Coloquio de proyectos
de Becarios en Seguridad Informática

Sistema de revisiones de seguridad 6to Coloquio PBSI

Ulises Viveros Campos
Arturo Samuel Santiago Mancera

UNAM CERT

DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Contenido

- Introducción
- Especificación del proyecto
- Implementación
- Funcionalidades del sistema
- Demostración
- Oportunidades de mejora
- Conclusiones

Introducción

¿Qué es una revisión de seguridad del CSI/UNAM-CERT?

Proceso mediante el cual se realizan pruebas de penetración a uno o más activos de la UNAM con la finalidad de obtener una evaluación de seguridad.

Introducción

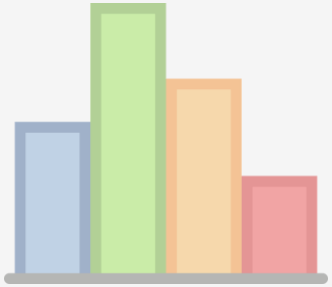
¿Cuál es el producto de una revisión de seguridad?

A partir de una revisión de seguridad se obtiene un reporte con los resultados de dicha evaluación.

Introducción

¿Para que nos sirven los reportes de una revisión de seguridad?

Los reportes de seguridad nos permiten atender las vulnerabilidades presentadas, así como obtener guías, manuales, artículos, boletines, recomendaciones, estadísticas, etcétera.



Especificación del proyecto

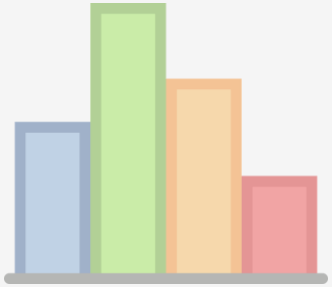
Objetivo

Implementar un sistema que permita gestionar los hallazgos derivados de las revisiones de seguridad, personal asignado y sitios involucrados, el cual genere una base de datos disponible para la obtención de un histórico y los reportes respectivos de cada revisión.

Especificación del proyecto

Requerimientos funcionales

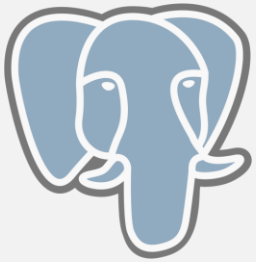
- Autenticación mediante LDAP
- Gestión y control de usuarios y roles
- Gestión de catálogo de sitios y activos
- Gestión de catálogo de hallazgos
- Gestión de flujo de trabajo de revisiones de seguridad
- Generación de reportes
- Generación de estadísticas



Implementación

Requerimientos

- Sistema operativo Debian 9.5
- Apache 2.4.25
- Drupal 7.59
- PostgreSQL 9.6.10
- Python 2.7.13 (python-docx 0.8.9)
- PHP 7.0
- Drush 7.0.0



Funcionalidades del sistema

Módulos en Drupal 7

- **Contributed**
  - Comunidad de Drupal (drupal.org)
  - LDAP, gráficas, envío de email
- **Custom**
  - Creados por el desarrollador
  - Tienen un objetivo particular

Funcionalidades del sistema

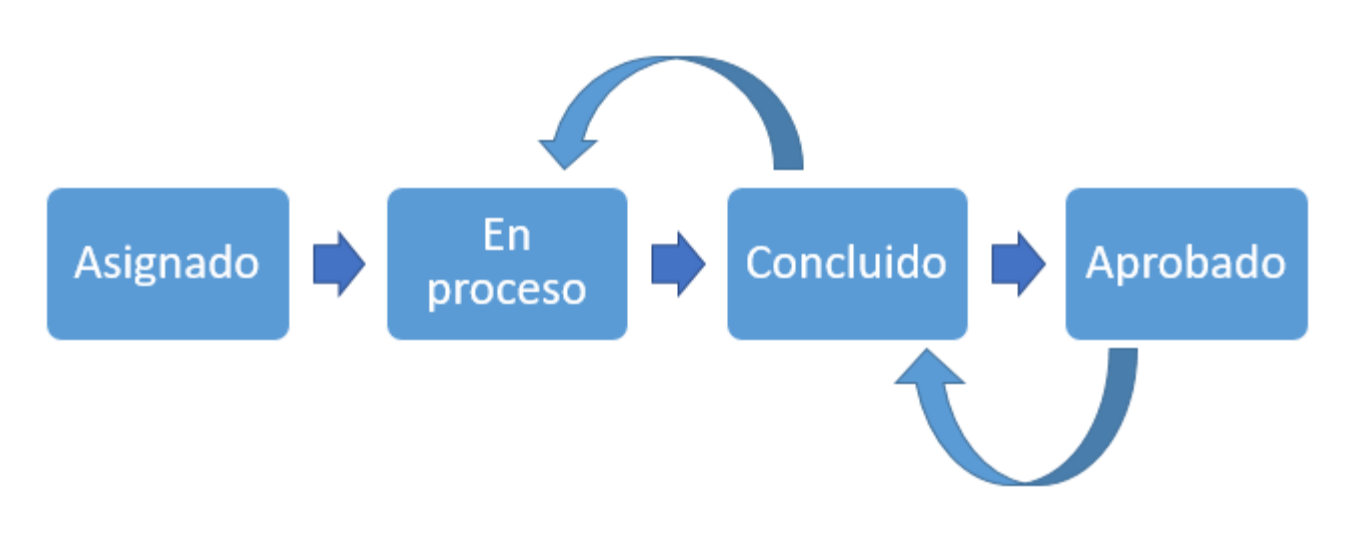
Módulos desarrollados (Custom)

- Core (Sistema de Revisiones)
- Sitios y hallazgos
  - Formulario y CSV
- Revisiones
  - Flujo de trabajo
  - Notificaciones
- Estadísticas

Funcionalidades del sistema

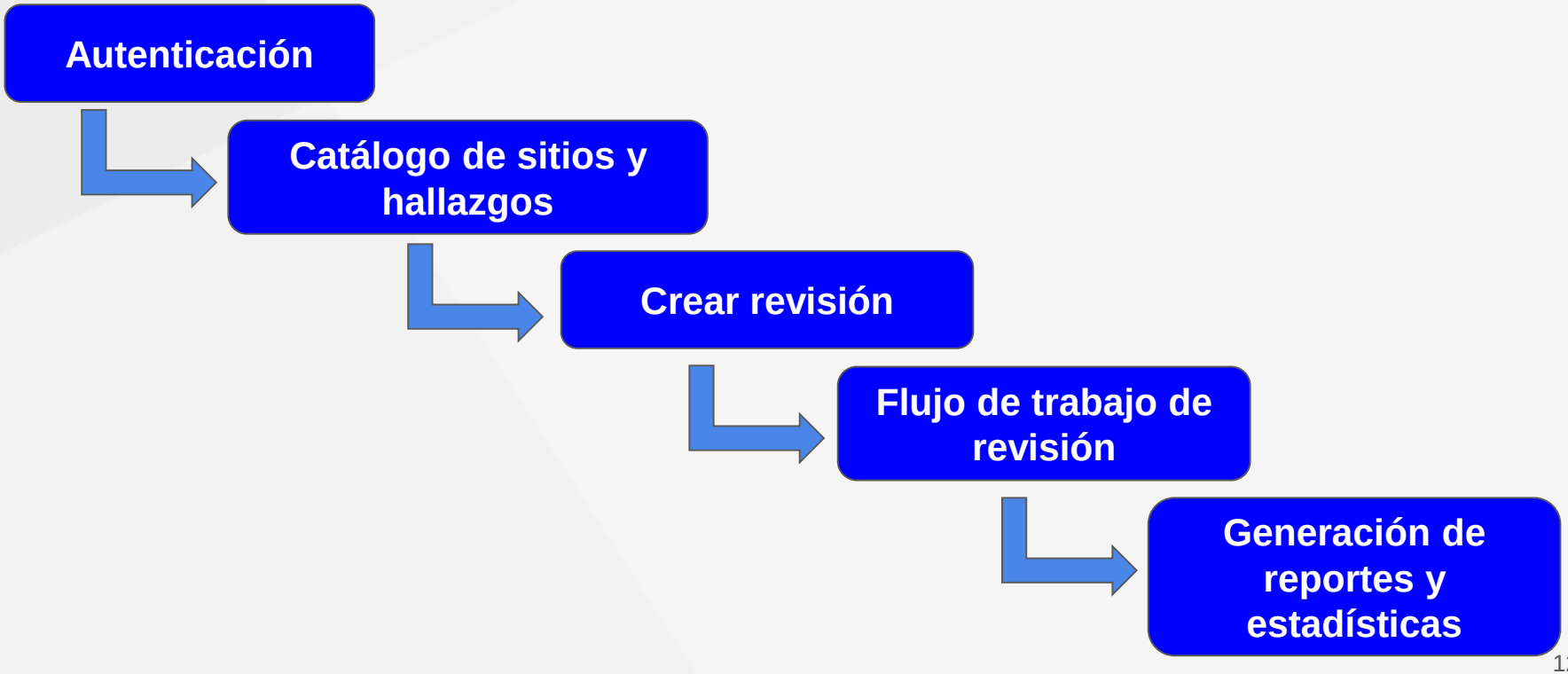
¿Cómo controlar el flujo de trabajo?

- Estados o Estatus
- Control de las revisiones



Funcionalidades del sistema

Funcionalidades



Funcionalidades del sistema

Autenticación

- Autenticación mediante LDAP
- Definición de roles
  - Coordinador
  - Pentester
  - Auxiliar
- Privilegios por rol

Funcionalidades del sistema

Catálogo de sitios y hallazgos

- Altas, bajas y edición de sitios
  - URL
  - Dependencia (catálogo)
  - IPv4
- Altas, bajas y edición de hallazgos
  - Nombre
  - Descripción
  - Solución
  - Recomendaciones
  - Impacto (CVSS v3)
  - Referencias

Funcionalidades del sistema

Crear revisión

- Definición de tipo de revisión
  - Circular
  - Oficio
  - Seguimiento
- Asignación de pentester(s)
- Asignación de sitios

Funcionalidades del sistema

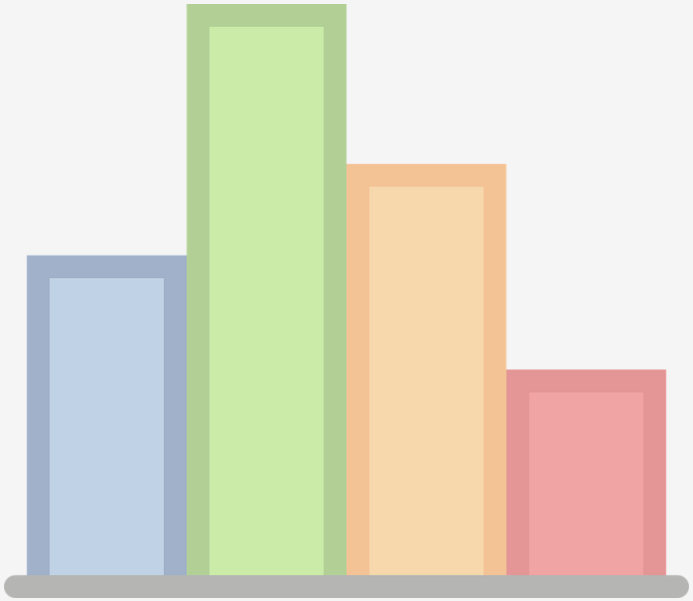
Flujo de trabajo de revisión

- Asignación de hallazgos de catálogo
- Edición de información particular de hallazgos asignados
- Gestión de comentarios
- Aprobación de la revisión

Funcionalidades del sistema

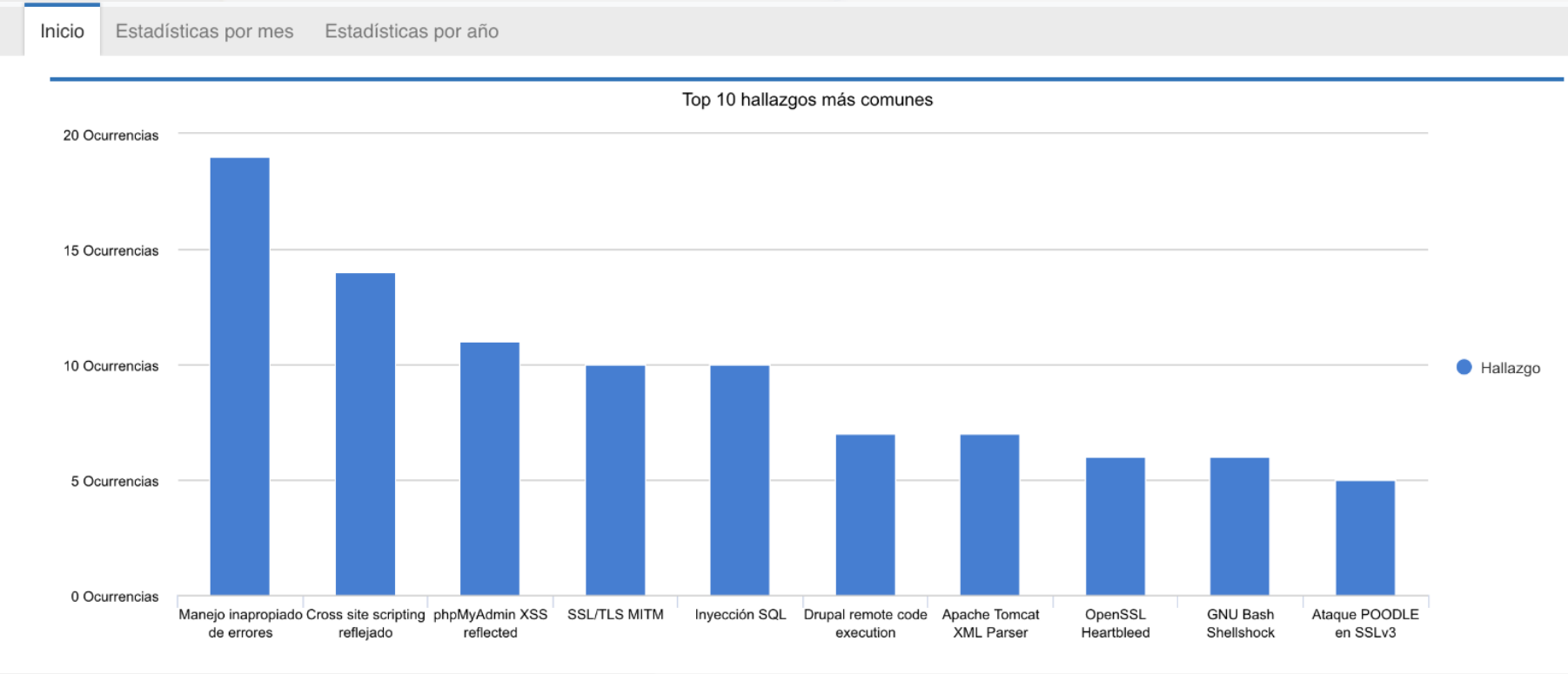
Generación de reportes y estadísticas

- Generación de reportes en formato .docx
- Generación de estadísticas
  - Por mes y año
  - Por dependencia
  - Por impacto
  - Por pentester



Funcionalidades del sistema

Hallazgos más comunes



Funcionalidades del sistema

Hallazgos por impacto

Filtro por Año

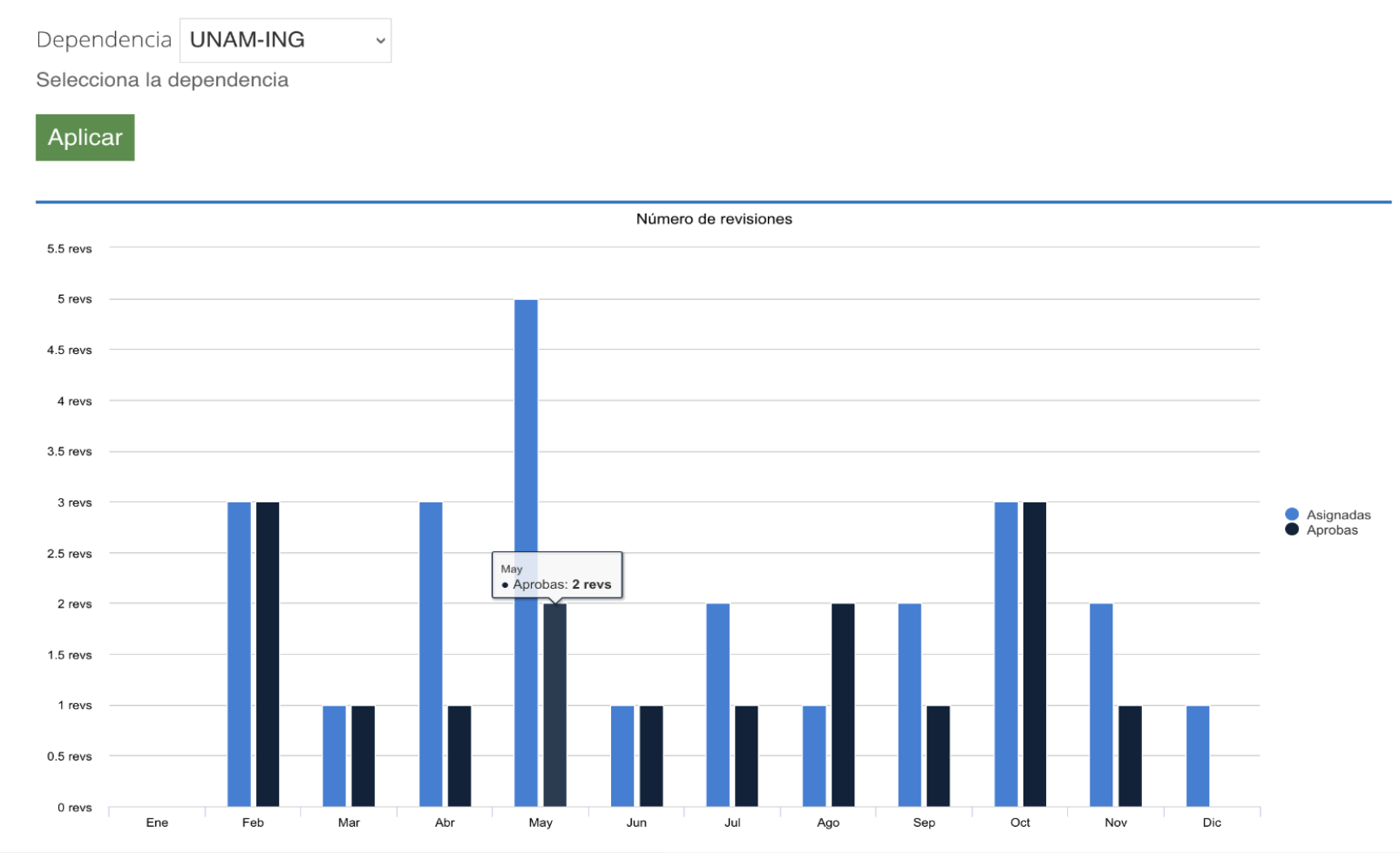
Año 2018

Selecciona el año para filtrar las gráficas

Aplicar

Funcionalidades del sistema

Revisiones por dependencia



Demostración

Oportunidades de mejora

- Agregar más tipos de gráficas
- Implementar un tema acorde a la institución
- Soporte para adjuntar más tipos de archivos a los hallazgos
- Implementación de notificaciones dentro de la sesión de usuario

Conclusiones

- Reducción de tiempos en el flujo de trabajo de una revisión
- Generación de histórico
- Visualización de resultados
- Sistema modular
- Apoyo a los procesos del UNAM-CERT de de principio a fin
- Se cumplió con el objetivo

GRACIAS

Ulises Viveros Campos
Universidad Nacional Autónoma de México
ulises.viveros@bec.seguridad.unam.mx

Arturo Samuel Santiago Mancera
Instituto Politécnico Nacional
arturo.santiago@bec.seguridad.unam.mx