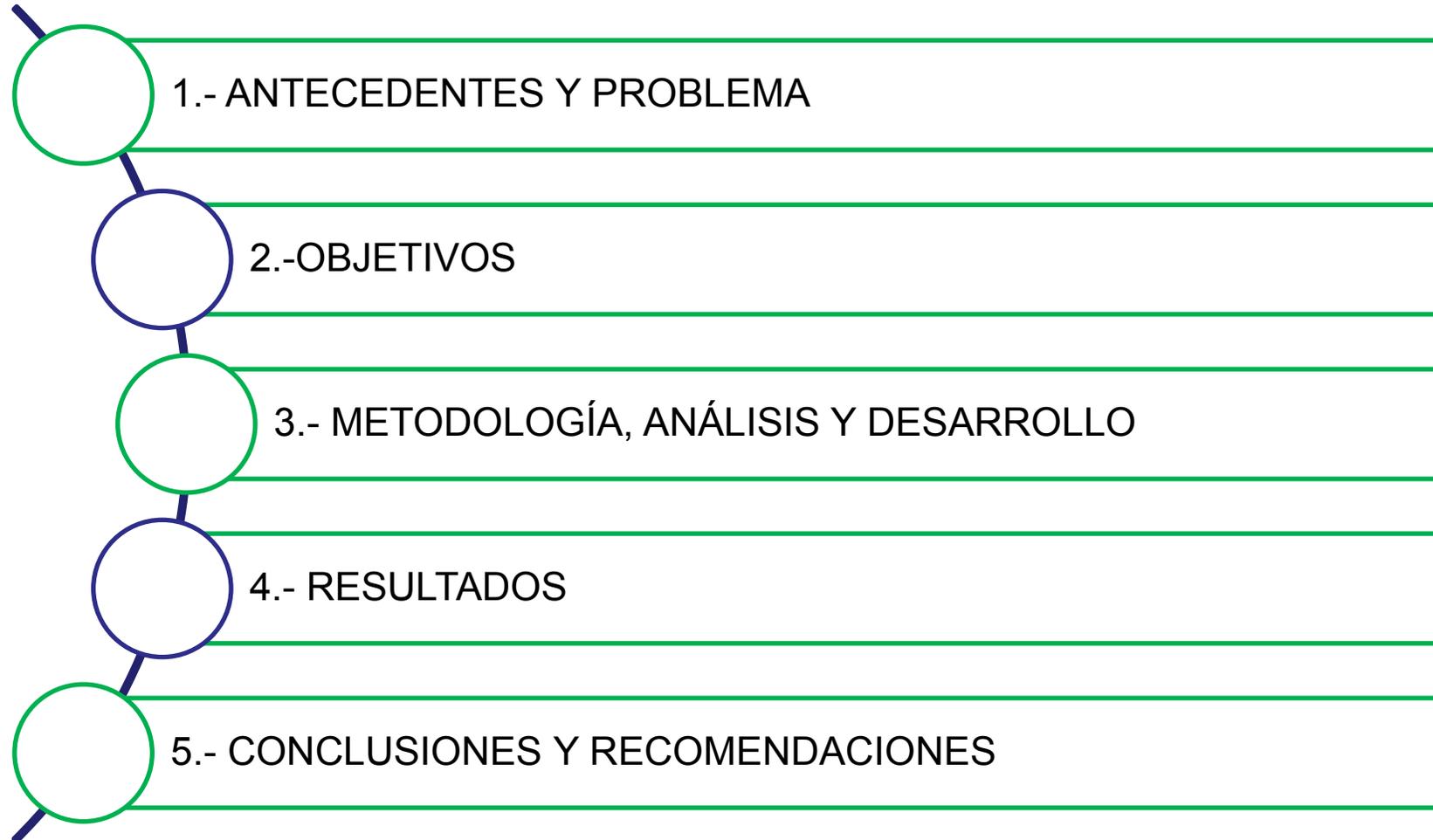


AGENDA



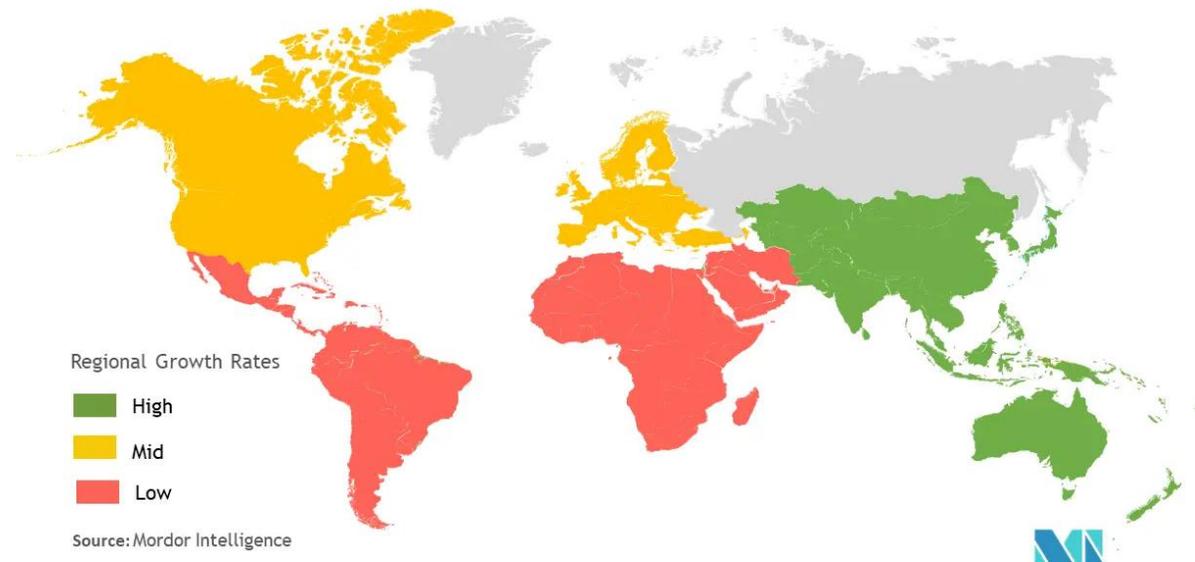


16 de Septiembre del 2019

- 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 tránsito;
- No llevar el registro de usuarios dentro de la red;
- No analizar 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.

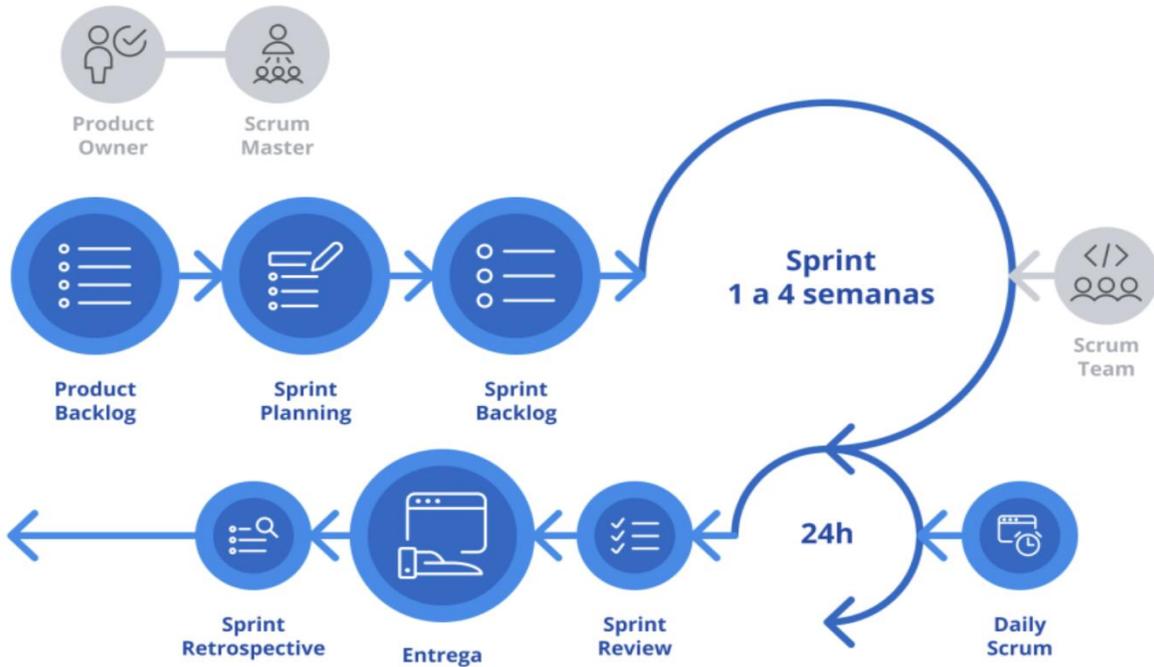


Objetivos Específicos

- 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

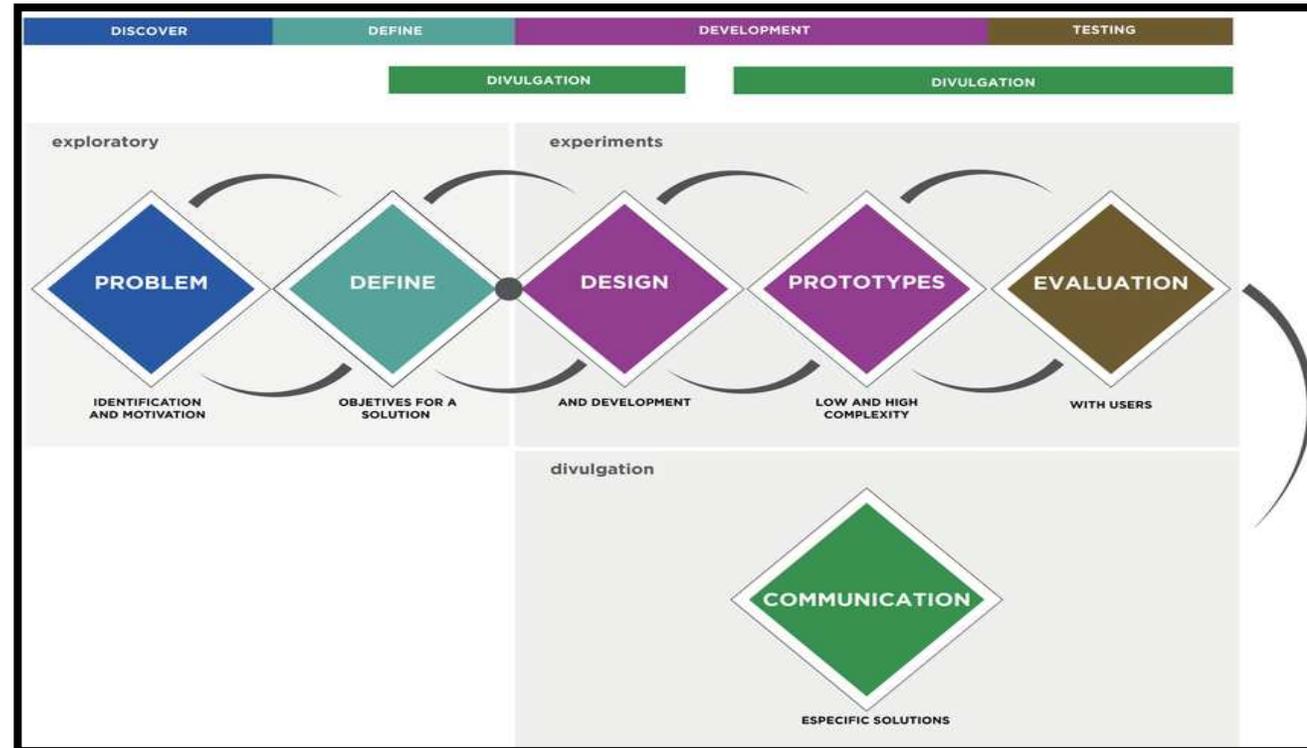
Ciclo Scrum



Metodología Scrum (Hevner, 2019).

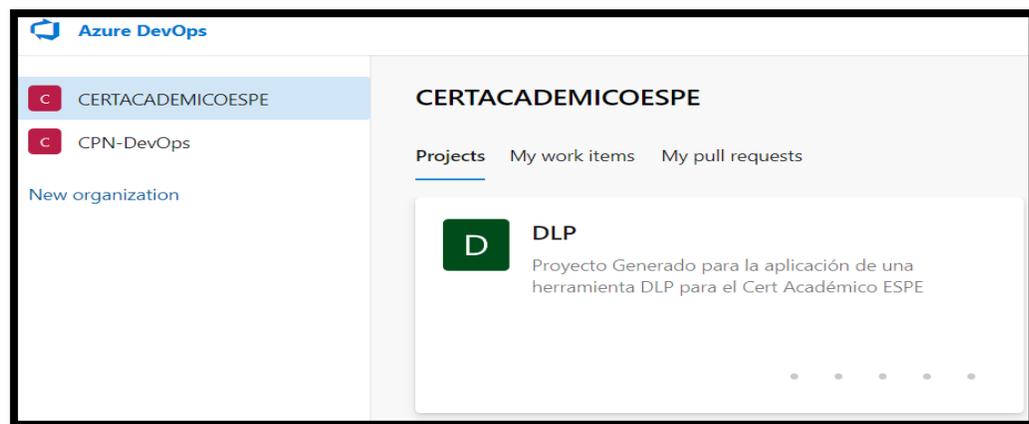
Design Science

Metodología Design Science propuesta por Hevner

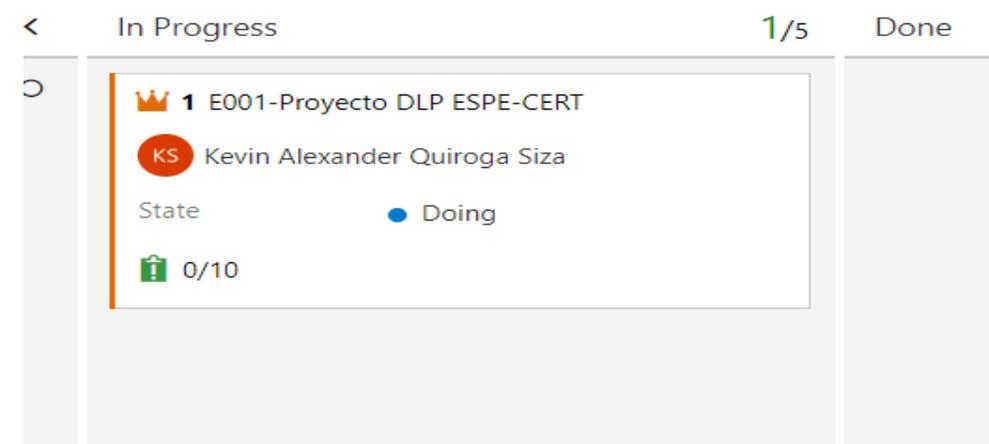


Metodología Design Science (Hevner, 2007).

Creación de Artefactos Scrum en AzureDevOps



Proyecto



Historia Épica

Creación de Artefactos en AzureDevOps

Done <

68 F025 Sprint Review

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 2/2

69 F026 Pruebas en Cert Académico ESPE

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 2/2

70 F027 Configuración de consola Teramind en Cert Académico ESPE

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 2/2

71 F028 Revisión Documento

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 1/1

Done <

58 F022 Actualización documento con revisiones

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 1/1

61 Revisión de estado herramienta Teramind

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 2/2

62 Generación de Políticas en Teramind

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 2/2

59 F021 Sprint Review

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 1/1

Done <

36 F014 Implementación de Prueba

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 1/1

22 F007 Políticas de Seguridad

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 1/1

5 F002 Creación de Documento Formato Tesis

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 3/3

3 F001-Herramientas DLP

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 2/2

Done <

13 F004 Análisis de Herramientas DLP Parte2

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 2/2

15 F006 Análisis de Infraestructura para DLP

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 2/2

14 F005 Fuentes Bibliográficas

KS Kevin Alexander Quiroga Siza

State ● Done

✓ 2/2

23 F008 Levantamiento de Información para DLP

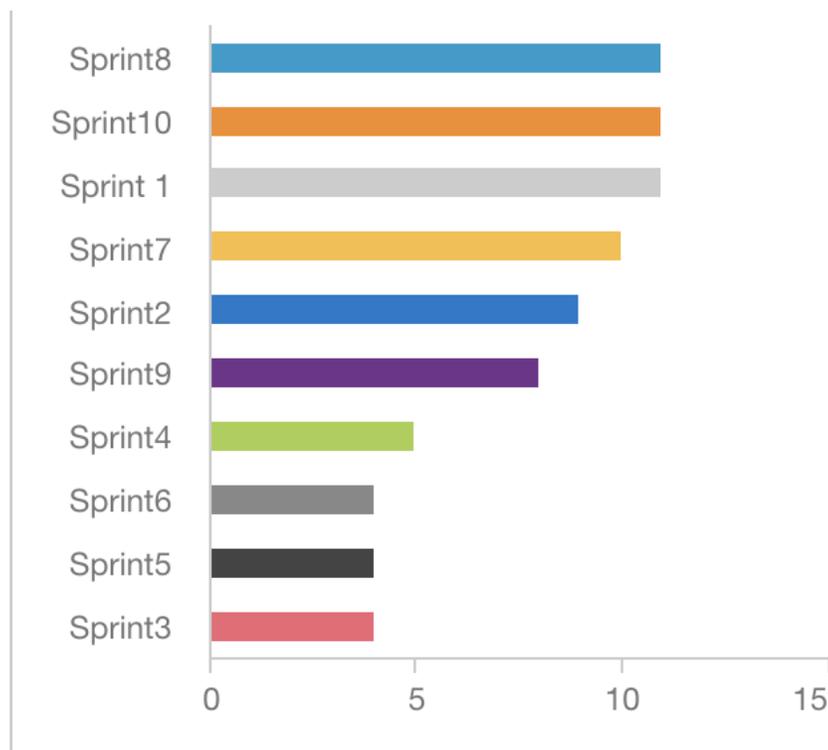
KS Kevin Alexander Quiroga Siza

State ● Done

✓ 1/1

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	<ul style="list-style-type: none"> <input type="checkbox"/> F003 Revisión de perfil de Tesis 	Kevin Alexand...	Doing
	11	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Validación de Fuentes Bibliográficas 	Kevin Alexand...	Done
	12	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Comprobación de la Redacción 	Kevin Alexand...	Done
2	3	<ul style="list-style-type: none"> <input type="checkbox"/> F001-Herramientas DLP 	Kevin Alexand...	Doing
	4	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Análisis de la Herramientas DLP 	Kevin Alexand...	Done
	8	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Investigación sobre temas DLP 	Kevin Alexand...	Done
3	5	<ul style="list-style-type: none"> <input type="checkbox"/> F002 Creación de Documento Formato Tesis 	Kevin Alexand...	Doing
	6	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Validación Formato Tesis Biblioteca 	Kevin Alexand...	Done
	7	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Actualización de Documento 	Kevin Alexand...	Done
	9	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Validación formato de referencias bibliográficas 	Kevin Alexand...	Done

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

Order	ID	Title	Assigned To	State
1	13	<ul style="list-style-type: none"> <input type="checkbox"/> F004 Análisis de Herramientas DLP Parte2 	Kevin Alexand...	Doing
	20	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Validación de herramientas disponibles 	Kevin Alexand...	Done
	21	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Validación de integraciones 	Kevin Alexand...	Done
2	14	<ul style="list-style-type: none"> <input type="checkbox"/> F005 Fuentes Bibliográficas 	Kevin Alexand...	Doing
	18	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Revisión bibliográfica acerca de soluciones de seguridad ... 	Kevin Alexand...	Done
	19	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Creación de Referencias en formato APA 	Kevin Alexand...	Done
3	15	<ul style="list-style-type: none"> <input type="checkbox"/> F006 Análisis de Infraestructura para DLP 	Kevin Alexand...	Doing
	16	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Búsqueda de información despliegues DLP 	Kevin Alexand...	Done
	17	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Validación de integraciones 	Kevin Alexand...	Done

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

Order	ID	Title	Assigned To	State
1	23	<ul style="list-style-type: none"> <input type="checkbox"/> F008 Levantamiento de Información para DLP 	Kevin Alexand...	Doing
	24	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Investigación de documentación 	Kevin Alexand...	Done
2	22	<ul style="list-style-type: none"> <input type="checkbox"/> F007 Políticas de Seguridad 	Kevin Alexand...	Doing
	25	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Investigación sobre políticas de seguridad 	Kevin Alexand...	Done

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

Order	ID	Title	Assigned To	State
1	26	<ul style="list-style-type: none"> <input type="checkbox"/> F009 Elección herramienta DLP 	Kevin Alexand...	Doing
	29	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Revisión Bibliografica 	Kevin Alexand...	Done
	30	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Validación de Herramienta Teramind DLP 	Kevin Alexand...	Done
2	27	<ul style="list-style-type: none"> <input type="checkbox"/> F010 Documentación Tesis 	Kevin Alexand...	Doing
	28	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> 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	<input type="checkbox"/> F011 Búsqueda Bibliográfica	Kevin Alexand...	● Doing
	34	<input checked="" type="checkbox"/> Búsqueda de información sobre herramienta Dlp y Terami...	Kevin Alexand...	● Done
2	32	<input type="checkbox"/> F012 Analisis Teramind DLP	... Kevin Alexand...	● Doing
	33	<input checked="" type="checkbox"/> Validación de documentación Teramind	Kevin Alexand...	● Done

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

Order	ID	Title	Assigned To	State
1	36	<input type="checkbox"/> F014 Implementación de Prueba	Kevin Alexand...	● Doing
	37	<input checked="" type="checkbox"/> Validación de tipos de despliegue Teramind DLP	Kevin Alexand...	● Done
2	35	<input type="checkbox"/> F013 Actualización documento con apartado de Desarr...	... Kevin Alexand...	● Doing
	38	<input checked="" type="checkbox"/> Insertar imagenes de prueba y Desarrollo de el despliegue...	Kevin Alexand...	● Done

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

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

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

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

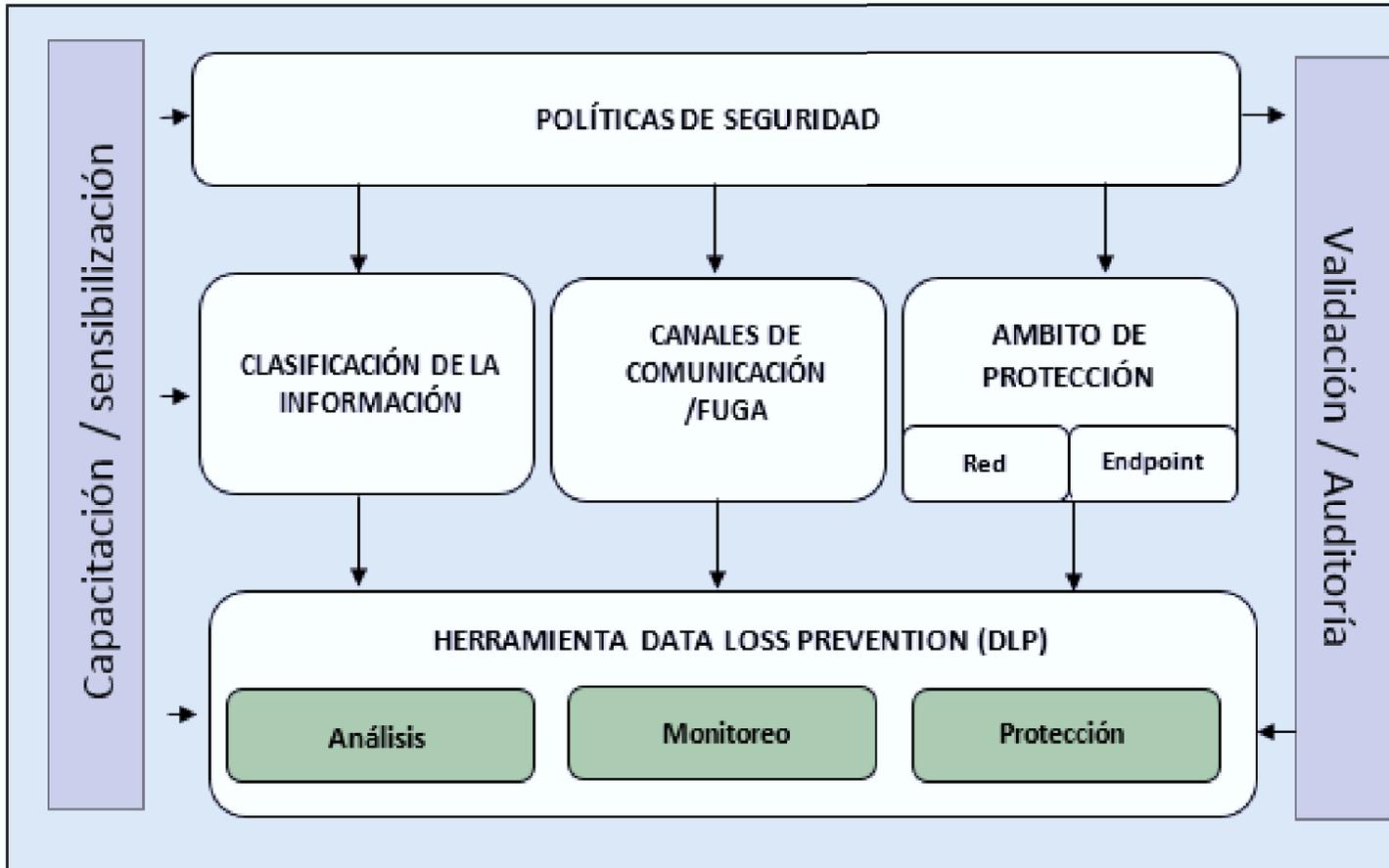


Comparativa de herramientas DLP

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

03. Modelo de seguridad

Modelo de seguridad tomando en cuenta el estándar ISO27001



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

Arquitectura de despliegue en Azure

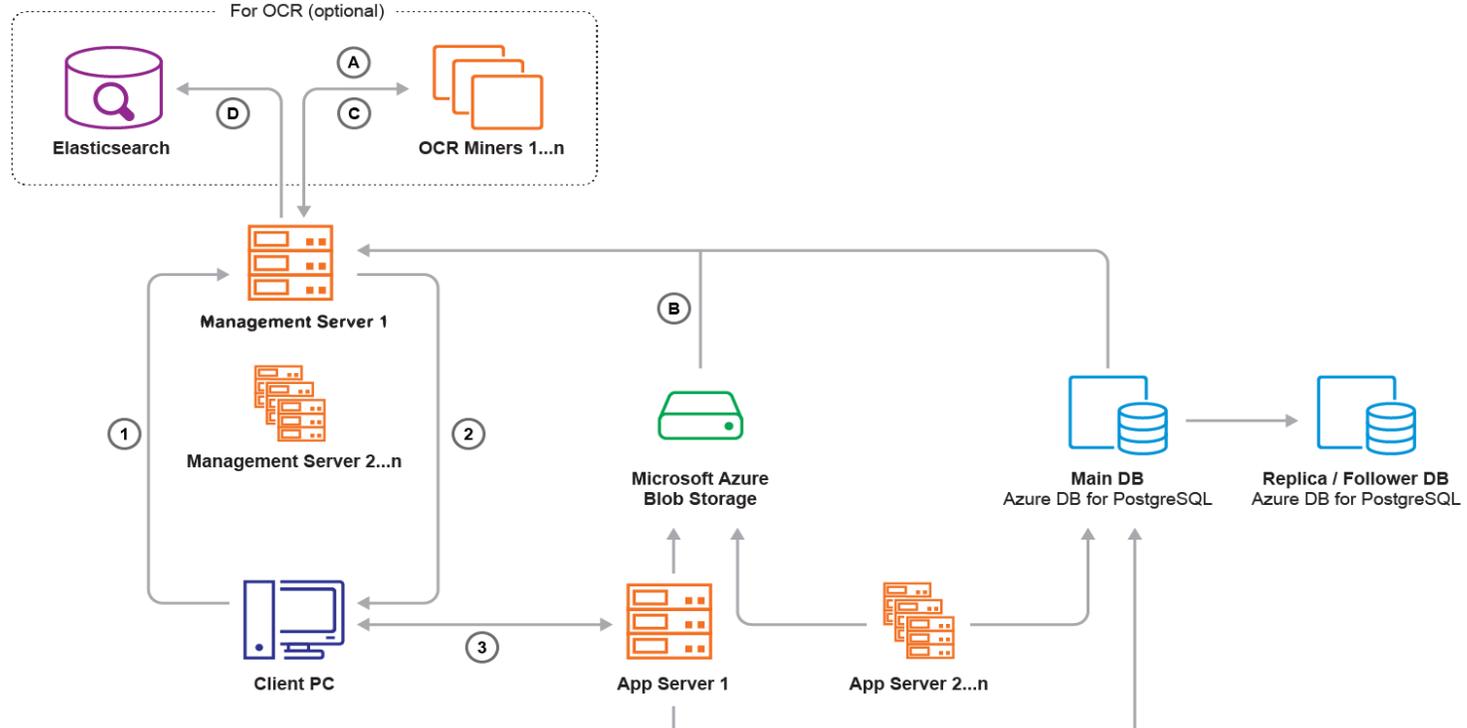
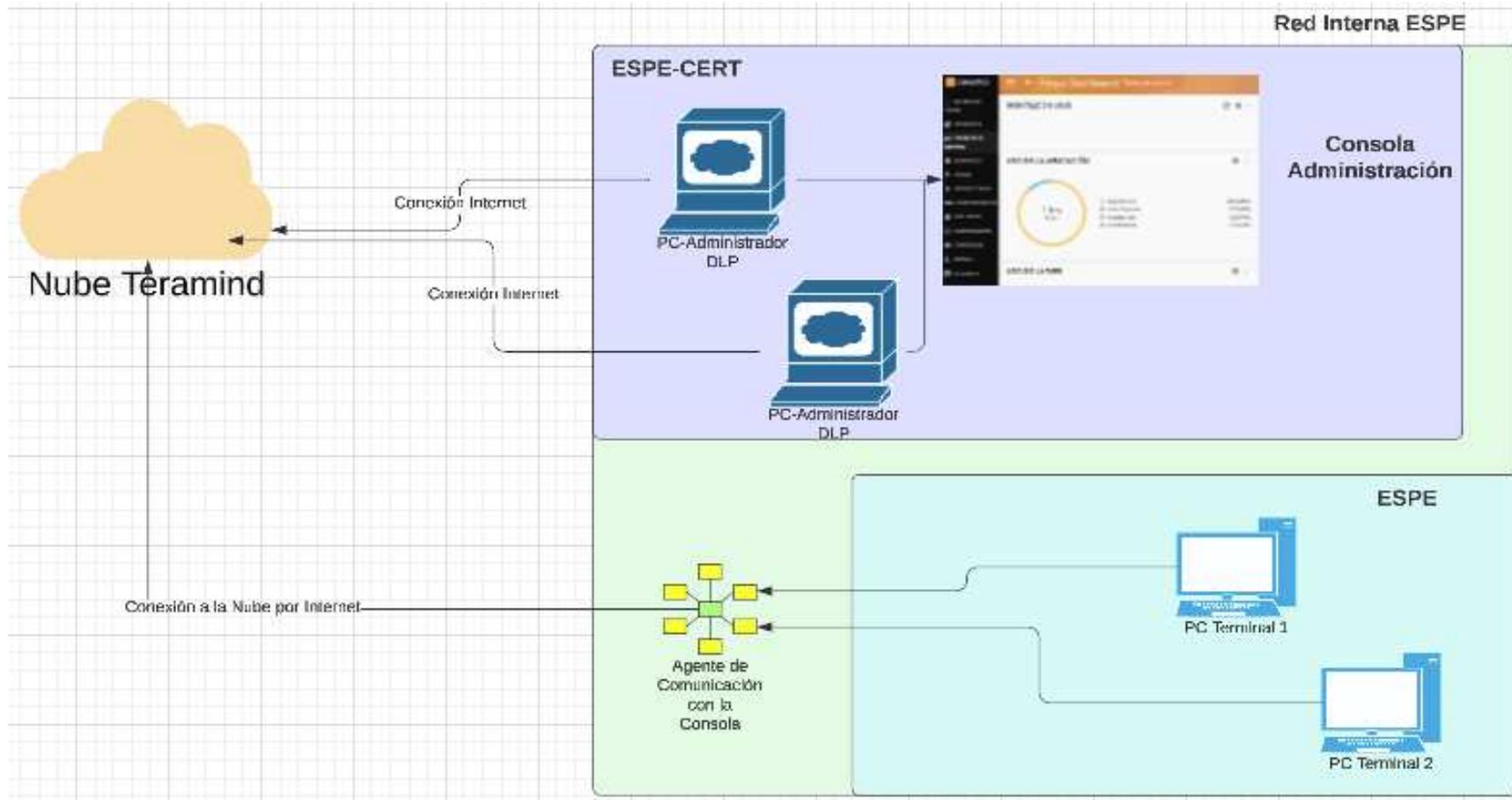
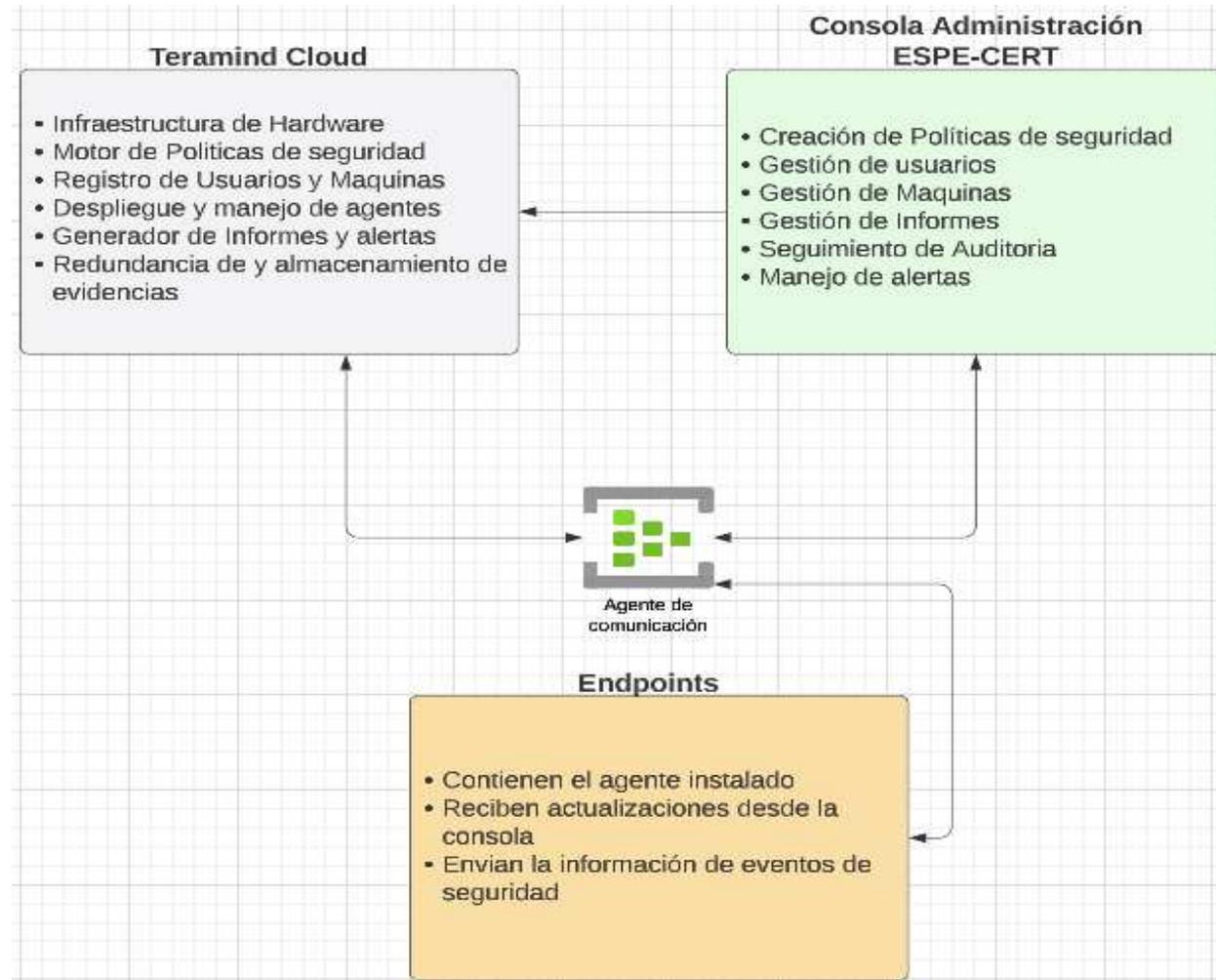


Diagrama de Comunicación

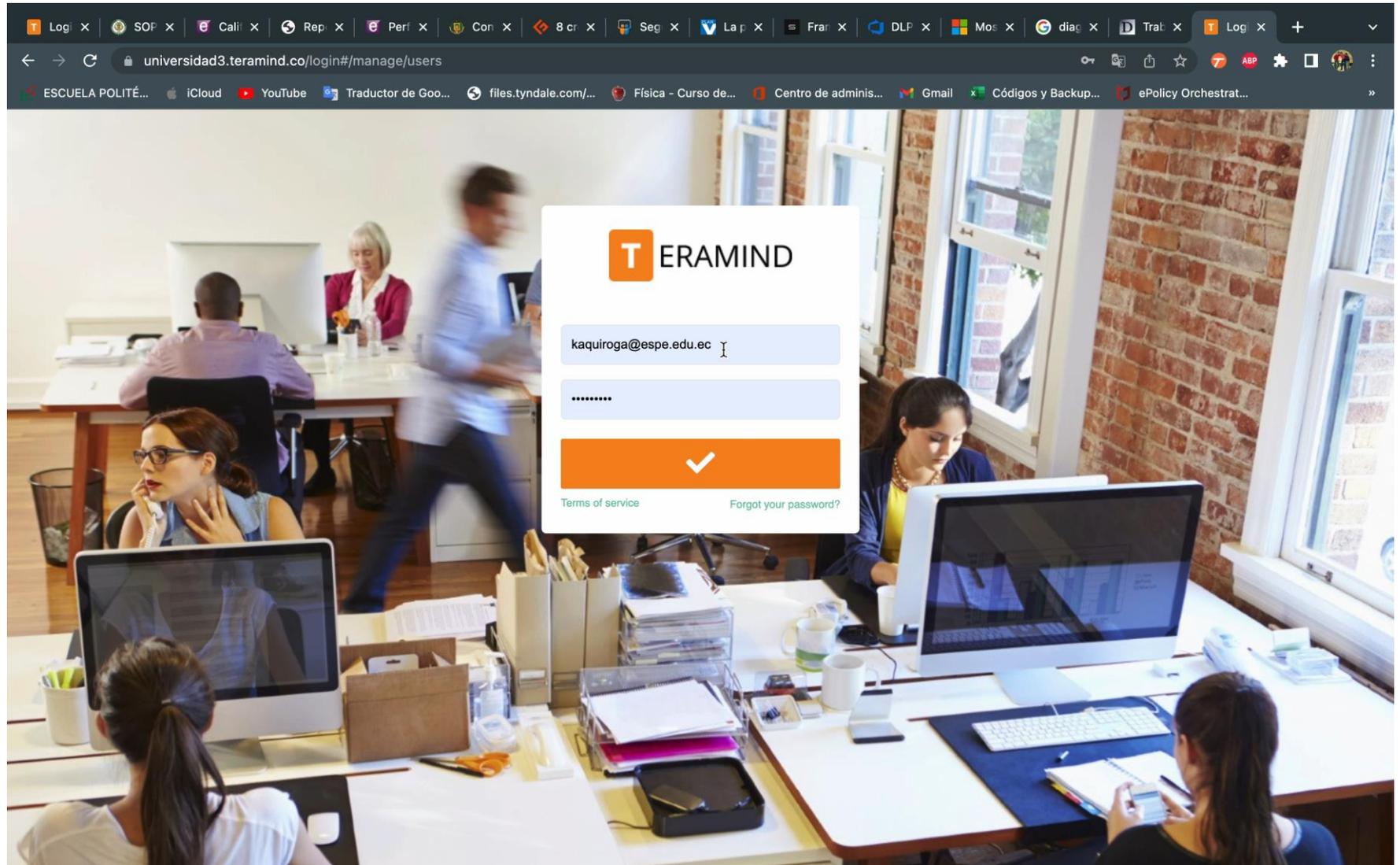


Descripción de la estructura



03. Demo consola Administración

Inicio de Sesión en Consola



03. Demo consola Administración

Registro de Usuarios y Máquinas

The screenshot displays the ERAMIND administration console interface. At the top, the browser address bar shows the URL `universidad3.teramind.co/#/report/4`. The dashboard header includes the ERAMIND logo, a navigation menu, and the user profile of Kevin Quiroga, Administrator. The main content area is titled "Tablero de control" and shows a date range of "feb. 27, 2023 - mar. 5, 2023".

Key features and widgets include:

- EMPLEADOS CONECTADOS:** A table with columns for Empleado, Computadora, Tarea actual, Actividad actual, Tiempo trabajado, and Actividad. It shows 0 Conectados and 0 Inactivos.
- MONTAJE EN VIVO:** A live monitoring widget.
- USO DE LA APLICACIÓN:** A widget showing application usage, currently displaying "Sin datos para las fechas seleccionadas".
- ULTIMAS CAPTURAS DE PANTALLA:** A widget for recent screenshots, also showing "Sin datos para las fechas seleccionadas".
- REGISTRO DE EMAIL:** A widget for email activity, showing "Sin datos para las fechas seleccionadas".
- USO DE LA WEB:** A widget for web usage, showing "Sin datos para las fechas seleccionadas".

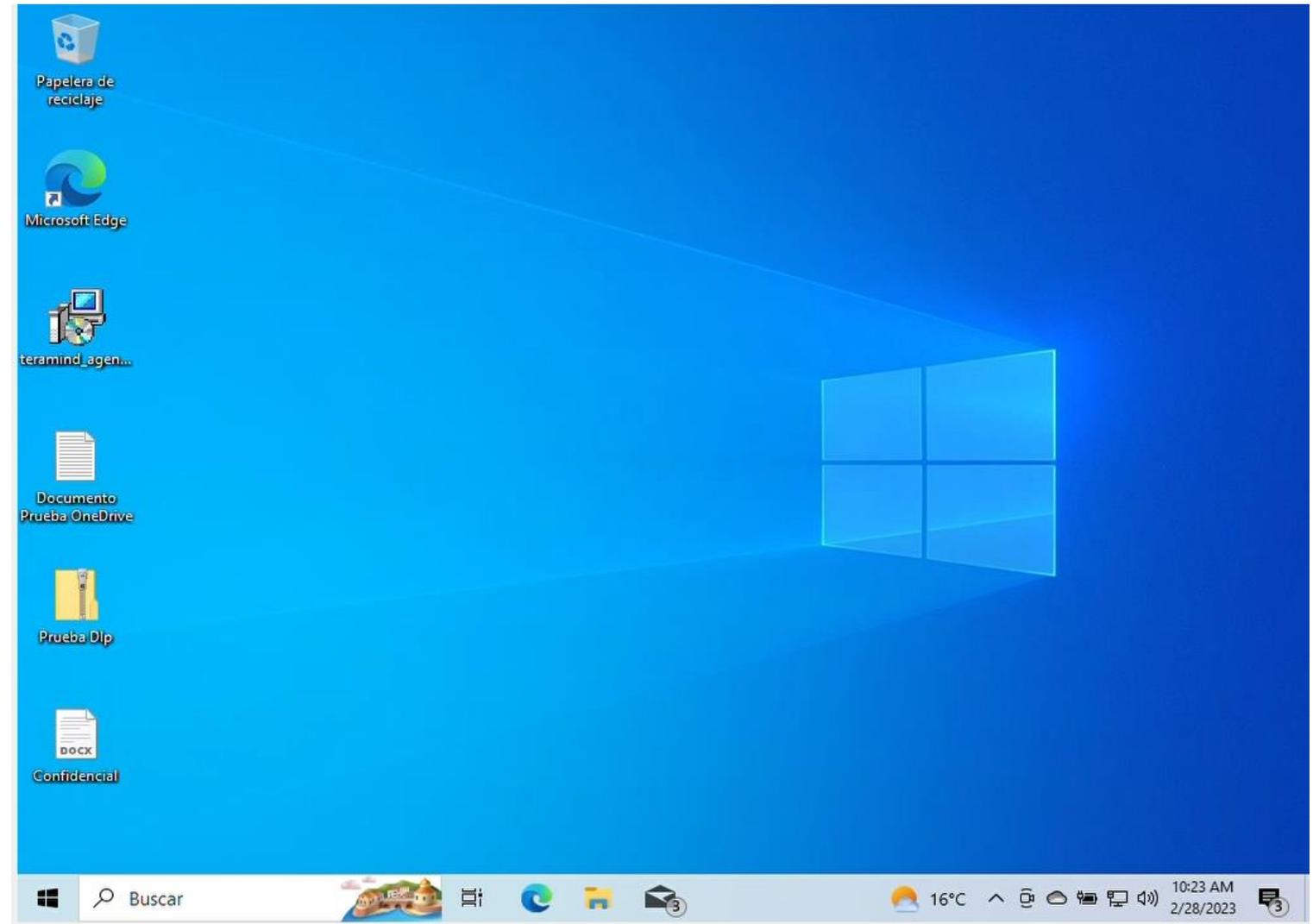
The left sidebar contains navigation options: RASTREO DE TIEMPO, REPORTES BI, TABLEROS DE CONTROL, MONITOREO, RIESGO, PRODUCTIVIDAD, COMPORTAMIENTO, EMPLEADOS, COMPUTADORAS, CONFIGURAR, SISTEMA, and MI CUENTA. A "Chat" button is located in the bottom right corner.

03. Demo consola Administración

The screenshot shows the TERAMIND administration console interface. The browser address bar displays 'universidad3.teramind.co/#/computer/5'. The page title is 'Detalles de la PC'. The user is identified as 'Kevin Quiroga Administrador'. The main content area shows details for computer 'espe04' for the period 'feb. 27, 2023 - mar. 5, 2023'. A message states: 'No hay datos a mostrar para el rango de fechas seleccionado'. The interface includes a sidebar with navigation options like 'RASTREO DE TIEMPO', 'REPORTES BI', 'TABLEROS DE CONTROL', 'MONITOREO', 'RIESGO', 'PRODUCTIVIDAD', 'COMPORTAMIENTO', 'EMPLEADOS', 'COMPUTADORAS', 'CONFIGURAR', 'SISTEMA', and 'MI CUENTA'. The top navigation bar includes 'ACTIVIDAD', 'MONTAJE EN VIVO', 'ALERTAS', 'CAPTURAS DE PANTALLA', 'EMAIL', 'TRANSFERENCIA DE ARCHIVOS', 'MONITOREO DE RED', and 'HISTORIA'. A 'Chat' button is visible in the bottom right corner.

Políticas y reglas de seguridad

Alerta Máquina Final



Consola Administración Políticas

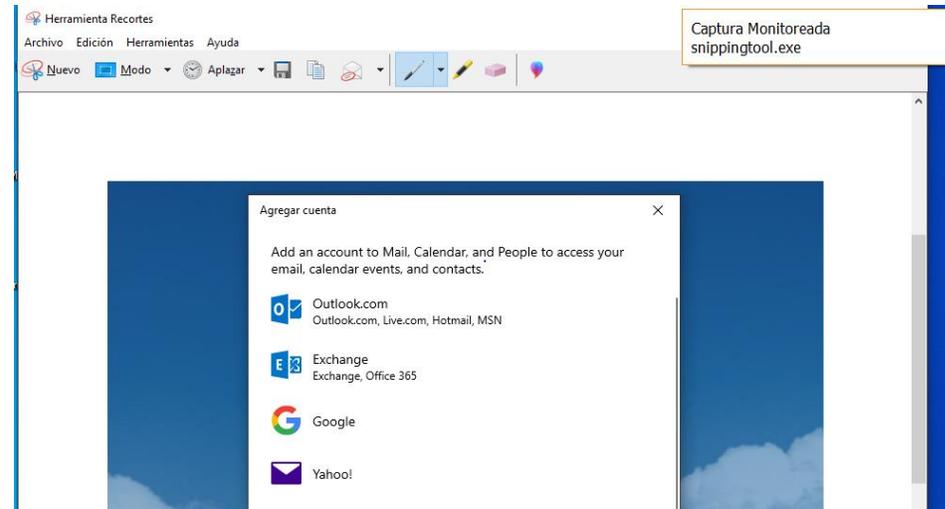


Agente de Conexión

Regla Herramienta de captura de pantalla/recortes Resumen

- Políticas de Descubrimiento Política
- Categoría
- Actividad
- Usuarios
 - Aplicar a **Everyone**
- Aplicaciones
 - Nombre de la aplicación **contiene snippingtool.exe**
- Pulsaciones de teclado
 - Texto ingresado **contiene <PrtSc>** o **contiene <Shift+PrtSc>**
- Acciones
 - Notificar **kaquiroya@espe.edu.ec** y Mostrar advertencia con mensaje **Captura Monitoreada**

Descripción de Regla



Alerta Usuario

03. Política y reglas de Monitoreo

Políticas de Descubrimiento ^

6 reglas

Everyone

SI



Verificación envío a Correos Externo Alerta cuando los usuarios envían correos a destinos diferentes @espe.edu.ec	Categoría de regla: Actividad		<input checked="" type="checkbox"/> SI		
Validación cuerpo de correo Alerta cuando el cuerpo del correo contiene la palabra confidencial	Categoría de regla: Actividad		<input checked="" type="checkbox"/> SI		
Documento con Marca Confidencial Alerta cuando se comparte un archivo con marca Confidencial	Categoría de regla: Compartir contenido		<input checked="" type="checkbox"/> 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		<input checked="" type="checkbox"/> SI		
Subir archivos a la nube Notificar cuando los usuarios cargan archivos en Google Drive, OneDrive, Box o DropBox	Categoría de regla: Actividad		<input checked="" type="checkbox"/> SI		
Guardar un archivo en un medio extraíble Alerta cuando los usuarios guardan archivos en USB u otros medios externos	Categoría de regla: Actividad		<input checked="" type="checkbox"/> SI		



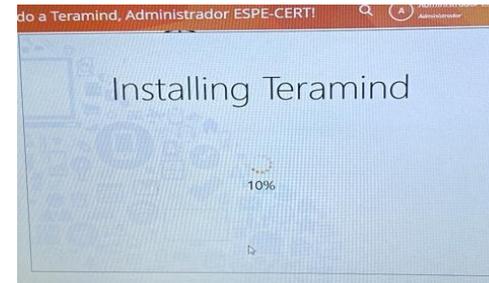
04. Instalación de agente

Descargar el Agente Teramind

Repositorio Teramind



Descarga



Instalación de Agente



espe04

Monitorear computadora

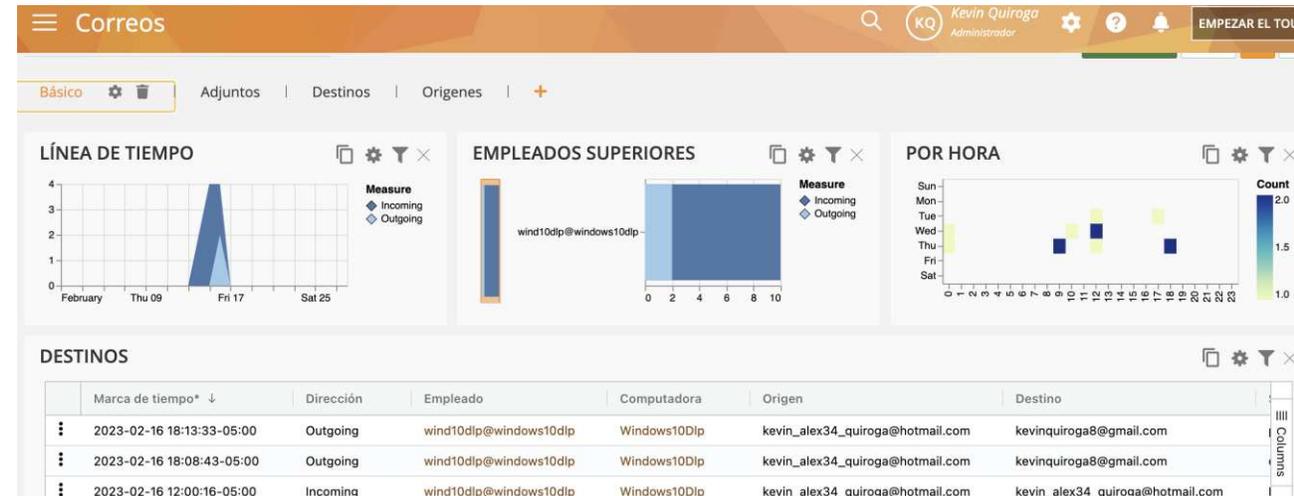
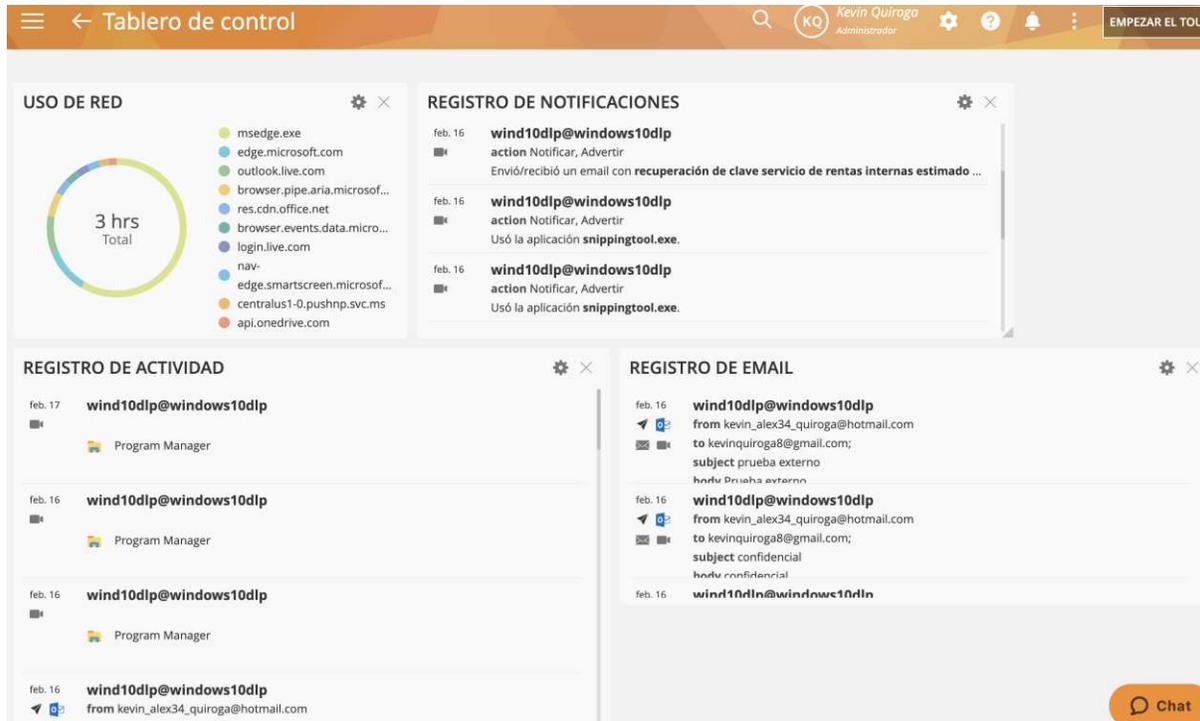
[EDITAR INFORMACIÓN](#)

DESINSTALAR AGENTE DE LA PC

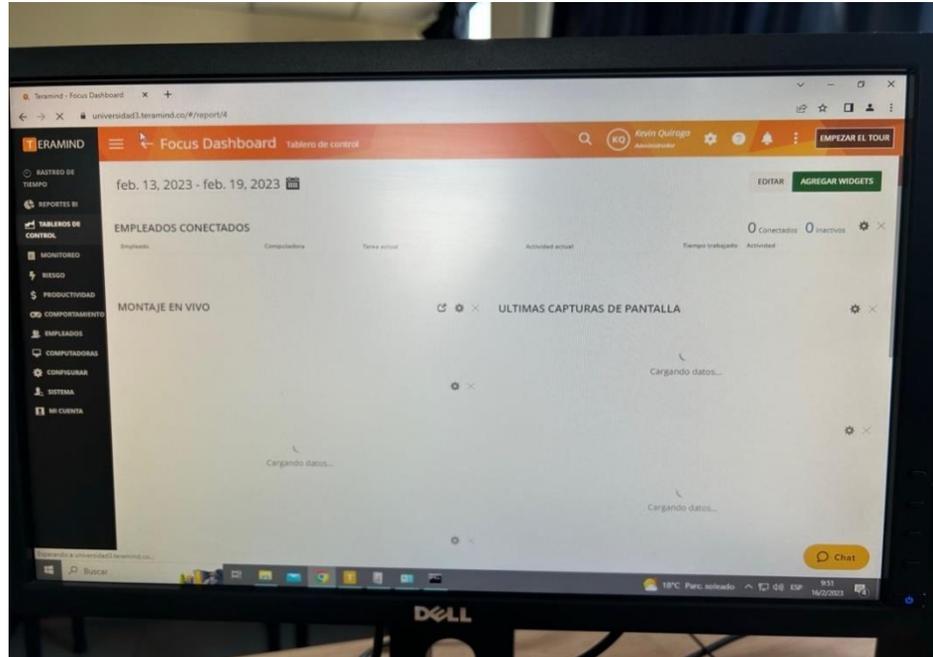
S.O.:	Windows 10
IP:	192.188.58.24
Versión del cliente:	8.0.1009
Modo Cliente:	Oculto
Usuarios en línea:	0

Agente desplegado

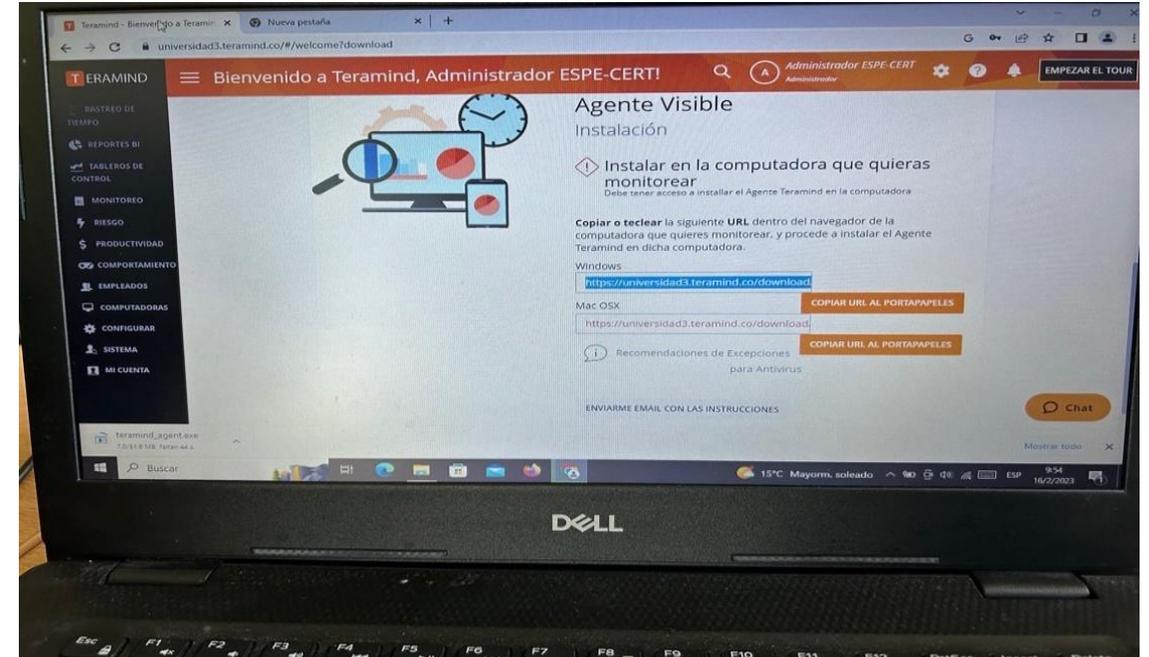
04. Reporte de actividad y alerta



04. Configuración Cert Académico ESPE



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