



Soluciones Virtuales e Infraestructura Tecnológica

INFORME TÉCNICO: CORRECCION DE VULNERABILIDADES v2.0

Preparado por

Fabian Toapanta
ftoapanta@virtualit.com.ec

Enero, 2018



SOLUCIONES VIRTUALES E
INFRAESTRUCTURA
TECNOLOGICA VIRTUALIT S.A.

RUC: 1792018080001

Calle Gaspar Escalona N38-39
y Villalengua

Quito - Ecuador

Tel (593) 2 381 5950

www.virtualit.com.ec

CONTENIDO

1	Antecedentes	2
2	Objetivos	2
3	Planificación de actividades.....	2
4	Conclusión	4
5	Consideraciones.....	4

1 Antecedentes

Durante el periodo de capacitación del Portal a la Corporación Nacional de Telecomunicaciones se observaron y receptaron distintas críticas y peticiones con relación al funcionamiento actual del portal por lo cual se hace necesario realizar una planificación para afrontar las nuevas necesidades.

2 Objetivos

- Diagnosticar las mejores soluciones para satisfacer las necesidades o requerimientos del portal CNT.
- Realizar la implantación de las soluciones en el entorno de desarrollo para su correspondiente aprobación.

3 Planificación de actividades

Nº	Tarea	Detalle	Complejidad	Tiempo (Horas)
1	Integración del campo RUC en registro de cliente	Se debe añadir el campo ruc en la base de datos y las solicitudes a dicha tabla incluyendo la vista de registrar e integrar a las vistas que contengan información sobre el cliente	Baja	2
2	Verificación de autenticación con la organización	Se requiere la creación de una tabla en base de datos que contenga la información de la organización y los componentes modelo, vista y controlador para la gestión de dicha información (Se debe buscar la integración con la tabla de clientes ya existente y sus respectivas compras almacenadas en carrito)	Alta	16
3	Información en relación al producto y la asesoría por parte del personal comercial de CNT	Se requiere colocar información con relación a los productos en la cual detalle que el producto puede ser modificado y resaltar que se puede disponer de asesoramiento por parte del personal comercial (esta información debe ser dinámica ya que se debe poder modificar en cualquier momento sin necesidad de ingresar a código fuente)	Baja	4

4	Asignación de usuarios a solicitudes de carrito dependiendo el estado de la solicitud	Se requiere la creación de una tabla que almacene la relación entre carrito–usuarios, además la implementación de modelo, vista y controlador que gestionen dicha información.	Alta	20
5	Notificación a clientes mediante SMTP con texto personalizables (Forma de formular el contenido)	Se requiere poder almacenar el texto que se enviará al cliente cuando en el cambio de estado se encuentre habilitado la opción de envío de correo a clientes (se debe modificar la base de datos y todas las peticiones que se realizan al modelo de notificaciones. Además, se hace necesario implementar un formato en el cual el usuario pueda manipular el orden de presentación de la información en el texto de la notificación)	Alta	8
6	Implementación de estatus posventa	Se requiere la creación de un nuevo rol y el análisis de contenido y acciones al cual podrá acceder este nuevo rol Postventa (se debe crear una nueva vista o bloquear el acceso a la función de cambio de estado)	Baja	3
7	Control de acceso a estados de un producto	Se requiere buscar un control de estados en el cual el usuario no pueda ejecutar la función cambio de estado si no posee los permisos para dicho estado (Esta implementación se encuentra en alisáis de una posible solución y puede variar del ser necesario)	Alta	16
8	Carga de archivos dependiendo el estado en que se encuentren	Se debe permitir la subida de archivos en los estados que se requieran (requiere la creación de una tabla en base de datos en el cual lleve el registro de documentos y permita una óptima organización y búsqueda)	Alta	24
9	Solución a vulnerabilidad del portal contra ataques DDOS	Se debe implementar módulos al servidor web (esta opción dependerá de la compatibilidad con el entorno de xampp), aplicar reglas en el firewall que bloquen este tipo de ataques (se debe resaltar que esta opción funciona para ataques en pequeñas escalas) y	Alta	16

		se debe buscar otras soluciones que ayuden a enfrentar este tipo de ataques.		
10	Archivos navegables en el servidor web	Se debe ejecutar pruebas de vulnerabilidades al servidor web con el objetivo de mitigar cualquier acceso que permita la navegabilidad o ejecución de comandos en el servidor	Alta	8
11	Detener el servidor de aplicaciones Tomcat	Se requiere detener el servidor Tomcat y bloquear los puertos de acceso HTTP y HTTPS (8080 y 8443)	Media	2
Total de Horas				119

4 Conclusión

- Se realizó un estimado de horas trabajo concluyendo que para las tareas previamente detalladas se requiere un total de 119 Horas o 2 semanas y 3 días.

5 Consideraciones

Se debe tener en cuenta que el tiempo de desarrollo se puede alterar dependiendo la variación de una necesidad, actividades de la empresa, el tiempo en que una necesidad sea validad y aceptada.