



INGENIERIA DE SISTEMAS – SPTI 2021-1

LABORATORIO:

Aplicado Análisis de Riesgos

GERSON DAVID QUINTERO RODRIGUEZ

Autor:

Torres Segura Duck James Alexander

Jimmy Armando Chirivi Nivia

- Configuración de red de la máquina virtual donde se ejecuta Eramba.

```

maquina [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2228 bytes 158504 (158.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2228 bytes 158504 (158.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@eramba:/home/eramba# ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.55 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe92:5b53 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:92:5b:53 txqueuelen 1000 (Ethernet)
    RX packets 106 bytes 8824 (8.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 96 bytes 7094 (7.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2228 bytes 158504 (158.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2228 bytes 158504 (158.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@eramba:/home/eramba# ping www.google.com
PING www.google.com (142.250.78.68) 56(84) bytes of data.
64 bytes from bog02s16-in-f4.1e100.net (142.250.78.68): icmp_seq=1 ttl=118 time=92.8 ms
64 bytes from bog02s16-in-f4.1e100.net (142.250.78.68): icmp_seq=2 ttl=118 time=12.3 ms
^C
--- www.google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 12.336/52.604/92.872/40.268 ms
root@eramba:/home/eramba#

```

Ilustración 1: Configuración de red

- Verificación de la ip asignada y el acceso a Eramba desde la IP asignada.

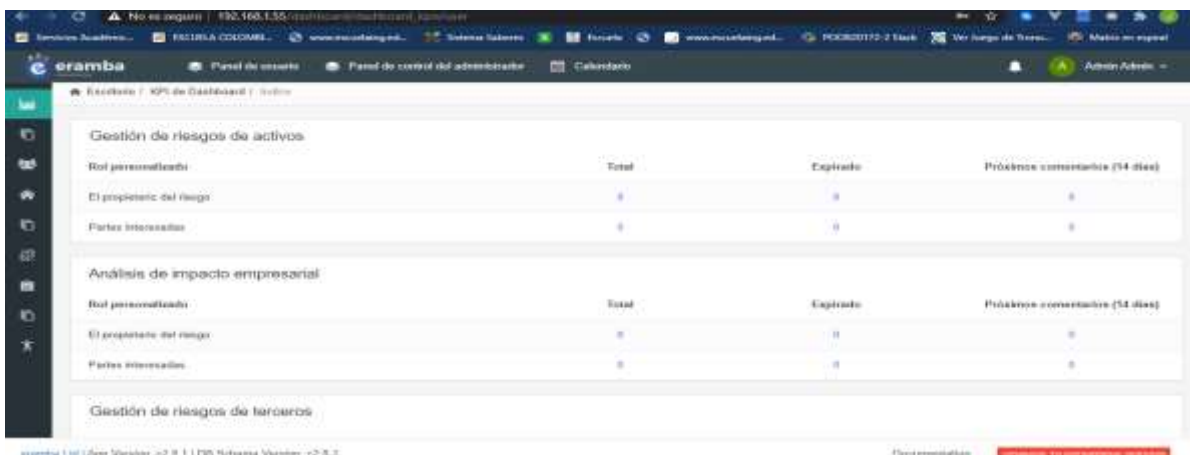


Ilustración 2: Verificación de ip

- Configuración y cargue de los paquetes de cumplimiento

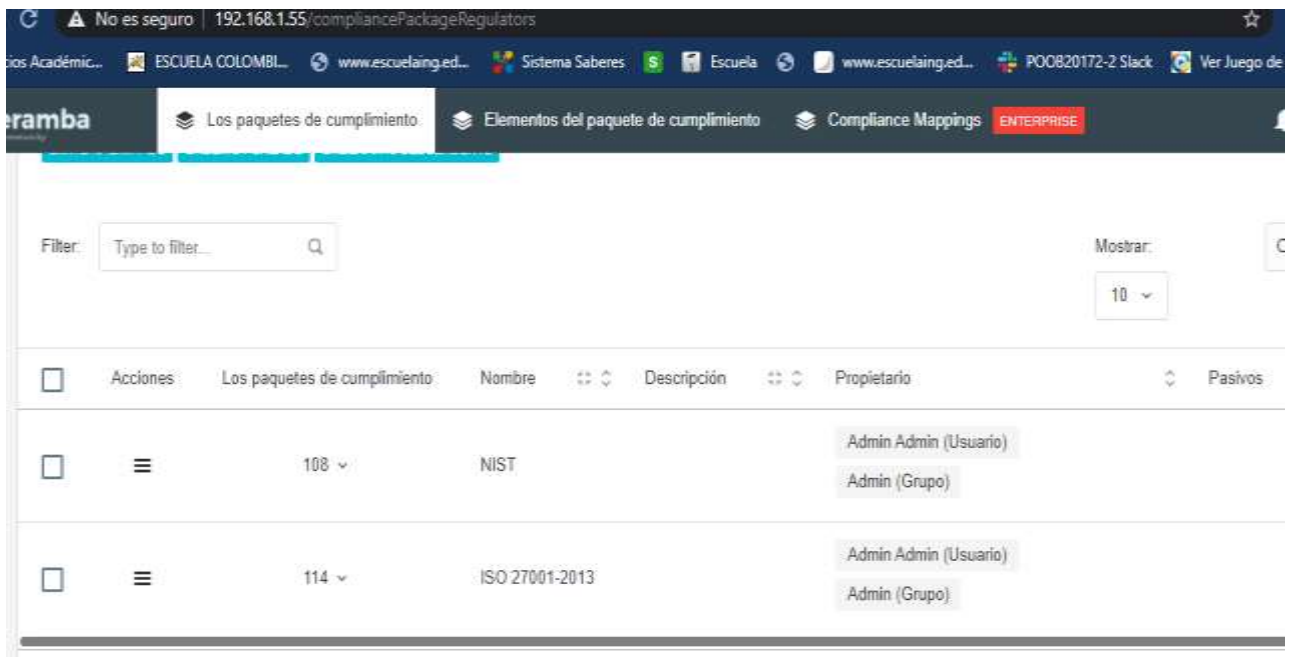


Ilustración 3: cargue de paquetes

- configuración de los activos de la organización

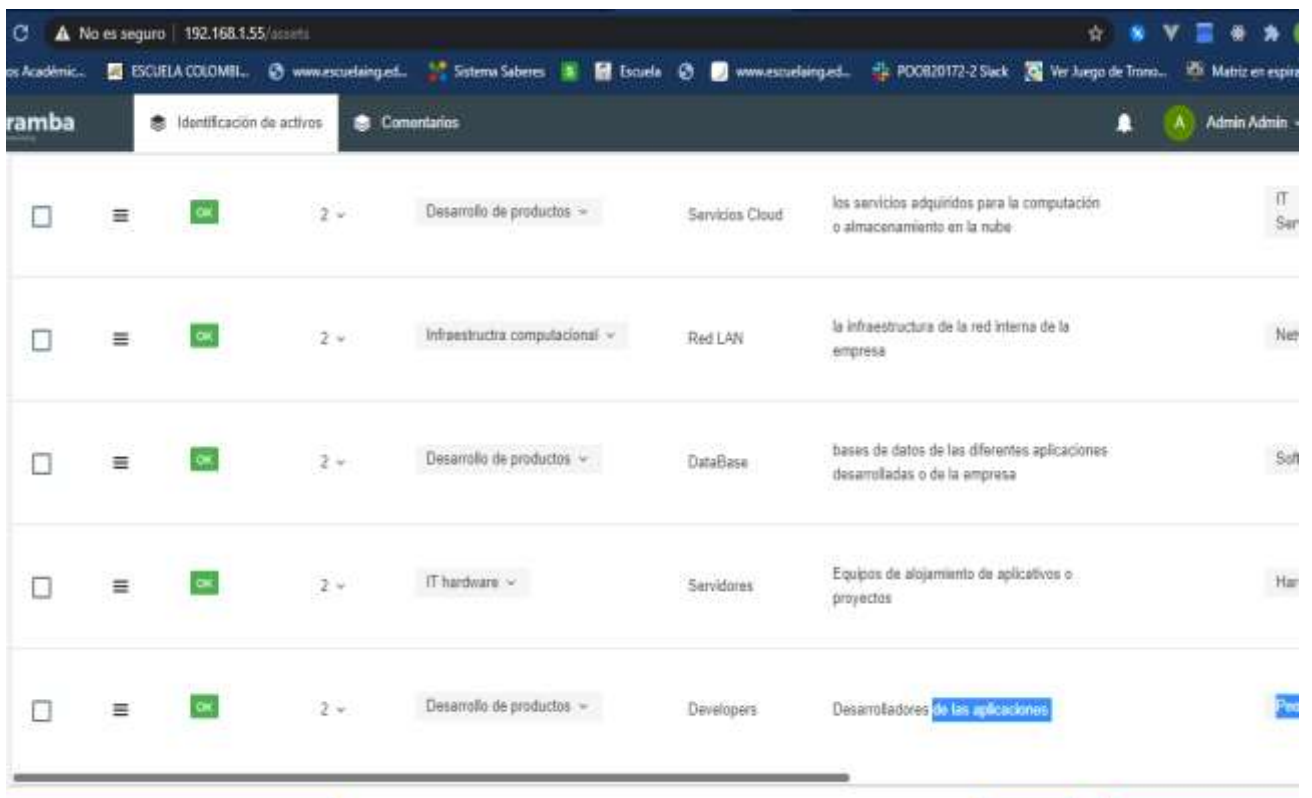


Ilustración 4: Configuración de los activos de la organización.

- Agregamos los controles internos de la organización en este caso al ser del sector TI.

| Estado | Icono | Control | 0 | 0 | 0 | Descripción |
|--------|-------|---|---|---|---|---|
| OK | | Servidor de archivos privados | 0 | 0 | 0 | Servidor de archivos privados |
| OK | | controles de archivo | 0 | 0 | 0 | controles de archivo |
| OK | | Backups | 0 | 0 | 0 | Backups |
| OK | | Cuarto de computación con protección especial ante terremotos | 0 | 0 | 0 | Cuarto de computación con protección especial ante terremotos |
| OK | | Auditoría de cuentas y permisos de usuario | 0 | 0 | 0 | Auditoría de cuentas y permisos de usuario |
| OK | | Backups, herramientas de versionamientos | 0 | 0 | 0 | Backups, herramientas de versionamientos |
| OK | | Firewalls, herramientas y personal de control en ciberseguridad y Backups | 0 | 0 | 0 | Firewalls, herramientas y personal de control en ciberseguridad y Backups |
| OK | | Sistema de control temprano de incendios | 0 | 0 | 0 | Sistema de control temprano de incendios |

Ilustración 5: Controles internos

Agregamos planes de continuidad de negocio para evitar algún caso de pérdida del flujo del trabajo de la organización.

| Estado | Tareas de continuidad del negocio | Auditorías del plan de continuidad del negocio | Título | Objetivo |
|--------|-----------------------------------|--|---------------------------|---|
| OK | 0 | 0 | BPC Continuidad comercial | Mantener su negocio en funciones es una preocupación clave una vez se ha atendido los asuntos de seguridad. Los planes deben contar con la administración y un proceso lógico para continuar o reanudar y recuperar las funciones empresariales esenciales interrumpidas. Esto debe incluir apoyo coordinado entre las sedes corporativas y los lugares de trabajo locales. |
| OK | 0 | 0 | BPC Sismos | Manejo de crisis. Acción rápida y eficientemente para implementar su plan de manejo de crisis y al personal para comprender proactivamente los posibles impactos a las personas, la propiedad y las operaciones, y tome decisiones sobre políticas/estrategias para abordar y manejar esos impactos. |
| OK | 0 | 0 | BPC CiberAtaques | es importante identificar los activos de información más valiosos de la organización, las conocidas joyas de la corona que deben ser custodiadas, así como aquella información personal que está bajo la custodia de la organización (ya sea de empleados, proveedores, clientes, etc.) y que por ley debe ser protegida. |

Ilustración 6: Planes de continuidad

Creamos una política de tratamientos de datos para la organización.

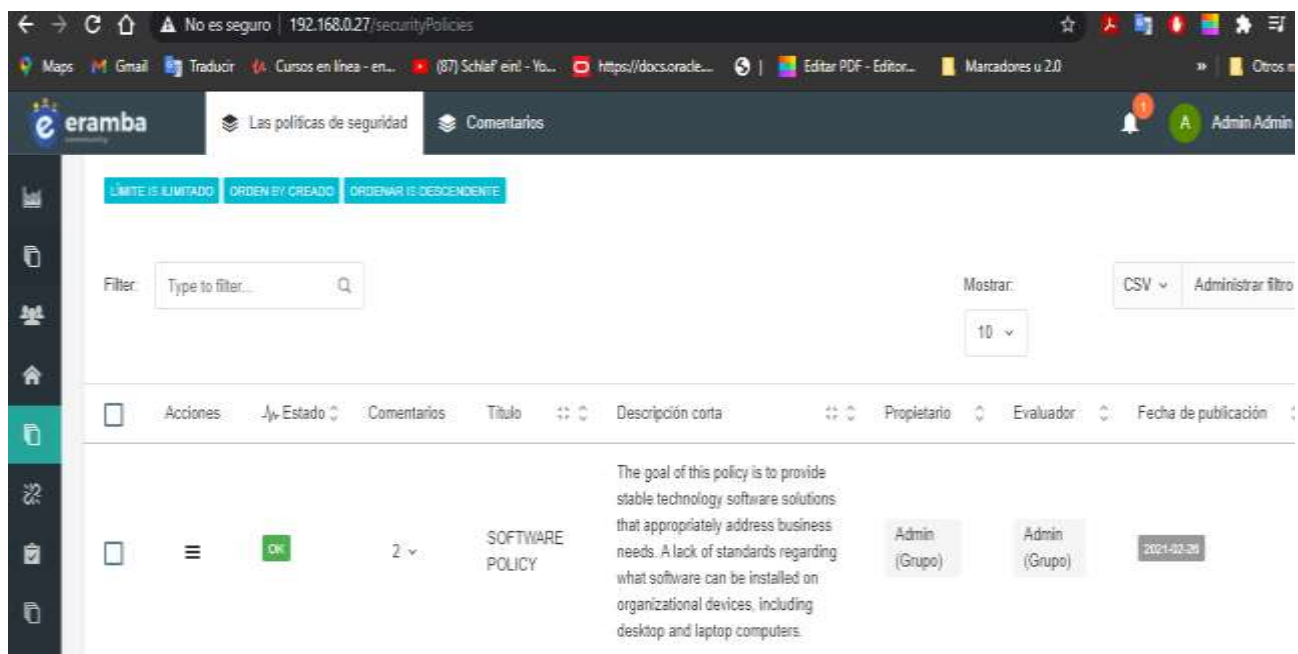


Ilustración 7: políticas

Añadimos los riesgos que contiene la organización y su posterior plan, políticas puntaje.

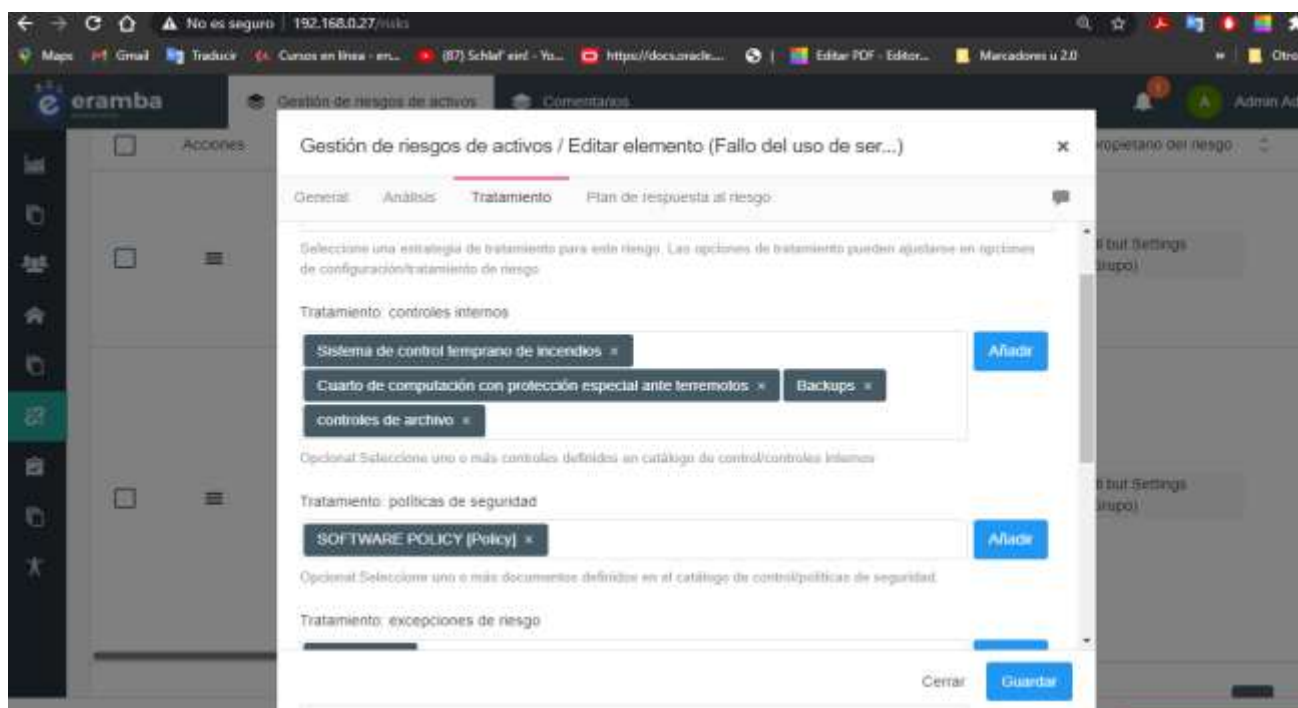


Ilustración 8: riesgos

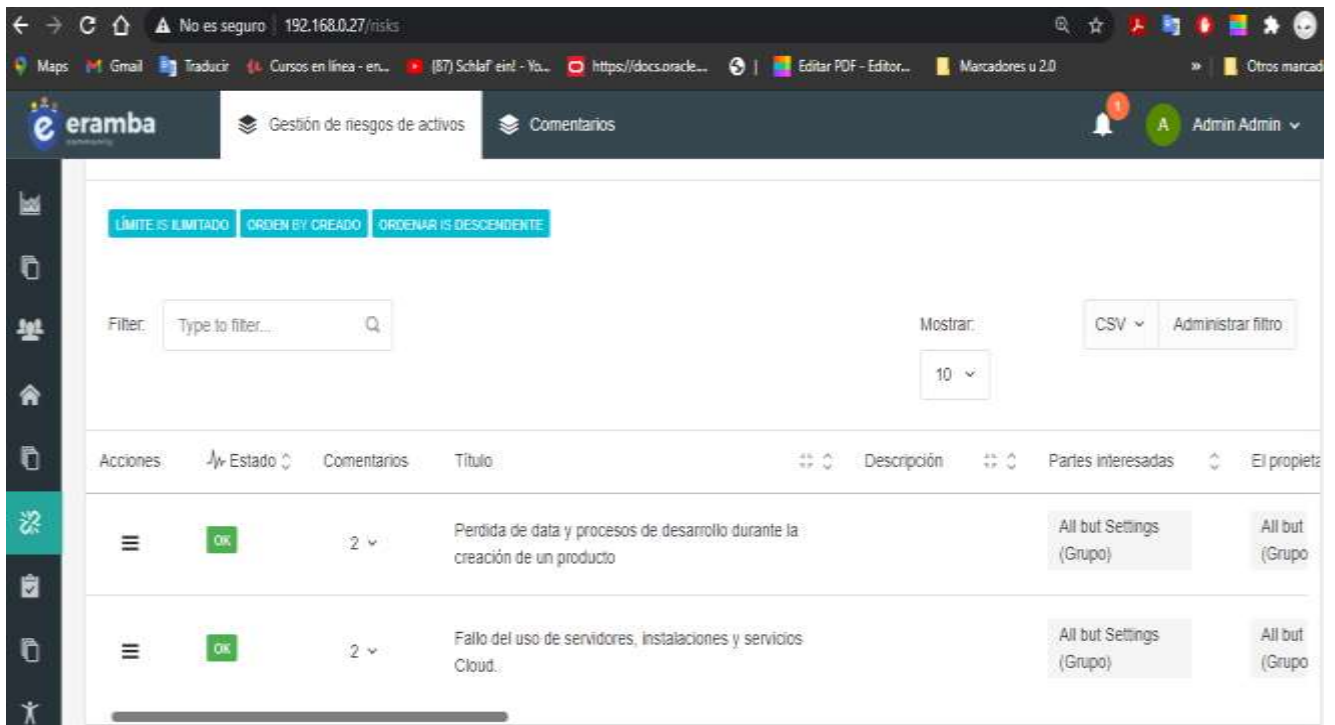


Ilustración 9: agregando riesgos

Colocamos su clasificación de riesgo y nuestros riesgos pasar o sobresaltaran las alarmas de análisis.

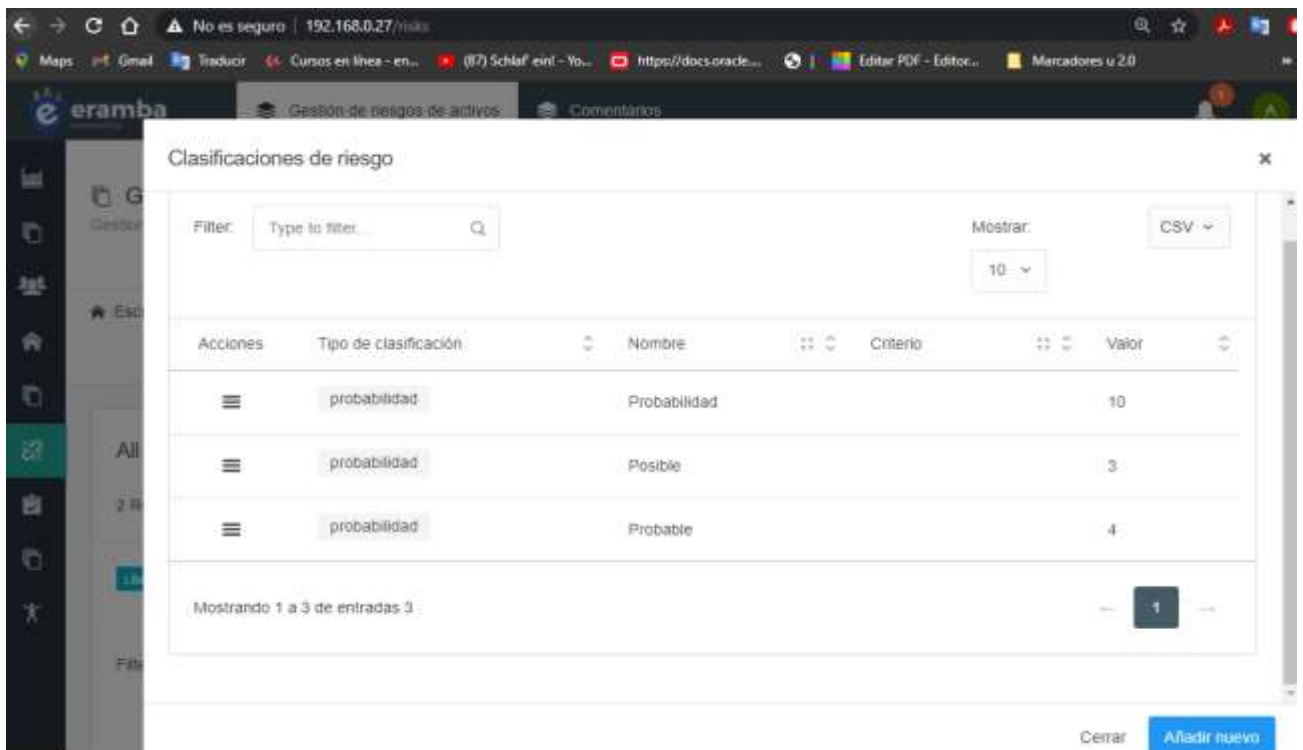


Ilustración 10: creando clasificación

| Acciones | Estado | Comentarios | Título | Descripción | Partes interesadas |
|----------|------------------------|-------------|---|-------------|--------------------------|
| | OK | 2 | Pérdida de data y procesos de desarrollo durante la creación de un producto | | All but Settings (Grupo) |
| | POR ENCIMA DEL APETITO | 2 | Fallo del uso de servidores, instalaciones y servicios Cloud. | | All but Settings (Grupo) |

Ilustración 11: Resultado

| Por encima del apetito | Revisión caducada | Clasificación de riesgo de análisis | Risk Analysis Score | Activo |
|------------------------|-------------------|-------------------------------------|---------------------|--|
| NO | NO | probabilidad (Posible) | 3 | Developers, Servicios Cloud |
| SI | NO | probabilidad (Probable) | 4 | Servidores, DataBase, Red LAN, Servicios Cloud |

Ilustración 12: Resultado

Agregamos excepciones a estos riesgos los cuales son cuando se practican simulacros de ataque, etc.

| Acciones | Estado | Título | XXX | Vencimiento | Etiquetas | Fecha de cierre | Estado | Riesgo de activos |
|--------------------------|--------|-----------|-----|-------------|-----------|-----------------|---------|--|
| <input type="checkbox"/> | | Simulacro | | 2021-11-10 | | 2021-02-26 | Cerrado | Fallo del uso de servicio Pérdida de data y proce |

Ilustración 13: Excepciones