



DESARROLLO FULL STACK INTERMEDIO.

UNIDAD 11

Conocimientos básicos sobre
el concepto Full Stack

Objetivo

Evaluar los conocimientos en seguridad y redes

Temática

Seguridad y redes Introducción a IPv6

Descripción de la actividad

Describa un escenario tecnológico real, donde se evidencia una posible amenaza y/o riesgo, para esto tenga en cuenta el siguiente gráfico.

➤ Paso para definir un riesgo.

1. ¿Cuál es su riesgo?
2. ¿Cuál es su amenaza?
3. Causas de probabilidad de ocurrencia del riesgo, mínimo 3 máximo 5.
4. ¿Por qué de las causas?
5. Consecuencia del riesgo asociado al impacto.
6. Control (fecha, responsable, evidencia)

➤ Clasificación de evento de riesgo y/o amenaza tecnológica.

AMENAZA (descripción)

RIESGO (descripción)

CAUSA (descripción)

**Probabilidad /
impacto (cualitativo)**

POR QUÉ (descripción)

CAUSA RAÍZ (descripción)

CONSECUENCIAS (descripción)

CONTROL (descripción)

FECHA: DD-MM-AAAA

RESPONSABLE:

Evidencia (imágenes)

Para el siguiente ejercicio, es importante aclarar que se hace con fines académicos y prácticos de ethical hacking. La Universidad Distrital Francisco José de Caldas no se hace responsable por el uso indebido que pueda ocasionar terceros ya terceros.

Objetivo: Conocer a través de un ejercicio práctico ethical hacking cómo funciona y opera software de phishing a través de un simulador de correo web.

1. Ingrese al enlace desde una red diferente a la de la Universidad Distrital (bloqueo de dirección web). En caso de no poder acceder utilice una VPN web para poder acceder, el sitio mencionado por se un generador de correo es bloqueado por navegadores, antivirus web y algunos navegadores.
<https://emkei.cz/>
2. A continuación para este caso se diligencia la siguiente información con fines académicos.
3. From Name: (Nombre de la entidad remitente) - Fabrica Proximus
4. From E-mail: (Cuenta de correo a suplantar) – gerencia@proximus.com
5. To: (Cuenta de correo destinatario) – su cuenta de correo
6. Subject: (Asunto de correo) – Bono de Compra – prueba
7. Attachment: (Imágenes de tecnología) – opcional
8. Text: (Cuerpo del correo) – Me permito remitir bono para compra de productos de tecnología.

Figura. 2 generador de correo ejercicio

Figura. 3 diligenciamiento generador de correo ejercicio

Figura. 4 bandeja de correo ejercicio

Conclusión, existen diversas herramientas, sistemas y métodos para realizar ataques informáticos o ciberataques; sin embargo, en el ecosistema tecnológico se debe estar constantemente informado para saber cómo operan organizaciones, métodos y/o herramientas maliciosas, cuyo objetivo es irrumpir la tranquilidad de los usuarios y el robo de información.