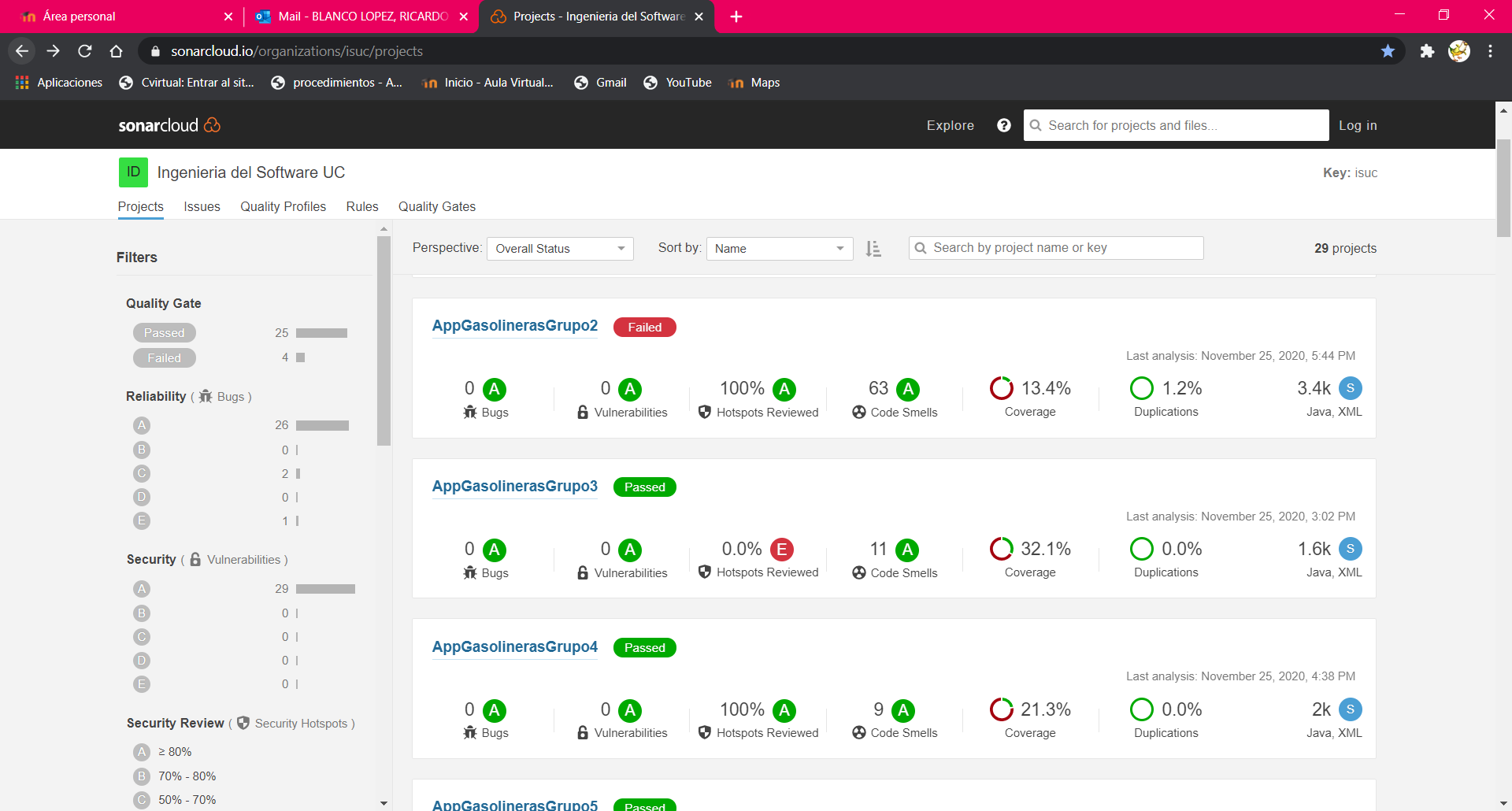
## **­­­ANÁLISIS 25 NOVIEMBRE 2020**

**CAPTURA**



**INCIDENCIAS**

El análisis pasa los criterios de calidad definidos por la empresa, siendo la deuda técnica de 2 horas, sin embargo, se han encontrado 9 vulnerabilidades de seguridad, las cuales ponen en riesgo la integridad de la aplicación.

**PLAN DE ACCIÓN**

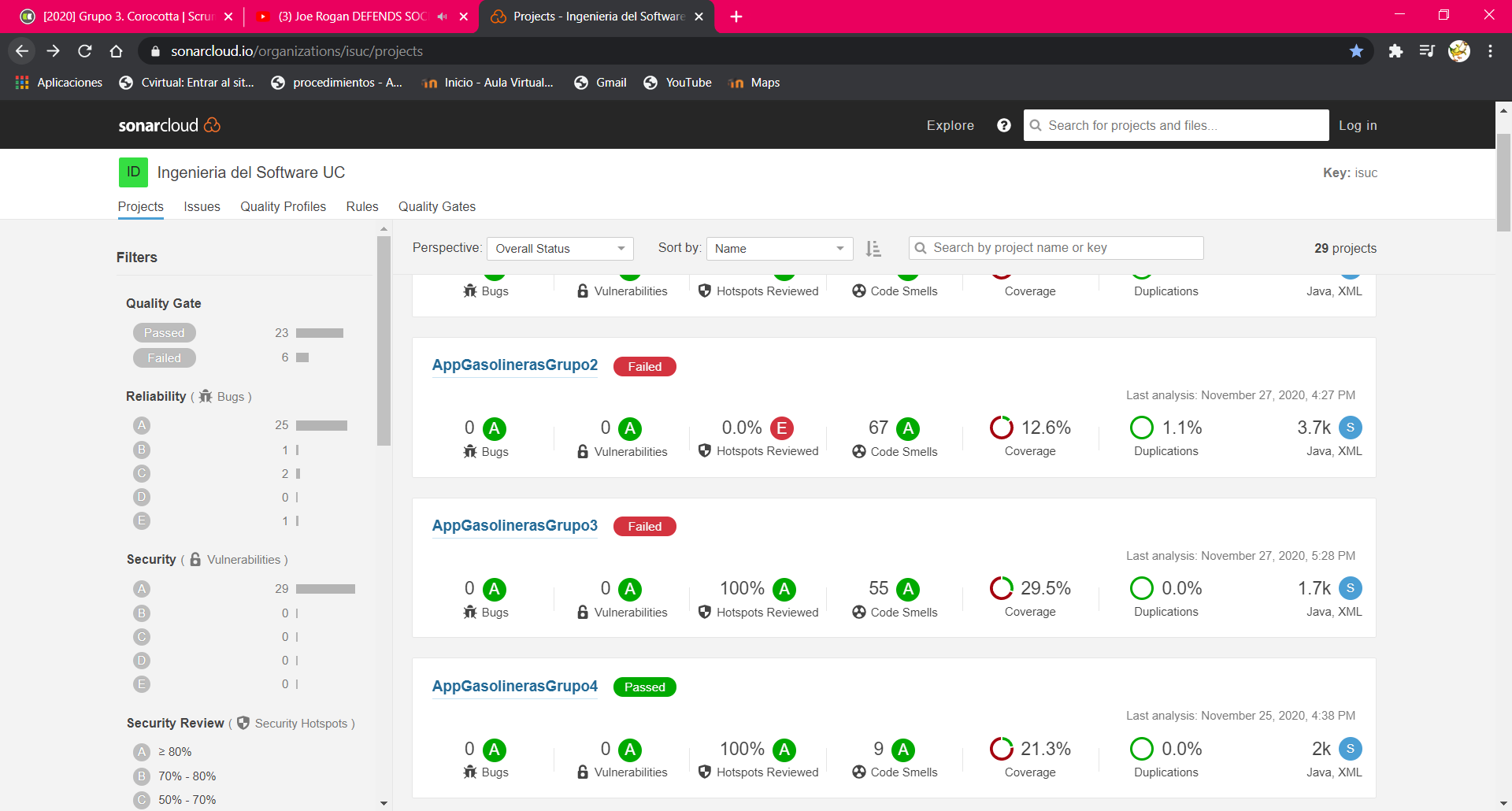
1. Arreglar los 9 security hotspots con severidad baja.

**COMENTARIOS**

* Con estas acciones a corregir, se restarían un total de 9 security hotspots, logrando pasar el review de los security hotspots.

## **­­­ANÁLISIS 27 NOVIEMBRE 2020**

**CAPTURA**



**INCIDENCIAS**

El análisis no pasa los criterios de calidad definidos por la empresa, siendo la deuda técnica de 4 horas y 40 minutos, dicha deuda técnica se ha provocado debido a los code smells del código.

**PLAN DE ACCIÓN**

1. Eliminar 3 code smells con severidad baja (variables no usadas).
2. Eliminar 8 code smells con severidad baja(catch vacios).

**COMENTARIOS**

Con estas acciones, se ha logrado que se cumplan los criterios de calidad, siendo la nueva deuda técnica menor a 4 horas y 10 minutos a 3 horas y 10 minutos.