

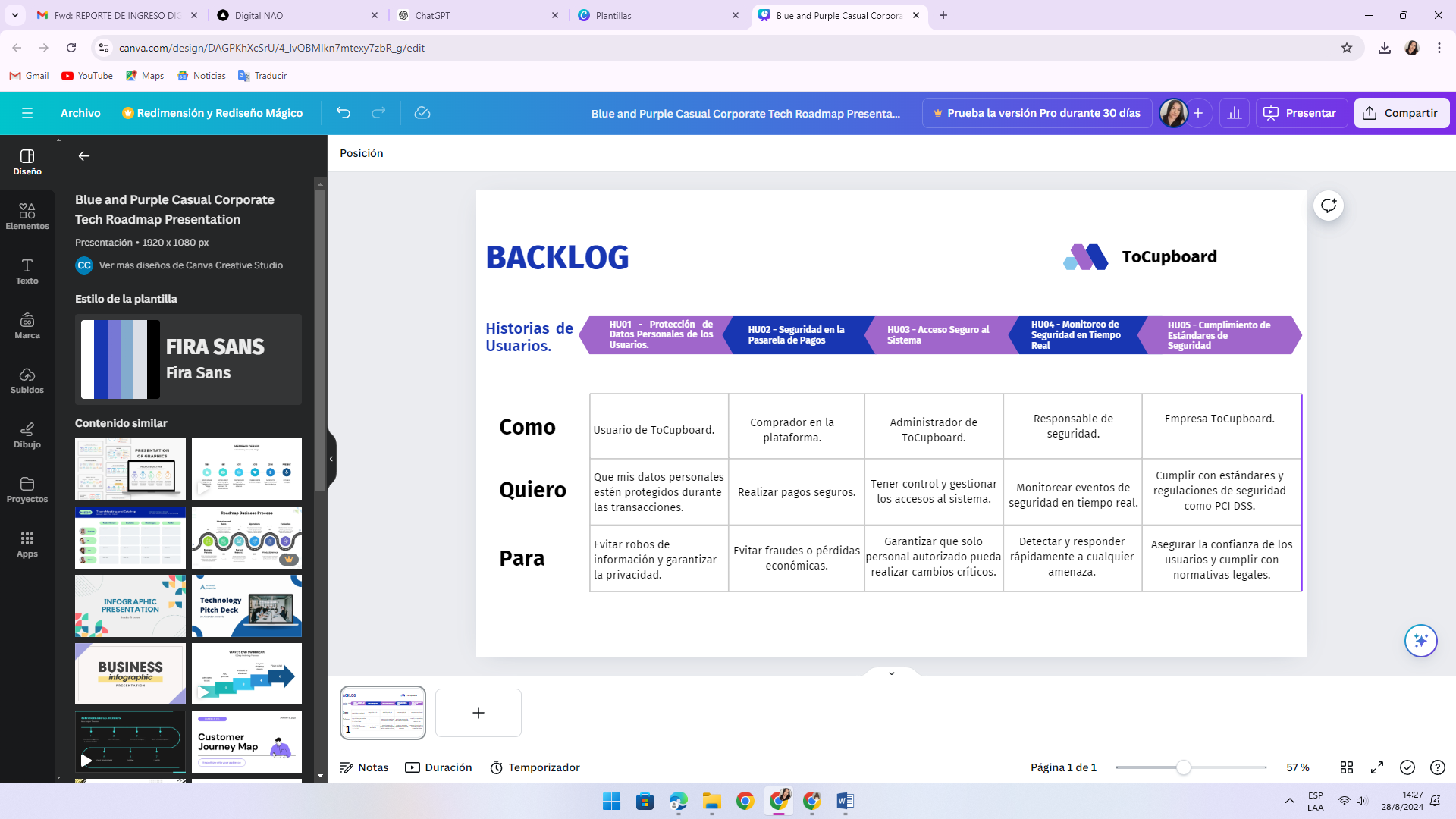
**ALUMNA:** CARMEN LISETH TRIGUERO ALVARADO

**NAO ID:** 3114

**FECHA:** LUNES, 2 SEPTIEMBRE 2024

**TRAYECTORIA:** PROTOCOLOS DE SEGURIDAD CON PESTENTING Y CRIPTOGRAFIA

**RETO 2: SPRINT 1 – PLANIFICA y DESARROLLA**

**Sprint 1**

**Backlog**

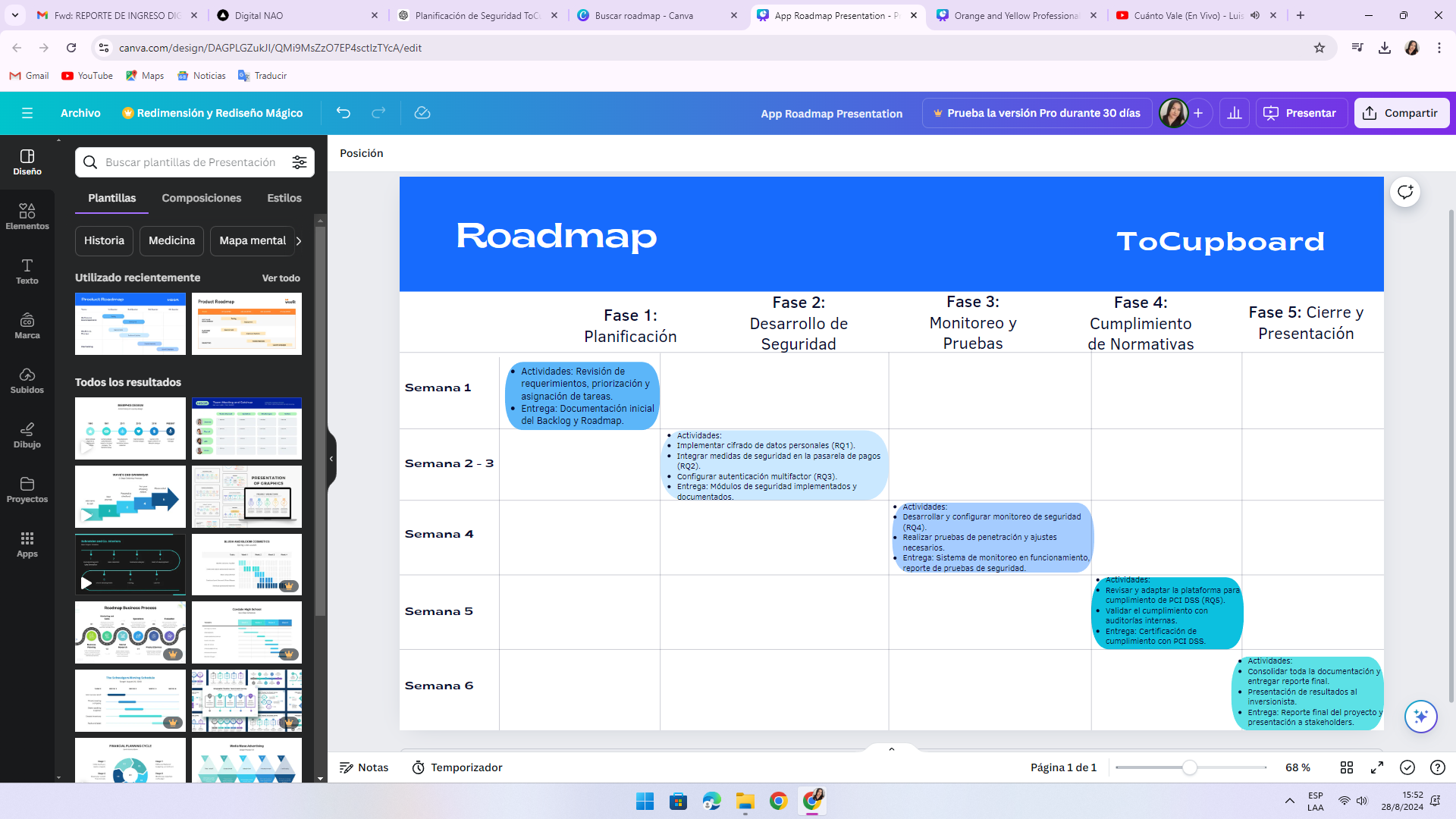
**Tabla 1. Lista de Requerimientos**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Requerimiento | Prioridad | Estimación (horas) | Responsable |
| RQ1 | Implementar cifrado de datos personales de usuarios | Alta | 20 | Juan Carlos |
| RQ2 | Integrar seguridad en la pasarela de pagos | Alta | 25 | Juan Carlos |
| RQ3 | Configurar autenticación multifactor para administradores | Media | 15 | Juan Carlos |
| RQ4 | Desarrollar sistema de monitoreo de eventos de seguridad | Alta | 30 | Juan Carlos |
| RQ5 | Adaptar la plataforma para cumplir con PCI DSS | Alta | 40 | Juan Carlos |

**Tabla 2. Registro de Tareas**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Tarea | Requerimiento | Estimación (horas) | Responsable | Estado |
| T01 | Desarrollar módulo de cifrado de datos | RQ1 | 10 | Juan Carlos | Pendiente |
| T02 | Pruebas de penetración en pasarela de pagos | RQ2 | 10 | Juan Carlos | Pendiente |
| T03 | Implementar autenticación multifactor | RQ3 | 15 | Juan Carlos | Pendiente |
| T04 | Configurar monitoreo de seguridad en SIEM | RQ4 | 20 | Juan Carlos | Pendiente |
| T05 | Evaluar conformidad con PCI DSS | RQ5 | 20 | Juan Carlos | Pendiente |

**Roadmap**



**Desarrolla**

**Presentación Ejecutiva: Modelo DevSecOps para ToCupboard**

**Introducción**

**Objetivo:** Implementar un modelo DevSecOps en ToCupboard para integrar la seguridad en todas las etapas del ciclo de vida del desarrollo de software (CI/CD), asegurando la protección de datos sensibles y la confiabilidad de la plataforma.

**Descripción del Modelo DevSecOps**

**Definición de DevSecOps:** DevSecOps es la práctica de integrar la seguridad en cada etapa del ciclo de vida del desarrollo de software, combinando las disciplinas de desarrollo (Dev), operaciones (Ops), y seguridad (Sec) para mejorar la eficiencia y la seguridad.

**Componentes Principales del Modelo:**

* **Integración Continua (CI):** Proceso de automatización para construir, probar y validar código continuamente.
* **Entrega Continua (CD):** Automatización del despliegue de aplicaciones seguras a entornos de producción.
* **Monitoreo y Respuesta:** Supervisión constante para identificar y responder a vulnerabilidades en tiempo real.

**Proceso de Integración de la Seguridad en CI/CD:**

* **Automatización de Pruebas de Seguridad:** Incluye análisis de código estático, escaneo de dependencias y pruebas de seguridad de aplicaciones.
* **Pipeline de Seguridad:** Integrar pruebas de seguridad en el pipeline de CI/CD para detectar vulnerabilidades temprano.
* **Respuesta a Incidentes Automatizada:** Implementación de alertas y acciones automatizadas ante eventos de seguridad.

**Beneficios del Modelo DevSecOps**

* **Mejora en la Seguridad de los Productos:**
* Reducción de vulnerabilidades desde el inicio del desarrollo.
* Incremento en la rapidez de detección y mitigación de amenazas.
* **Impacto Esperado en ToCupboard:**
* Fortalecimiento de la confianza de los usuarios e inversionistas.
* Cumplimiento de estándares y normativas de seguridad como PCI DSS.
* **Ejemplos de Buenas Prácticas:**
* Uso de herramientas como OWASP ZAP para pruebas de seguridad de aplicaciones.
* Implementación de autenticación multifactor y gestión de acceso con roles definidos.

**Implementación del Modelo**

**Pasos Específicos para Implementar el Modelo en ToCupboard:**

1. **Evaluación Inicial:** Diagnóstico de la infraestructura y aplicaciones actuales.
2. **Definición de Políticas de Seguridad:** Establecer políticas claras que guíen la integración de seguridad en el ciclo de desarrollo.
3. **Automatización del Pipeline de CI/CD con Seguridad:** Configurar pipelines que incluyan análisis de seguridad automatizados.
4. **Capacitación del Equipo:** Formación continua del equipo de desarrollo en prácticas de seguridad.

**Herramientas y Tecnologías Recomendadas:**

* **Jenkins:** Para la automatización de CI/CD.
* **SonarQube:** Para análisis de código estático y detección de vulnerabilidades.
* **Nessus:** Para escaneo de vulnerabilidades en aplicaciones y redes.

**Roles y Responsabilidades:**

* **Desarrollador:** Implementar código seguro y participar en revisiones de seguridad.
* **Ingeniero de Seguridad:** Liderar la integración de seguridad y monitoreo de eventos.
* **DevOps:** Mantener el pipeline de CI/CD y automatización de despliegues seguros.

**Conclusiones y Recomendaciones**

**Resumen de los Puntos Clave:**

* La adopción de DevSecOps permitirá a ToCupboard integrar la seguridad desde la fase inicial del desarrollo, reduciendo riesgos y costos asociados a vulnerabilidades.
* El modelo fortalecerá la posición de la empresa frente a competidores y mejorará la experiencia del usuario al garantizar la seguridad de sus transacciones y datos.

**Recomendaciones para la Implementación Exitosa:**

* **Involucrar a Todo el Equipo:** La seguridad es una responsabilidad compartida; todo el equipo debe participar en el proceso.
* **Monitoreo Continuo y Mejora:** Establecer un ciclo de retroalimentación constante para mejorar la seguridad de manera continua.
* **Adopción Gradual:** Implementar DevSecOps de manera progresiva para facilitar la adaptación del equipo y la infraestructura.