la continuidad de las operaciones.

Caso de estudio

La empresa ciber-resiliente: la nueva estrella de la ciberseguridad

Presentar 2 informes, en formato Word al correo (hasta la 5pm se recepcionará):
area@unfv.edu.pe