UNIVERSIDAD TÉCNICA DE COTOPAXI
FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS
INGENIERÍA EN SISTEMAS DE LA INFORMACIÓN

CONTROL Y AUDITORIA INFORMÁTICA

NOMBRE: Anthony David Toapanta Chancusig Fecha: 27/05/2025

INFORME DE AUDITORÍA

1. OBJETIVO

Realizar la valoración de los resultados obtenidos en el proceso de Auditoría Informática al sitio web: https://soporte.uce.edu.ec/pages/UI.php, con el fin de identificar vulnerabilidades de seguridad, deficiencias técnicas y oportunidades de mejora.

2. ALCANCE

La realización de esta auditoría se llevó a cabo en tres etapas:

- **Primera etapa:** Análisis del código fuente HTML del sitio, identificando prácticas inseguras, estructuras obsoletas y ausencia de medidas de protección del lado cliente.
- **Segunda etapa:** Evaluación de los niveles de seguridad mediante pruebas con la herramienta **Setoolkit** en **Kali Linux**, simulando ataques de ingeniería social para la obtención de credenciales.
- **Tercera etapa:** Diseño de un sitio web clonado con fines de prueba, demostrando la posibilidad de aplicar técnicas de **phishing** sin barreras de detección.

Adicionalmente, se analizó:

- La **seguridad física y lógica** del entorno web.
- El manejo del **almacenamiento y respaldos de información**.
- Existencia de **planes de mantenimiento**.
- Disponibilidad de **documentación técnica y administrativa** del sistema y sus componentes.

3. DESCRIPCIÓN DEL SITIO A AUDITAR

El sitio https://soporte.uce.edu.ec/pages/UI.php corresponde a una interfaz de soporte técnico de la Universidad Central del Ecuador. Este sistema permite el ingreso de usuarios mediante credenciales y brinda acceso a funcionalidades administrativas relacionadas con solicitudes de soporte. La página está desarrollada utilizando HTML básico sin cifrado HTTPS forzado, lo cual representa un riesgo elevado.

4. SITUACIÓN OBSERVADA (HALLAZGOS) Y RECOMENDACIONES

Área: Seguridad Lógica

Nombre del Componente: Acceso de los usuarios al Sitio.
Hallazgo: El sitio no cuenta con cifrado HTTPS por defecto, permitiendo la exposición de credenciales en texto plano. Además, no implementa mecanismos de autenticación robusta (como 2FA).
Recomendación: Forzar HTTPS en todo el sitio web, utilizar certificados SSL válidos, e implementar autenticación multifactor (MFA) para todos los accesos.

Nombre del Componente: Acceso de los usuarios a formularios y/o Aplicaciones.
Hallazgo: Los formularios no cuentan con validación del lado servidor ni protección contra inyecciones SQL o XSS.
Recomendación: Implementar validación del lado servidor, filtros de entrada de datos, y utilizar medidas anti-XSS como sanitización del contenido ingresado.

Área: Seguridad Física

Nombre del Componente: Control de accesos de los usuarios a las opciones de administración.
Hallazgo: No se detectó segmentación de accesos ni control adecuado de perfiles de usuario. Cualquier usuario autenticado parece poder acceder a secciones sensibles.
Recomendación: Aplicar controles de acceso basados en roles (RBAC) e implementar restricciones por nivel de privilegios.

Nombre del Componente: Niveles de seguridad o aplicaciones de seguridad Identificadas a nivel de sitio web
Hallazgo: El sitio no posee firewall de aplicaciones web (WAF), ni está protegido contra escaneos automatizados.
Recomendación: Implementar un WAF para prevenir ataques comunes (OWASP Top 10) y habilitar servicios de detección de intrusiones.

Nombre del Componente: Respaldo y Plan de contingencia **(DE SER EL CASO)**
Hallazgo:
Recomendación:

Nombre del Componente: Plan de Mantenimiento de Hardware y Software (**DE SER EL CASO)**.
Hallazgo:
Recomendación:

Nombre del Componente: Disposición de manuales de usuario y de instalación de los sistemas. **(DE SER EL CASO)**
Hallazgo:
Recomendación:

Nombre del Componente: Existencia de documentos de adquisición de equipos y software. **(DE SER EL CASO)**
Hallazgo:
Recomendación:

5. CONCLUSIONES.

El sitio auditado presenta múltiples vulnerabilidades críticas tanto a nivel lógico como físico. No supera ninguna de las etapas básicas de pruebas de seguridad, siendo susceptible a ataques de ingeniería social, suplantación de identidad y robo de información. Se recomienda una reestructuración integral del sitio, incluyendo implementación de protocolos de seguridad actualizados, planes de respaldo, documentación formal y controles de acceso avanzados. La situación actual pone en riesgo la integridad, disponibilidad y confidencialidad de la información institucional.