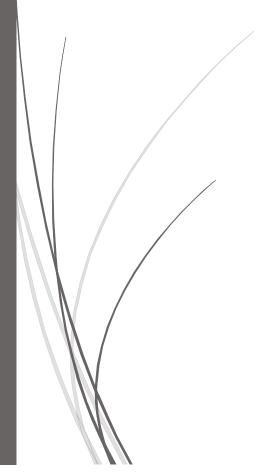
9/11/24

Caso Practico

Bootcamp de Desarrollo Web



Daniel Bonilla González UVM

Objetivo

Crear una página web sobre el tema de tu elección con el uso de HTML y CSS. Éste ejercicio tiene como objetivo desarrollar los conocimientos adquiridos durante el módulo 1, aplicando conocimientos como el uso de las diferentes secciones Head, Body de un HTML, así como el uso de estilado con CSS.

Instrucciones

Crear un archivo HTML que contenga la estructura de tu página web y que incluya varios de los elementos revisados en clase, como:

- Header
- Artículo
- Párrafo
- Imagen
- Crea un archivo CSS para dar estilo a tu página Web, haciendo uso de al menos 2 tipos de selectores (id, clase, etiqueta)

Enlace a github:

https://github.com/Nakajito/CasoPractico

Protección en la era digital

La ciberseguridad es un conjunto de prácticas, tecnologías y procesos diseñados para proteger los sistemas informáticos, redes y datos de ataques cibernéticos. En un mundo cada vez más conectado, la ciberseguridad es crucial para garantizar la confidencialidad, integridad y disponibilidad de la información. Los riesgos asociados con el cibercrimen, como el robo de datos, ataques de malware, phishing y ransomware, han crecido exponencialmente en los últimos años, afectando tanto a individuos como a grandes organizaciones.

Uno de los principales objetivos de la ciberseguridad es prevenir el acceso no autorizado a datos sensibles. Esto se logra implementando controles de seguridad, como el uso de firewalls, antivirus, cifrado de datos, y autenticación multifactorial (MFA). Estos mecanismos aseguran que solo las personas autorizadas puedan acceder a la información, reduciendo las posibilidades de brechas de seguridad.



¿Por qué es tan importante la ciberseguridad?

La ciberseguridad es fundamental en una sociedad digitalizada, ya que protege los activos más vallosos de empresas y personas: los datos. Un fallo en la seguridad puede provocar pérdidas económicas, daño a la reputación y, en casos graves, el colapso de infraestructuras críticas como servicios de salud, transporte o energía.

Además, con el aumento del trabajo remoto y el uso de dispositivos móviles, las amenazas cibernéticas han adoptado formas más sofisticadas. El uso de redes no seguras o la falta de concienciación en el manejo de información digital son factores que incrementan la vulnerabilidad ante ciberataques. Aquí es donde la concienciación en ciberseguridad juega un papel esencial. Educar a los usuarios para detectar correos de phishing, usar contraseñas fuertes y evitar conexiones públicas inseguras son medidas básicas pero efectivas.

Desafíos actuales en la ciberseguridad

Los ataques cibernéticos evolucionan continuamente, con nuevas amenazas apareciendo cada día. Entre los desafios más grandes destacan:

Ataques de día cero: Son vulnerabilidades desconocidas que los ciberdelincuentes explotan antes de que los desarrolladores puedan solucionarlas.

Ransomware: Este tipo de malware bloquea el acceso a los sistemas hasta que se paga un rescate...

Amenazas internas: No todas las amenazas provienen del exterior...

Futuro de la ciberseguridad

Con la llegada de tecnologías emergentes como el Internet de las Cosas (IoT), inteligencia artificial (IA) y blockchain, la ciberseguridad enfrentará nuevos retos. Estas tecnologías, si bien ofrecen beneficios significativos, también amplian la superficie de ataque. A medida que las empresas adoptan soluciones en la nube y los dispositivos conectados, será crucial establecer nuevos estándares y prácticas para mitigar los riesgos.

En resumen, la ciberseguridad es esencial para mantener la seguridad y privacidad en el mundo digital. Adoptar buenas prácticas, estar informado sobre las amenazas y utilizar herramientas avanzadas son pasos críticos para proteger nuestra información personal y empresarial.

Legal

```
sse"mandar nambar-espand-ig nambar-dark bg-dark border-bottom">
cl de scontion"
contion"
contion"
contion"
contion"
cl des se"mandar brefs"#">
intellemterc/as
duston classe "mandar brefs"#">
intellemterc/as
duston classe "mandar classe "mandar type-button" data-bs-topple="collapse" data-bs
-emandarContert "ata-espanded"
classe "mandar-topple"-icon">
classe "mandar
                                                                                                                                                                                                                        dys
discrete service serv
                                                                                                                              ticle>
-dl class="text-center mb-4'>Protectión en la era digital</hl>
-div class="text-center">
-div class="text-center">
-span class="text-center">
-span class="text-center">
-span class="deblock at-2" datetime="3824-11">
-time class="deblock at-2" datetime="
                                                                                                   "(pp lass="lead"»
*Uno de los principales objetivos de la ciberseguridad es prevenir el acceso no autorizado a datos sensibles. Esto se logra implementando controles de seguridad, como el uso de firewalls, antivirus, cifrado di datos, y autenticación multifactorial (MA). Estos escanismos aseguran que solo las personas autorizadas puedan acceder a la información, reducendo las posibilidades de brenhas de seguridad.

</p
    cibersegurudad*

- esection class="by-4">
- es
         mergia.

*/pp

*\pi class='lead'>

*\pi class=
riesgos.

-{pp.
-{
                                                          script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js" <mark>integrity=</mark>"sha384
Yf0tY3LMB6MNNkmXcSs9fDVZLE5aAA55MD2Oxhy9Gkc[dslkleN7N6j]EdEz" <mark>crossorigin=</mark>"anonymous"></script>
```