Implementación de políticas de seguridad de la Información mediante una solución de Prevención de perdida de datos (DLP) para el ESPE-CERT

Autor: Kevin Quiroga

Director: Ing. Fuertes Díaz, Walter Marcelo, PHD

AGENDA

1.- ANTECEDENTES Y PROBLEMA

2.-OBJETIVOS

3.- METODOLOGÍA, ANÁLISIS Y DESARROLLO

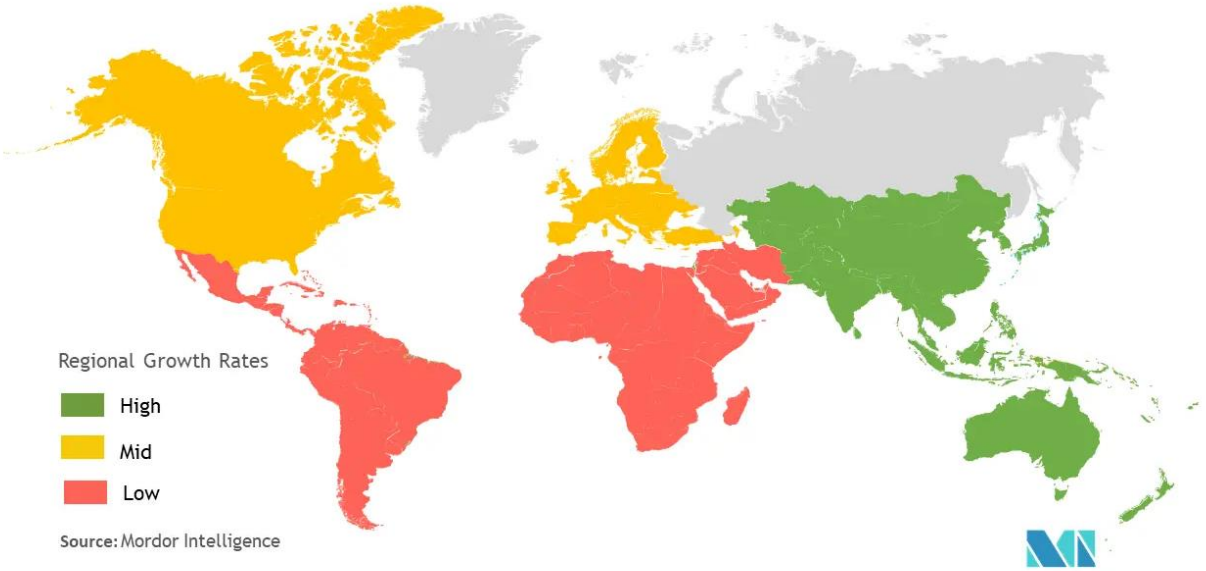
4.- RESULTADOS

5.- CONCLUSIONES Y RECOMENDACIONES

16 de Septiembre del 2019

- La empresa Novaestrat creada en el 2017 por dos exfuncionarios que trabajaron en la Senplades, Secom y en el Banco Nacional de Fomento. Tenían una base de datos de 20,8 millones de ecuatorianos.

Mercado mundial de prevención de pérdida de datos (DLP) 2021-2026



Fuente: https://www.mordorintelligence.com/es/industry-reports/data-loss-prevention-market

- La pérdida de información confidencial, los datos son considerados como un activo muy valioso, el cual está propenso a ser filtrados por medio de correos electrónicos, mensajería instantánea, impresión o copia en dispositivos de almacenamiento;
- No tener la trazabilidad de la información en reposo y en transito;
- No llevar el registro de usuarios dentro de la red;
- No análizar el comportamiento de los usuarios con la información que poseen.

Objetivo General

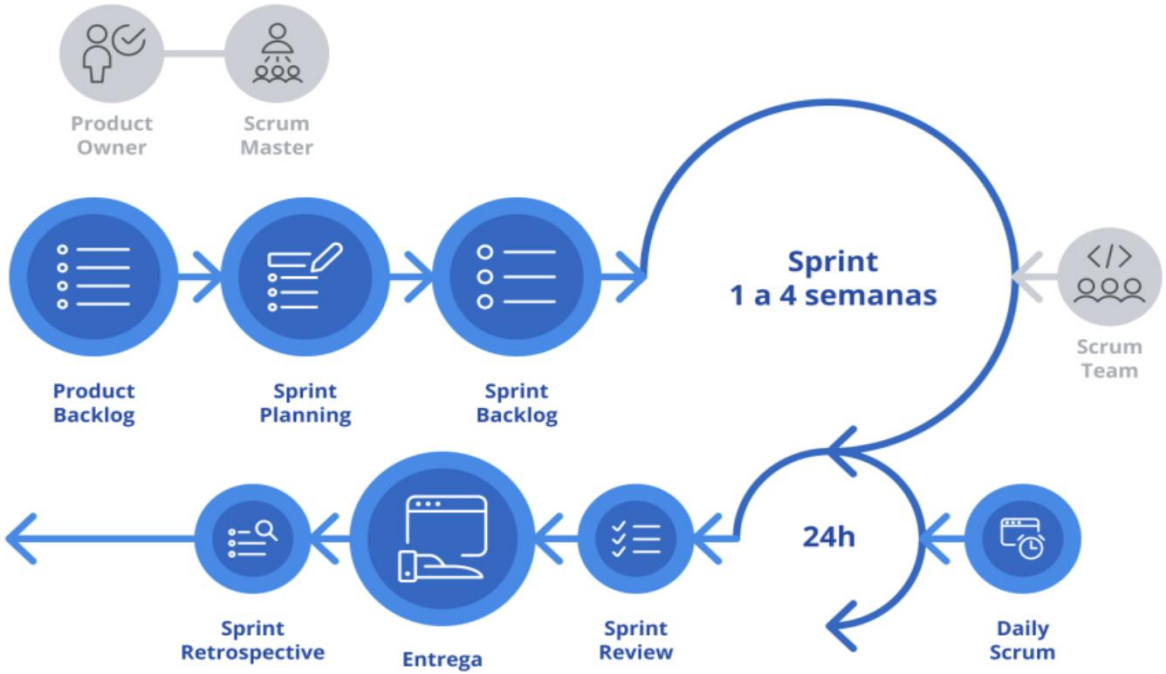
Implementar una solución DLP como una herramienta de seguridad, prevención y protección de la información mediante políticas y reglas dirigido al Cert Académico de la ESPE para su uso y administración como servicio.

Objetivos Específicos

1. Determinar políticas de seguridad de la información como monitoreo para que el Cert Académico ESPE brinde el servicio mediante un estudio de las tecnologías que ayude a la prevención de fuga de información.
2. Comparar las diversas herramientas de DLP aplicadas a la protección de pérdida de información para la implementación como servicio en el Cert Académico ESPE.
3. Implementar el artefacto de software DLP, para la administración y funcionamiento en el Cert Académico ESPE.
4. Elaborar una prueba de concepto, en donde se evidencie la implementación de políticas de seguridad.
5. Realizar validaciones que permitan identificar conectividad y aplicación de políticas de seguridad, mediante el registro en la consola de administración.

SCRUM

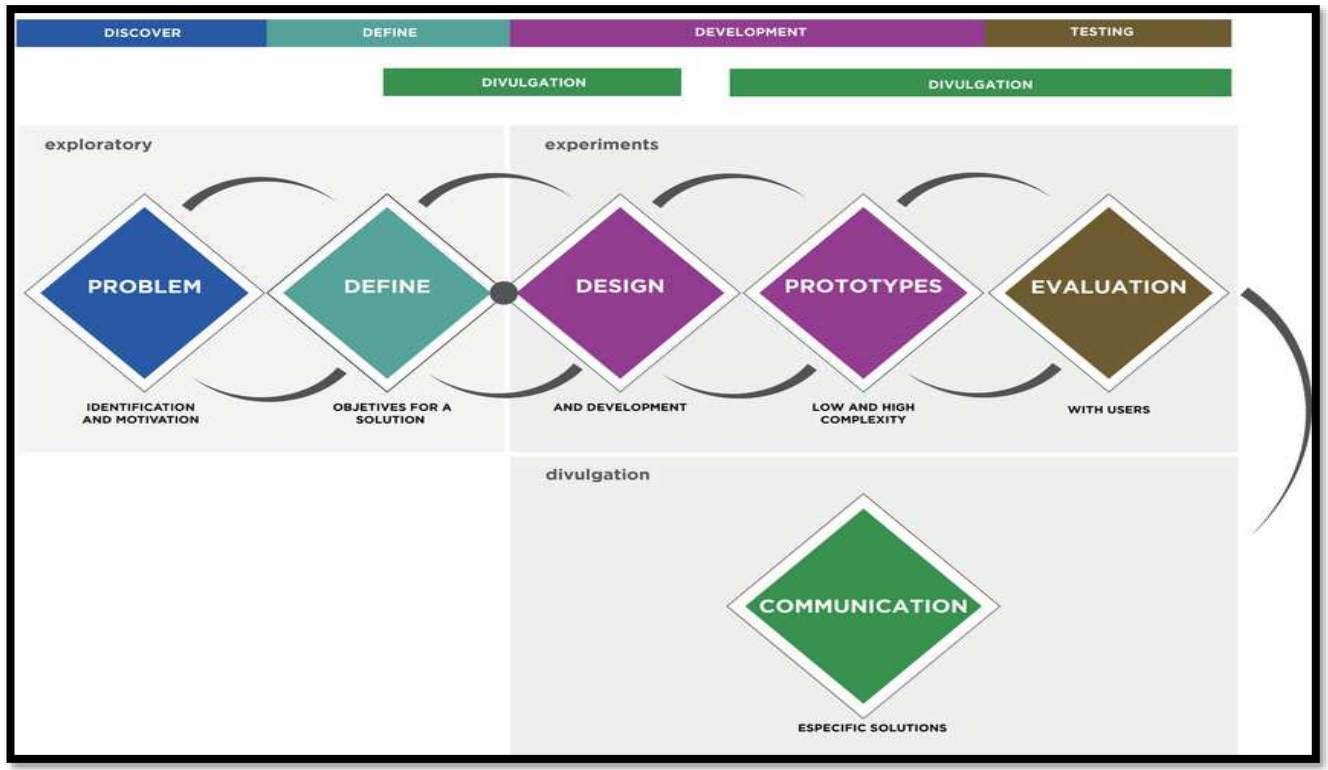
Ciclo Scrum



Metodología Scrum (Hevner, 2019).

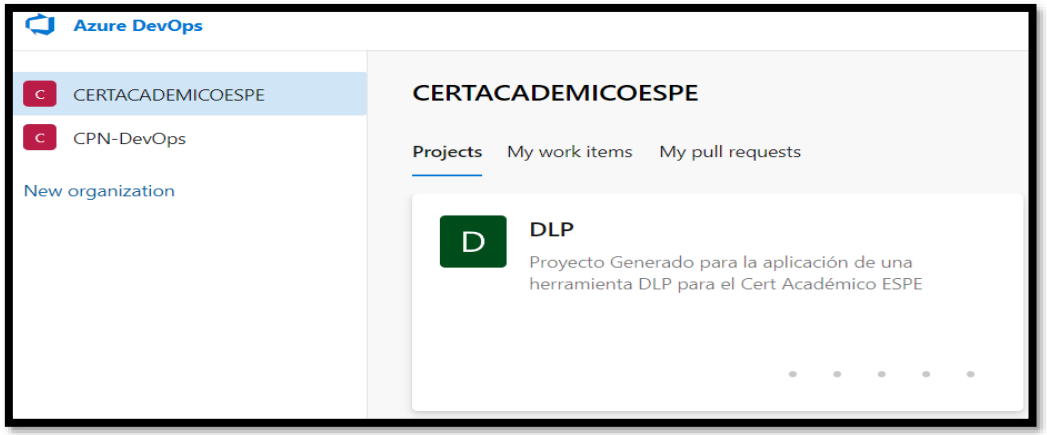
Design Science

Metodología Design Science propuesta por Hevner

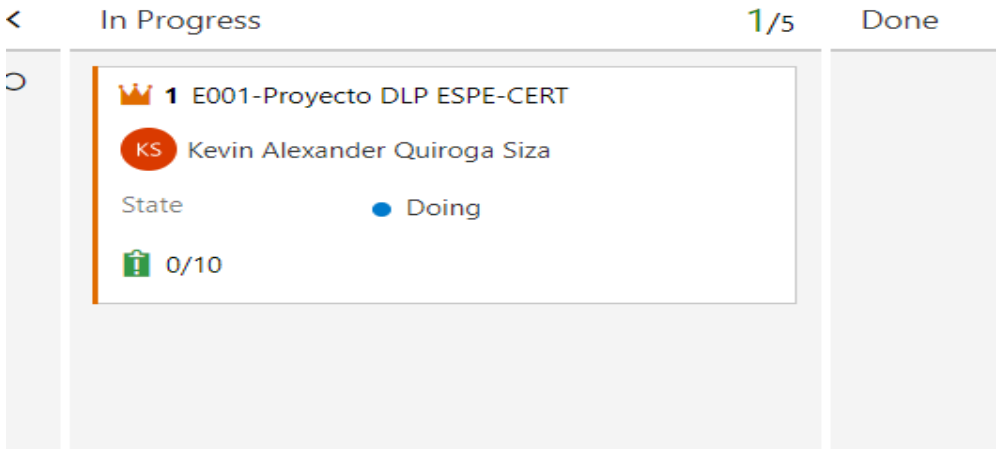


Metodología Design Science (Hevner, 2007).

Creación de Artefactos Scrum en AzureDevOps

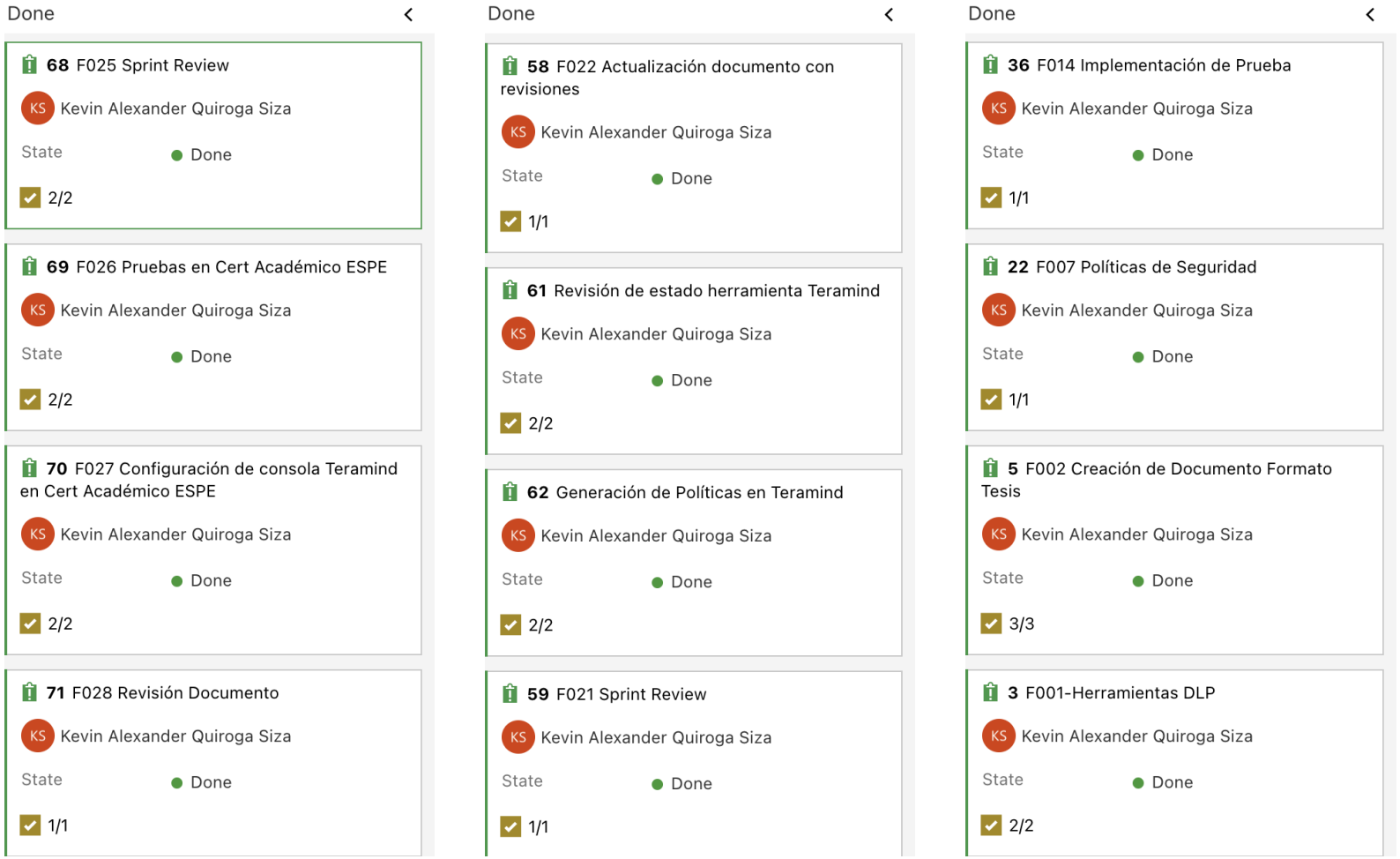


Proyecto



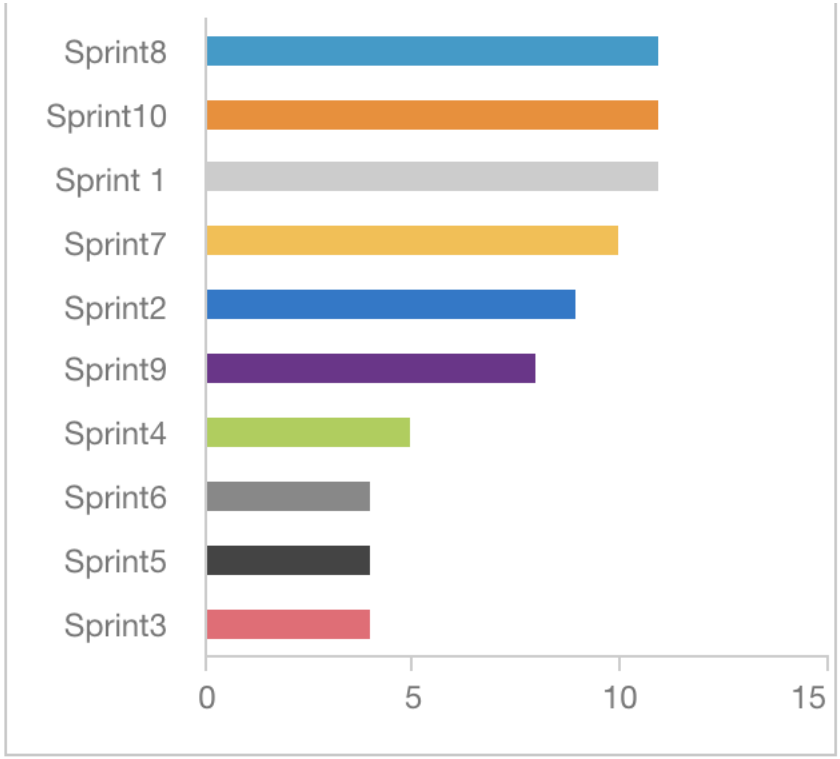
Historia Épica

Creación de Artefactos en AzureDevOps



Creación de Artefactos en AzureDevOps

Diagrama de barras Historias por Sprint



Cantidad de historias trabajadas por sprint

- **Sprints:** para el desarrollo se dividió en 10 Sprints con una duración de 15 días

Creación de Artefactos en AzureDevOps

Sprint1 10/1/2022- 10/15/2022

Order	ID	Title	Assigned To	State
1	10	F003 Revisión de perfil de Tesis	Kevin Alexand...	Doing
	11	Validación de Fuentes Bibliográficas	Kevin Alexand...	Done
	12	Comprobación de la Redacción	Kevin Alexand...	Done
2	3	F001-Herramientas DLP	Kevin Alexand...	Doing
	4	Análisis de la Herramientas DLP	Kevin Alexand...	Done
	8	Investigación sobre temas DLP	Kevin Alexand...	Done
3	5	F002 Creación de Documento Formato Tesis	Kevin Alexand...	Doing
	6	Validación Formato Tesis Biblioteca	Kevin Alexand...	Done
	7	Actualización de Documento	Kevin Alexand...	Done
	9	Validación formato de referencias bibliográficas	Kevin Alexand...	Done

Sprint2 10/16/2022- 10/31/2022

Order	ID	Title	Assigned To	State
1	13	F004 Análisis de Herramientas DLP Parte2	Kevin Alexand...	Doing
	20	Validación de herramientas disponibles	Kevin Alexand...	Done
	21	Validación de integraciones	Kevin Alexand...	Done
2	14	F005 Fuentes Bibliográficas	Kevin Alexand...	Doing
	18	Revisión bibliográfica acerca de soluciones de seguridad ...	Kevin Alexand...	Done
	19	Creación de Referencias en formato APA	Kevin Alexand...	Done
3	15	F006 Análisis de Infraestructura para DLP	Kevin Alexand...	Doing
	16	Busqueda de información despliegues DLP	Kevin Alexand...	Done
	17	Validación de integraciones	Kevin Alexand...	Done

Sprint3 11/1/2022- 11/15/2022

Order	ID	Title	Assigned To	State
1	23	F008 Levantamiento de Información para DLP	Kevin Alexand...	Doing
	24	Investigación de documentación	Kevin Alexand...	Done
2	22	F007 Políticas de Seguridad	Kevin Alexand...	Doing
	25	Investigación sobre políticas de seguridad	Kevin Alexand...	Done

Sprint4 11/16/2022- 11/30/2022

Order	ID	Title	Assigned To	State
1	26	F009 Elección herramienta DLP	Kevin Alexand...	Doing
	29	Revisión Bibliografica	Kevin Alexand...	Done
	30	Validación de Herramienta Teramind DLP	Kevin Alexand...	Done
2	27	F010 Documentación Tesis	Kevin Alexand...	Doing
	28	Actualización de marco metodológico	Kevin Alexand...	Done

Creación de Artefactos en AzureDevOps

Sprint5 12/1/2022- 12/15/2022

Order	ID	Title	Assigned To	State
1	31	F011 Busqueda Bibliográfica	Kevin Alexand...	Doing
	34	Busqueda de información sobre herramienta Dlp y Terami...	Kevin Alexand...	Done
2	32	F012 Analisis Teramind DLP	Kevin Alexand...	Doing
	33	Validación de documentación Teramind	Kevin Alexand...	Done

Sprint6 12/16/2022- 12/31/2022

Order	ID	Title	Assigned To	State
1	36	F014 Implementación de Prueba	Kevin Alexand...	Doing
	37	Validación de tipos de despliegue Teramind DLP	Kevin Alexand...	Done
2	35	F013 Actualización documento con apartado de Desarr...	Kevin Alexand...	Doing
	38	Insertar imagenes de prueba y Desarrollo de el despliegu...	Kevin Alexand...	Done

Sprint7 1/2/2023- 1/15/2023

Order	ID	Title	Assigned To	State
1	40	F016 Pruebas de despliegue en Ambiente Controlado	Kevin Alexand...	Doing
	43	Creación de ambiente controlado Máquina Virtual	Kevin Alexand...	Done
	44	Despliegue de teramind dlp en la nube	Kevin Alexand...	Done
	46	Configuración de Usuario y acceso a la consola	Kevin Alexand...	Done
	47	Instalación de agente en maquina de prueba	Kevin Alexand...	Done
2	41	F017 Actualización de documento Tesis	Kevin Alexand...	Doing
	42	Actualización de documento con pruebas en ambiente co...	Kevin Alexand...	Done
	48	Actualización de evidencia para prueba	Kevin Alexand...	Done
3	39	F015 Validación de solución Teramind DLP stakeholder	Kevin Alexand...	Doing
	45	Reunión validación Ing Mario Ron informante	Kevin Alexand...	Done

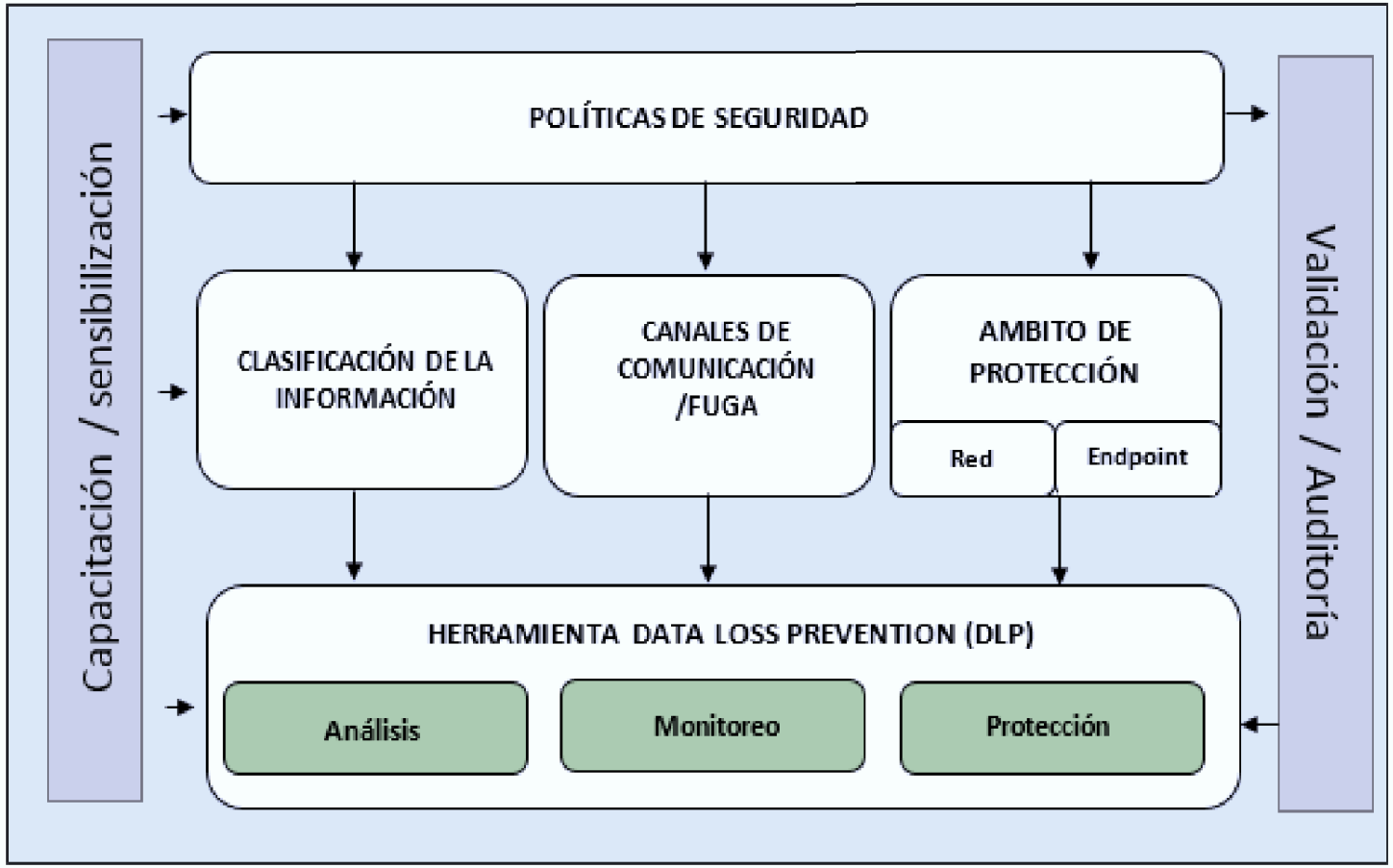
Sprint8 1/16/2023- 1/31/2023

Order	ID	Title	Assigned To	State
1	59	F021 Sprint Review	Kevin Alexand...	Done
	60	Reunión Virtual Ing Walter Fuertes	Kevin Alexand...	Done
2	51	F020 Documentación Pruebas	Kevin Alexand...	Done
	52	Toma de capturas y evidencia de pruebas	Kevin Alexand...	Done
	57	Actualización de documento con nuevas capturas y refere...	Kevin Alexand...	Done
3	49	F018 Análisis de Conectividad Teramind	Kevin Alexand...	Done
	53	Pruebas de conexión de agente con la consola Teramind	Kevin Alexand...	Done
	54	Validación de acceso usuarios nuevos a consola	Kevin Alexand...	Done
4	50	F019 Verificación de actividad en consola TeramindDLP	Kevin Alexand...	Done
	55	Validación de registro de máquina en consola Teramind	Kevin Alexand...	Done
	56	Validación de estado de máquina	Kevin Alexand...	Done

Comparativa de herramientas DLP

Característica	McAfee DLP	Symantec DLP	Trend Micro DLP	Forcepoint DLP	Teramind DLP	OpenDLP
Complejidad en la configuración de políticas	Fácil	Media	Media	Media	Fácil	Difícil
Personalización de alertas	Sí	Sí	Sí	Sí	Sí	No
Integración con sistemas de gestión de incidentes	Sí	Sí	Sí	Sí	Sí	No
Despliegue en la nube	Sí	Sí	Sí	Sí	Sí	No
Arquitectura basada en la nube	No	No	No	Sí	Sí	No
Capacidad de monitoreo de nube	No	No	No	No	Sí	No
Capacidad de monitoreo de aplicaciones	Sí	Sí	No	No	Sí	Sí

Modelo de seguridad tomando en cuenta el estándar ISO27001



Políticas de Seguridad	ISO27001
Canales, Clasificación, Ámbitos	ISACA
DLP	Teramind

Arquitectura de despliegue en Azure

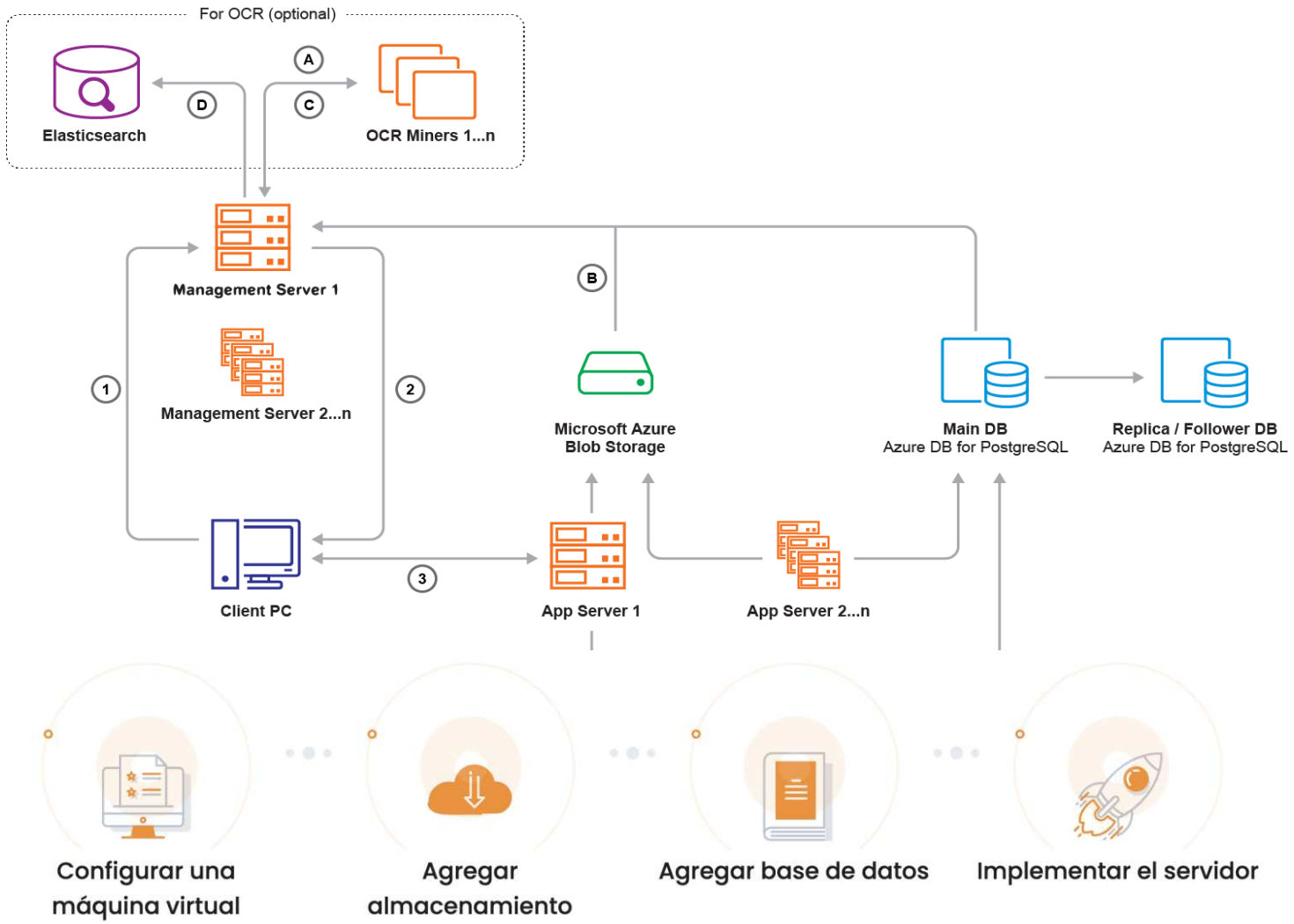
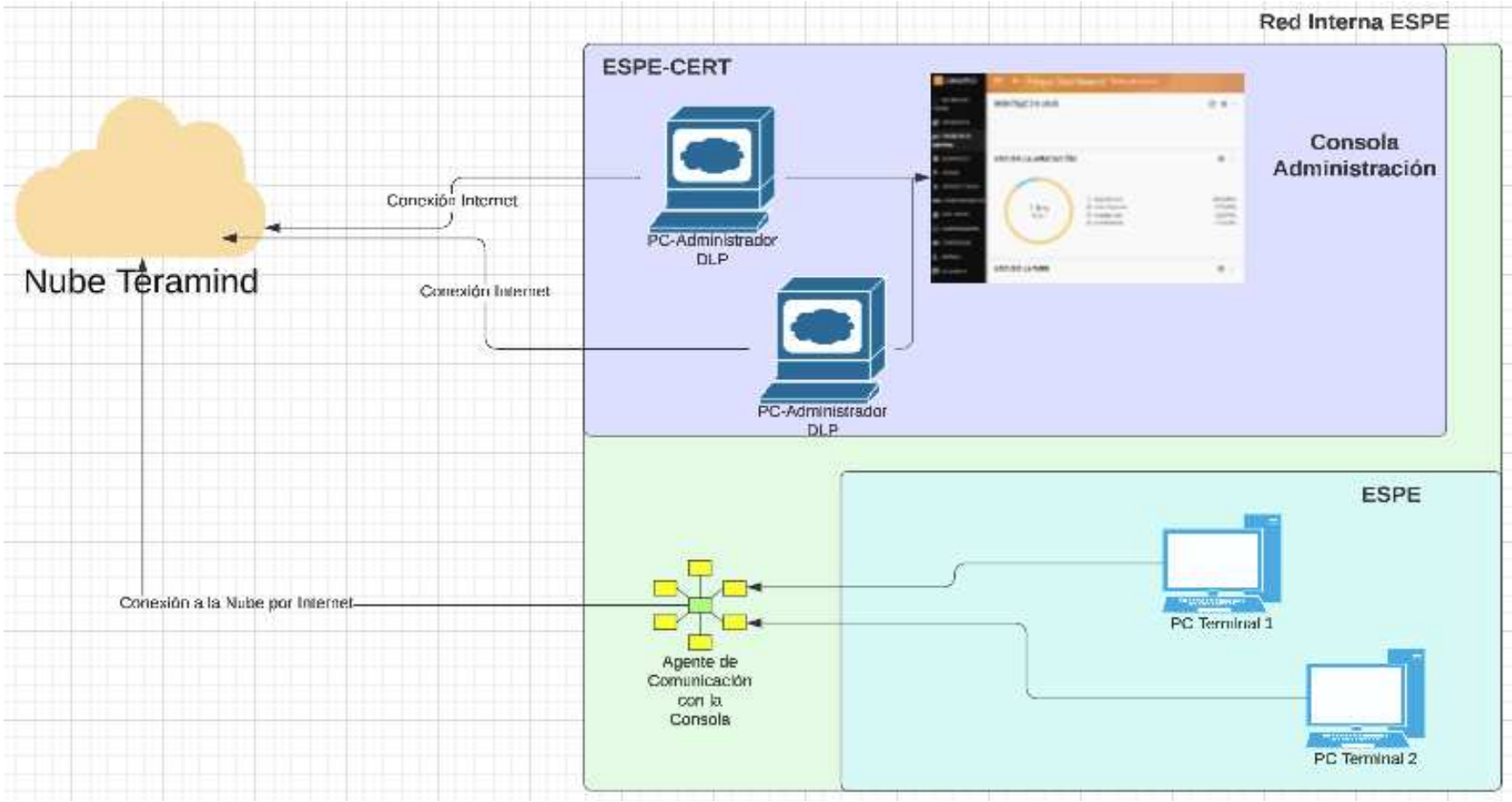
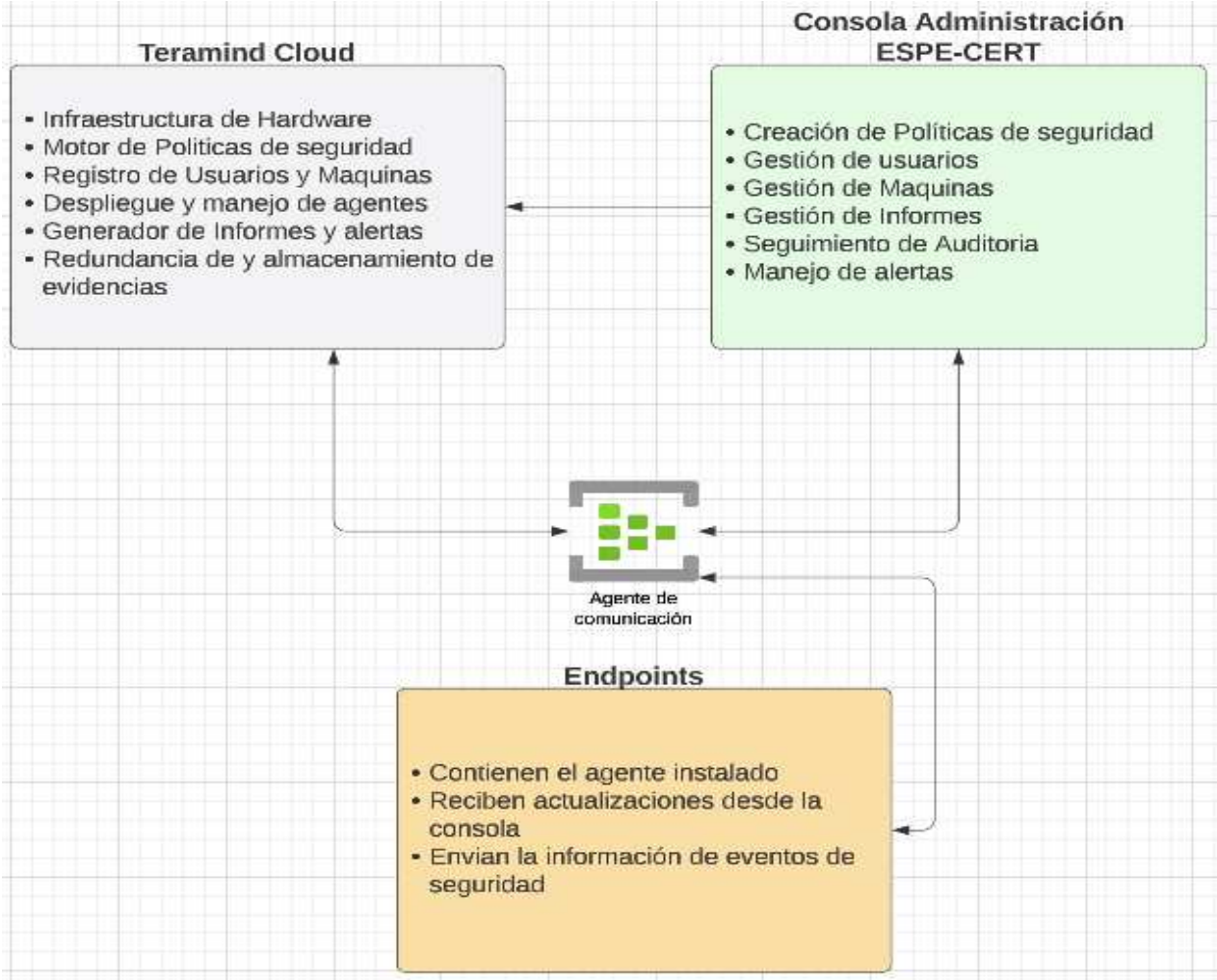


Diagrama de Comunicación

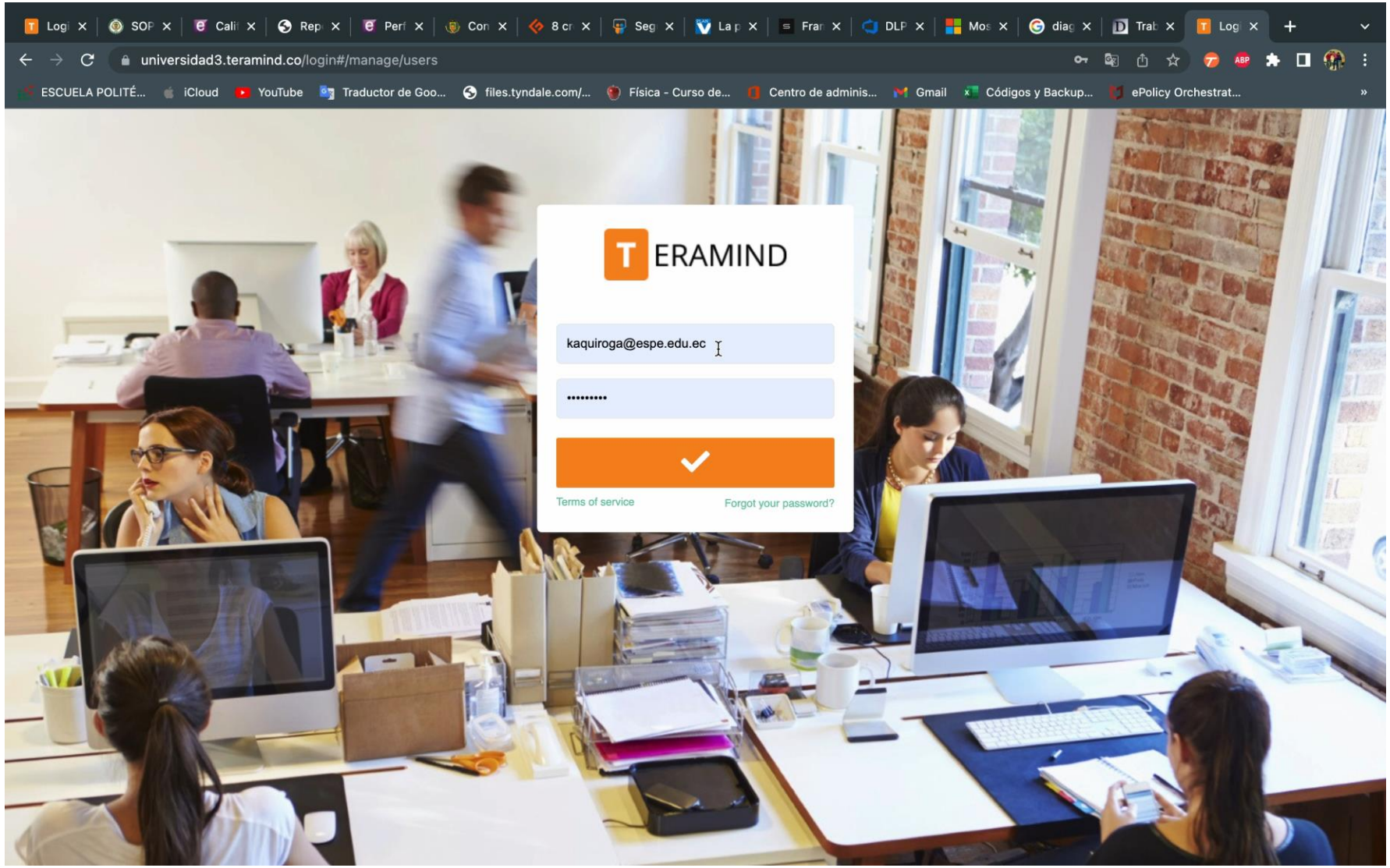


Descripción de la estructura



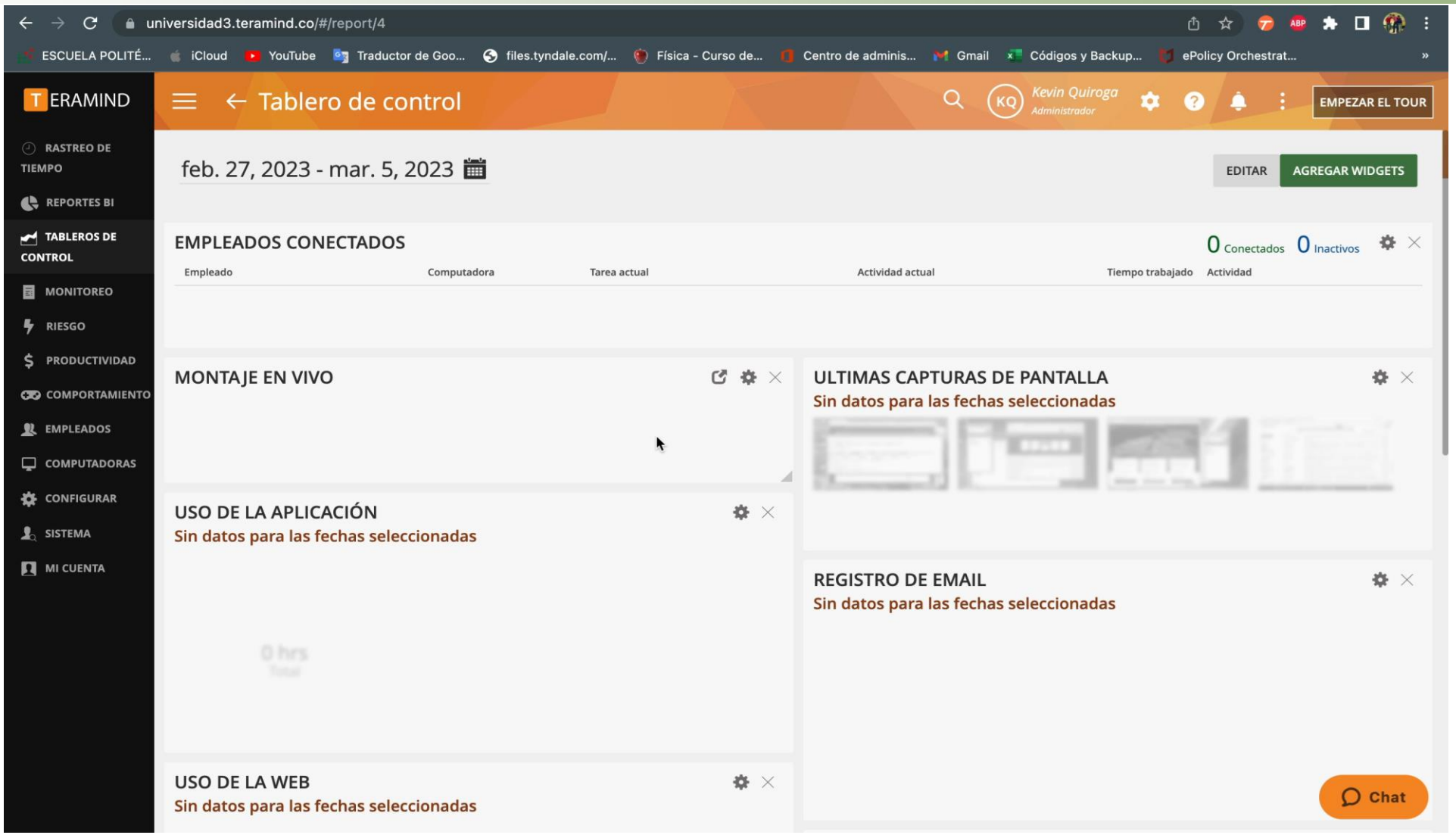
03. Demo consola Administración

Inicio de Sesión en Consola



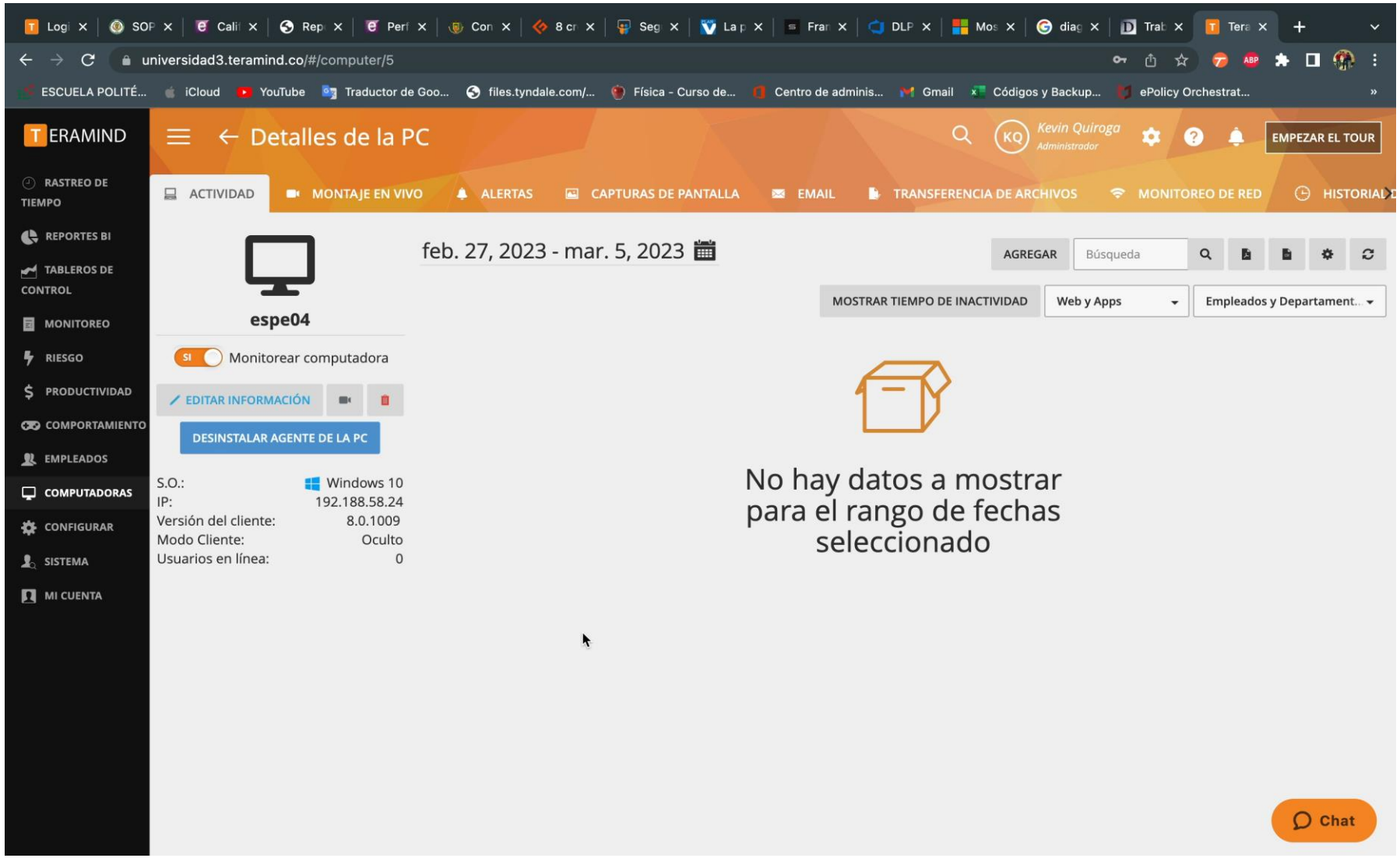
03. Demo consola Administración

Registro de Usuarios y Máquinas



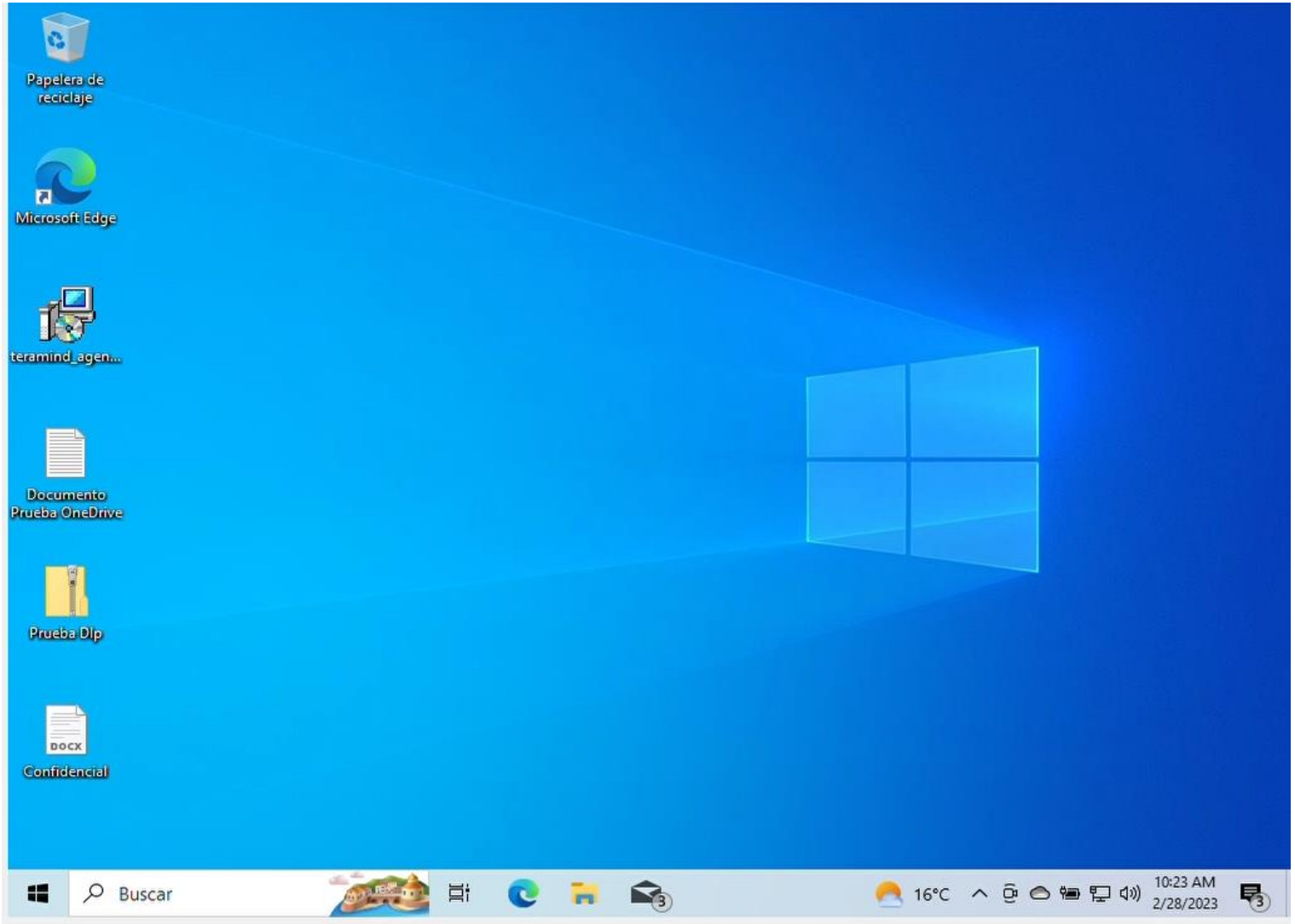
03. Demo consola Administración

Políticas y reglas de seguridad



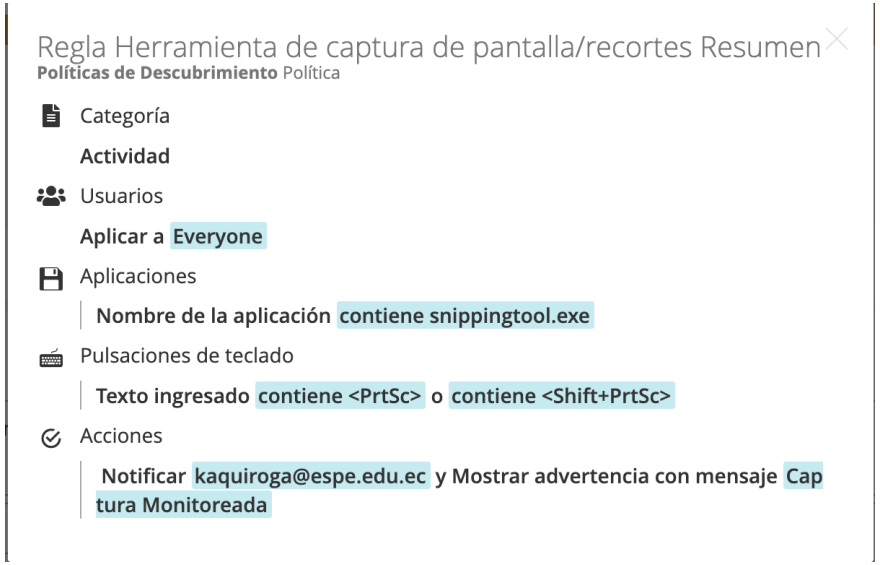
03. **Demo alerta usuario**

Alerta Máquina Final

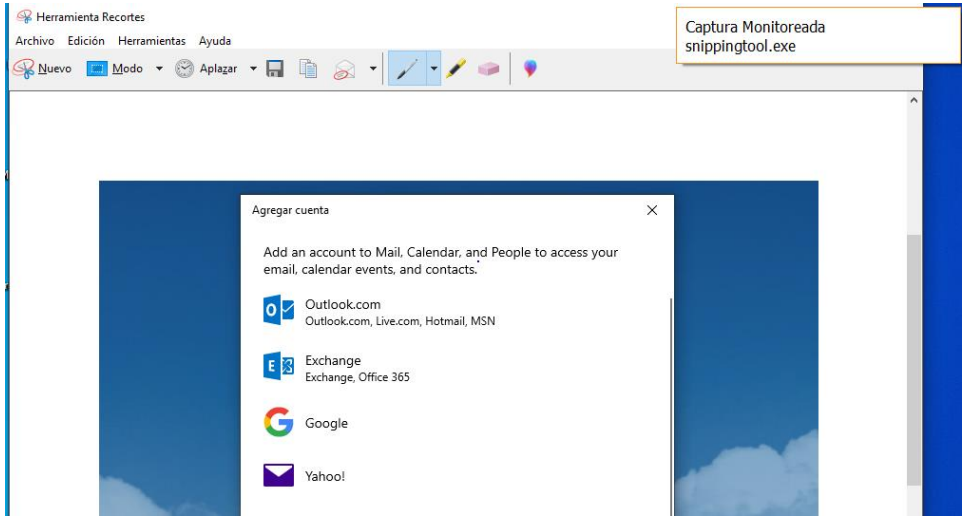


Consola Administración Políticas

Agente de Conexión



Descripción de Regla



Alerta Usuario

03. **Política y reglas de Monitoreo**

Políticas de Descubrimiento ^ 6 reglas Everyone SI

Verificación envio a Correos Externo Alerta cuando los usuarios envian correos a destinos diferentes @espe.edu.ec	Categoría de regla: Actividad	SI
Validación cuerpo de correo Alerta cuendo el cuerpo del correo contiene la palabra confidencial	Categoría de regla: Actividad	SI
Documento con Marca Confidencial Alerta cuando se comparte un archivo con marca Confidencial	Categoría de regla: Compartir contenido	SI
Herramienta de captura de pantalla/recortes El usuario tomó una captura de pantalla con una combinación de teclas de acceso rápido o lanzó la herramienta de recorte	Categoría de regla: Actividad	SI
Subir archivos a la nube Notificar cuando los usuarios cargan archivos en Google Drive, OneDrive, Box o DropBox	Categoría de regla: Actividad	SI
Guardar un archivo en un medio extraíble Alerta cuando los usuarios guardan archivos en USB u otros medios externos	Categoría de regla: Actividad	SI

04. Instalación de agente

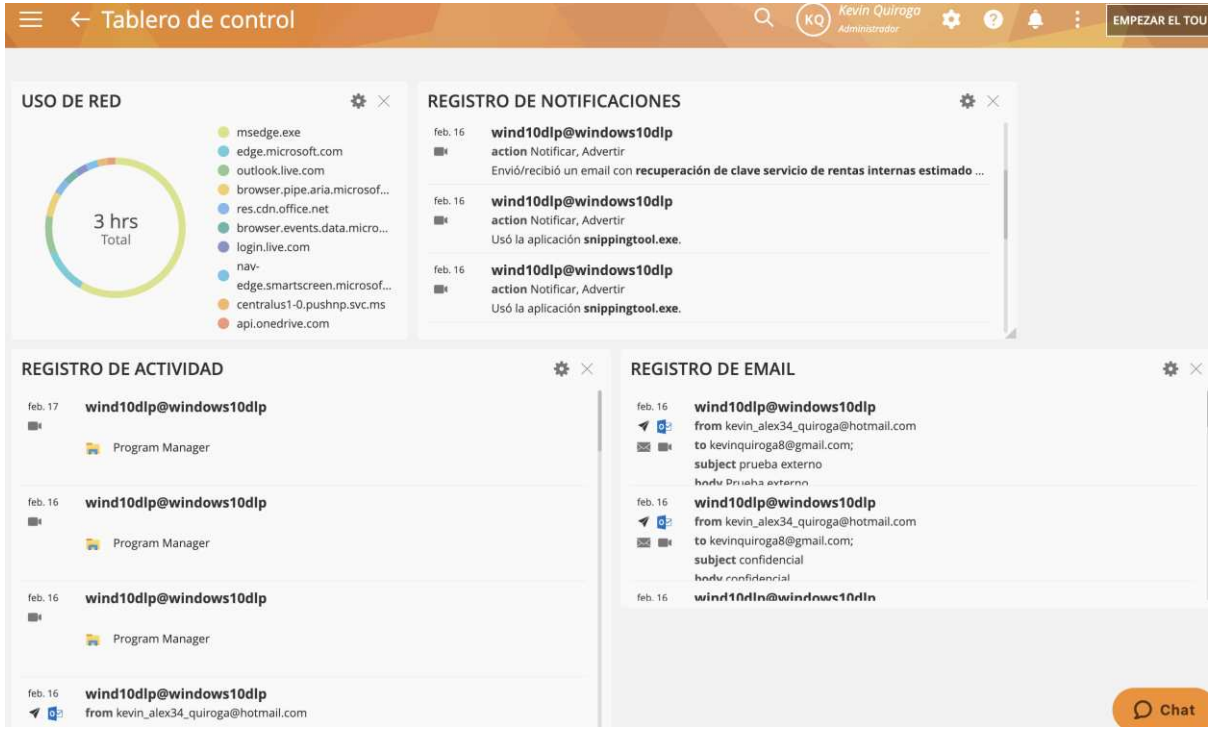
Repositorio Teramind

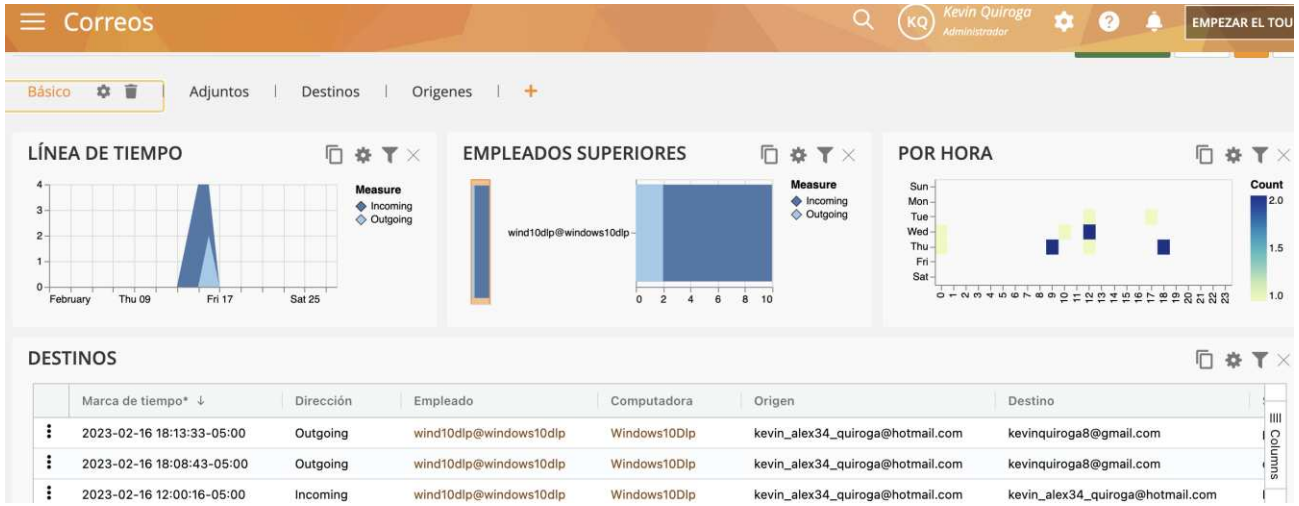
Descarga

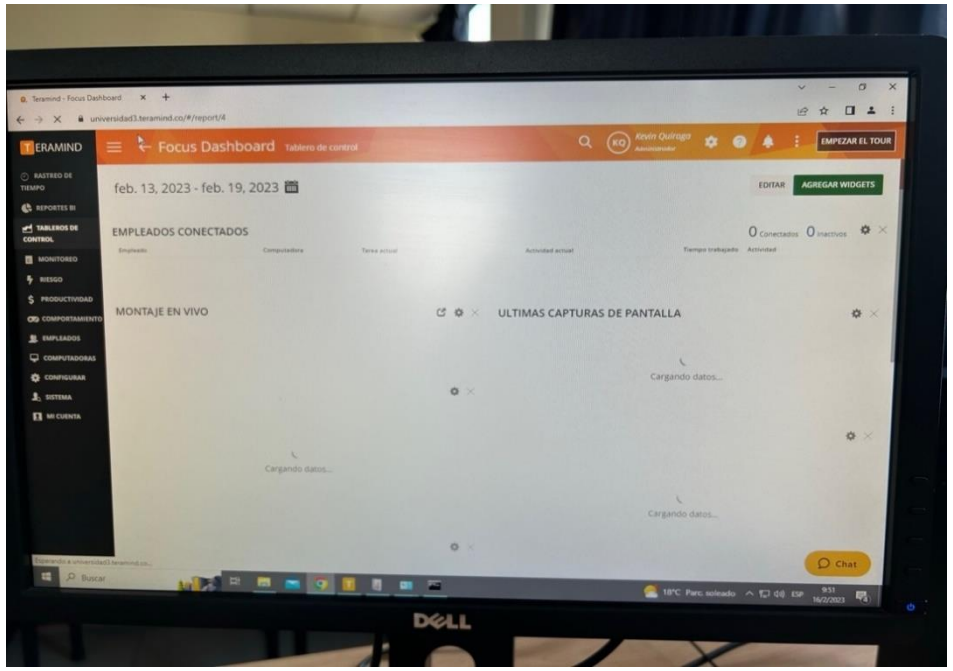
Instalación de Agente

Agente desplegado

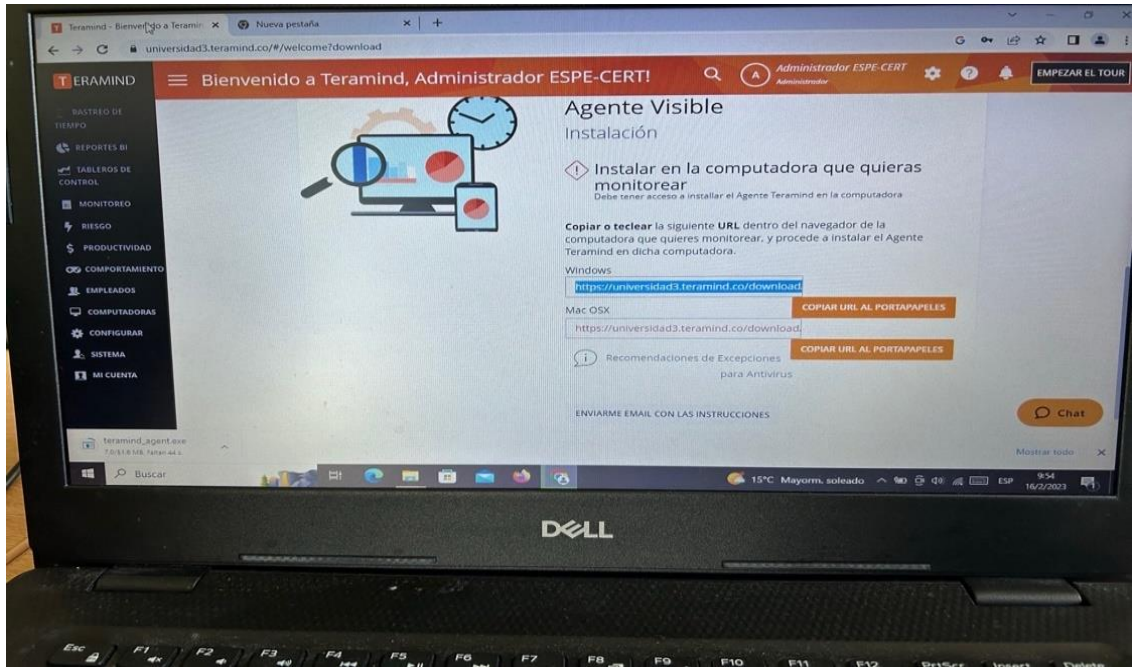
04. Reporte de actividad y alerta







Consola de Administración
máquina Operador ESPE



Consola de Administración
máquina Operador2 ESPE

- Con los datos de prueba obtenidos, se determinó que las políticas de descubrimiento implementadas alertaron el comportamiento del usuario.

- Con el despliegue en el Cert Académico ESPE se logró identificar que la conexión del agente dentro de la red Espe necesita de permiso de comunicación mediante Firewall

- Se realizó pruebas con notificaciones frecuentes sobre la herramienta de captura de pantalla a de más de envío de correos fuera del dominio.

- Con la información recolectada se genera tableros y reportes para el manejo de los operadores del Cert Académico ESPE

- Para la comunicación correcta del agente con la consola se recomienda revisar la conectividad de las maquinas terminales a la siguiente dirección y puerto: 141.144.250.131:32600

- Se recomienda tener un control y seguimiento de las alertas que se generan dentro de la herramienta a fin de que se pueda realizar un análisis de los registros obtenidos.

- Se recomienda analizar el uso de herramientas de recorte o de captura de pantalla para poder mitigar la captura de contenido sensible además de los destinatarios de correo electrónico.

- Se recomienda generar reportes semanales para dar un correcto seguimiento de los incidentes de seguridad