TRABAJO DE GRADO
Opción Seminario-Diplomado.

Mejora gerencial de la malla de ciberseguridad

Corporación Universitaria Remington.
Facultad de ingeniería
Ingeniería de sistemas

Autor: León Santiago Urrego Atehortua

Tutor: Johana Sepúlveda Jiménez
Seminario Gestión de proyectos y habilidades gerenciales
2026

Dedicatoria

Este trabajo es dedicado a Luisa Montoya, mi esposa, quien siempre ha apoyado en los momentos difíciles y con quien he aprendido a creer en mí y apoyándome para terminar mis estudios de forma integral.

Agradecimientos

Agradezco a GTD Colombia por el apoyo brindado durante mi formación, su confianza y respaldo no solo ha sido valioso en lo económico sino también en lo personal.

A mis padres por su ejemplo de trabajo duro y perseverancia. Gracias por cada sacrificio y por su apoyo constante, son motivación en cada logro cumplido.

A mis hermanos, gracias por siempre estar y hacer equipo, ustedes son parte fundamental de mi vida y de mis logros.

Y por último gracias a mis sobrinas porque sus sonrisas y ocurrencias han hecho más livianos mis días. Son mi motivación constante para seguir adelante y demostrarles que los sueños si se cumplen y que se puede ser mejor cada día.

Tabla de Contenidos

Resumen

Para el proyecto se quiere realizar una estrategia que permita desarrollar e integrar a nivel de ciberseguridad las plataformas multimarca en un solo proveedor, basado en los principios de liderazgo servicial y gestión de interesados. El proyecto busca pasar de un modelo de gestión fragmentada hacia un modelo de arquitectura mesh unificada, basado en el marco de implementación de SCRUMBAN.

El enfoque principal que se está dando, no solo está basado en lo técnico, sino también está basado en la organización, ya que con esto se pretende tener un control total de la solución de ciberseguridad y lograr así una mejora en los tiempos de respuesta ante incidentes.

Palabras clave: Estrategia, Plataformas, Ciberseguridad, Metodologías Ágiles, Scrumban

Marco conceptual y contextual

La compañía GTD actualmente tiene varias plataformas de ciberseguridad, las cuales están compuestas de la siguiente manera:

Plataforma de acceso seguro ZTNA

Plataforma de administración de accesos PAM

Plataforma de seguridad perimetral firewall

Plataforma de autenticación y autorización de accesos 2MFA

Estas no están homologadas en una sola marca, lo que genera, que se cuenten con administradores diferentes según cada plataforma; cada equipo administra permisos de uso y explotación y allí se detecta una amplia oportunidad de mejora. Una de las principales la vemos reflejada, que, al tener tantos proveedores, se generan fallas constantes de integración entre plataformas y equipos de trabajo, ya que al ser tantos y tan variados cada equipo se ha especializado en conocer y usar el producto de un solo proveedor en específico, dejando de lado los beneficios que se pueden obtener, al tener todos los productos unificados en un solo proveedor.

Para lograr la integración de todos los productos en una sola marca, debemos crear un proyecto a medio plazo, la idea es usar metodologías agiles, seleccionando el personal idóneo para realizar la migración de cada producto, la idea como gerente de proyecto es elegir al recurso humano adecuado y capacitado para hacer esta nueva integración. Dado lo anterior procederemos a consolidar un proyecto de migración y unificación de las plataformas de la

compañía en una sola, este proyecto lo enfocaremos con una mezcla de las metodologías Scrum y Kanban.

Scrum nos ayudará con la migración de las plataformas y la selección de un solo proveedor que nos facilite la integración de las plataformas, adicionalmente vamos a presentar hitos claros y despliegues por fases. Y Kanban aportará organización durante el proceso de migración ya que no podemos permitir errores en los servicios actualmente activos.

Desarrollo e implementación del aprendizaje

Identificación de riesgos

Debido a que los equipos están fragmentados por plataforma, tenemos los siguientes riesgos:

Puntos Ciegos: Como no se tiene una integración de las plataformas, es casi imposible lograr el rastreo de los comportamientos de los usuarios de extremo a extremo, se pueden detectar ataques, pero al no presentar una buena comunicación el atacante se puede mover de forma lateral y materializar ataques.

Fallas de integración: La interoperación entre plataformas depende de que se puedan aplicar APIs o configuraciones manuales, las cuales pueden fallar tras procesos de actualización, estas grietas temporales pueden ser las favoritas para los ciberdelincuentes.

Fallas en la identificación del usuario: Tener múltiples plataformas aumenta el riesgo de tener permisos huérfanos, estos pueden generar puntos y brechas de seguridad enormes ya que cualquier persona puede continuar ingresando a las plataformas por no tener claro qué permisos tenía para entrar a los recursos de la compañía.

Fatiga por alertas: Al recibir alertas de 4 proveedores diferentes, y no poder consolidarlas o correlacionarlas de manera unificada, genera un gran volumen de alertas que las personas, terminan ignorando o normalizando por agotamiento.

Conocimiento centralizado: Debido a que los expertos de cada plataforma son solo conocedores de su herramienta, se genera una dependencia de esta persona y en caso tal que presente su renuncia o una incapacidad, no se tiene quien lo reemplace y por ende la compañía se encuentra vulnerable y no permite tener un equipo que pueda gestionar el conocimiento para apoyarse entre sí.

Aumento de los tiempos de respuesta: El tiempo de validación de una plataforma es de 1 hora, sin embargo, como se debe validar en cada plataforma, los equipos pueden demorar entre 2 y 4 horas en encontrar las fallas.

Costos elevados: Mantener múltiples plataformas y contratos de soporte para cuatro proveedores es mucho más costoso que contar con un socio estratégico.

Poco escalable: Estas estructuras divididas generan conflictos en caso de necesitas hacer integraciones con nuevos servicios, generar integraciones en cuatro plataformas es mucho más complicado.

Auditorías: Tener auditorías es común en tecnología, sin embargo, preparar las auditorías del área de ciberseguridad es más complejo ya que se necesita llevar a cada experto de plataforma a validar accesos y pruebas, algo que deja huérfana la mesa de ayuda para atención de incidentes.

Definición de Roles

Con el proyecto se busca realizar una transición de puesto “Estático” hacia roles “Dinámicos” buscando que el eje central de las nuevas plataformas sean las personas y no las marcas, fomentando entonces el desarrollo de habilidades cruzadas y la autogestión del personal, pasando entonces así de una dependencia muy rígida y jerárquica hacia un equipo de trabajo colaborativo y alineado a la visión integral del éxito. Modelo de Habilidades Gerenciales de Robert Katz, el éxito técnico es inseparable de las habilidades humanas y conceptuales (Sepúlveda, 2026).

También estamos encontrando grandes beneficios con la definición de roles como lo son:

Eliminación de dependencias: Contar con un equipo que conoce la malla operativa, genera que, con la falta de una persona del equipo, se pueda continuar con la operación de manera constante.

Seguridad Psicológica: Tener roles claros permitirá al equipo tomar decisiones bajo presión con la confianza que significa tener tus funciones claras y definidas.

Los roles definidos para realizar de forma correcta la migración de las plataformas son:

Product Owner, persona líder de seguridad, quien va a priorizar las fases de migración y define los criterios de éxito al final de cada etapa.

Scrum Máster, encargado de facilitar las herramientas necesarias para no presentar bloqueos técnicos y asegurar que los equipos no pierdan el foco al momento de la integración.

Arquitecto de Integración, es quien permite garantizar que la nueva solución quede perfectamente instalada y unificada según los criterios empresariales.

Expertos de plataforma, son quienes con su experiencia apoyarán y darán los conceptos técnicos durante la migración y se convertirán en los administradores globales del servicio de ciberseguridad.

¿Cómo lo vamos a realizar?

Con el fin de encontrar el mejor producto, se utilizará la metodología Scrumban, se realizarán inicialmente sprints con una duración de 2 semanas, los siguientes eventos se estructuraron para llevar a cabo los sprint:

Sprint Planning: Se realizar la planeación de 1 hora, el objetivo es definir las políticas de ciberseguridad que deben ser migradas en el ciclo, además, definir objetivos del mes.

Daily Meet: Sesiones diarias de 15 minutos para verificar el estado del proyecto y detectar si se tienen bloqueos en las integraciones.

Sprint Review: Se realiza una demostración de 1 hora ante nuestros patrocinadores, para evidenciar como las plataformas unificadas están operando, esto con el fin de obtener un feedback temprano que se pueda incorporar en el siguiente sprint.

Sprint Retrospective: Se realiza una reunión al finalizar cada sprint con el objetivo de identificar cuáles son los ajustes técnicos y humanos que se deben de realizar para optimizar la migración, para ello utilizaremos el método básico **de 3 preguntas: ¿qué salió bien?, ¿qué salió mal? y ¿qué podemos mejorar?**

Mes 1 Sprint 1 y 2: Durante esta etapa se levantará la información técnica detallada de todas las plataformas que van a ser migradas y se realizará la definición de los requisitos, los cual deberán de ser entregados en una matriz de ponderación de proveedores, asegurando así que el proveedor elegido cumpla con la visión de ser un proveedor único.

Tabla 1. Matriz de ponderación de proveedores

Criterio de Evaluación	Peso (%)	Proveedor A (Líder)	Proveedor B	Proveedor C	Proveedor D	Nota Técnica (Módulo 4)
Integración Nativa (ZTNA+ 2MFA+PAM+FW)	40%					Mide la capacidad de consola única (Malla de Seguridad).
Experiencia en el Sector Telecomunicaciones	20%					Evalúa el conocimiento de entornos como GTD.
Costo Total de Propiedad (TCO)	20%					Equilibrio entre presupuesto y licenciamiento unificado.
Soporte y Escalabilidad	10%					Disponibilidad de soporte local y

		crecimiento modular.
Facilidad de Uso (UX)	10%	Reduce la curva de aprendizaje de la célula.
PUNTUACIÓN TOTAL	100 %	Proveedor Elegido: Proveedor A

Nota: Autoría propia.

Mes 2 Sprint 3 y 4: Se realiza la evaluación de los proveedores que entreguen los documentos (RFI/RFP) para la integración de las plataformas, aquí el proveedor deberá demostrar que es capaz de unir todos los servicios de forma integral, cumpliendo las siguientes métricas.

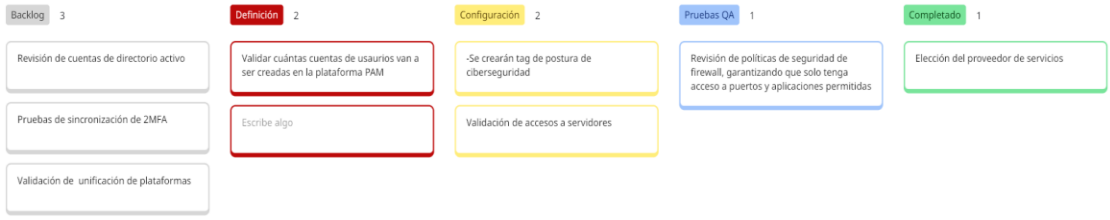
Métricas de Calidad: Ajustar al 100% los requisitos para garantizar un acceso remoto seguro.

Métricas Técnicas: Validación de que se unifica la plataforma de forma correcta y que se puede realizar seguimiento en una sola pantalla

Métricas de Productividad: Se evalúa el tiempo que toma la creación de un usuario en la nueva plataforma unificada, validando que este sea creado en las 4 plataformas integradas.

La fase de migración y mejora que estará bajo el enfoque de Kanban se iniciará una vez se tenga elegido el proveedor. Se presentará entonces un tablero Kanban el cual no solo será una

herramienta visual, también tendrá un flujo de trabajo con políticas explicitas y límites, para evitar que el equipo de trabajo presente saturación de tareas y visualizar así, los posibles cuellos de botella que se presenten durante cada fase.



Nota: Autoría propia. Esta es una simulación visual futura del proyecto.

Pilares por valorar:

Visualización de valor: Cada tarjeta presenta un requisito de seguridad moviéndose de izquierda a derecha y así evaluando cada momento los riesgos

Limites WIP: Se define que máximo puede haber 3 tareas en curso, y 2 tareas en fase final, si no se completa el 100% de la tarea, no se puede avanzar a la entrega del siguiente trabajo, y así evitamos la multitarea, estrés de las personas y cuellos de botella

Políticas Explicitas: En esta se define que cada tarea, para pasar al siguiente cuadro, debe de estar totalmente documentada y con sus respectivos entregables.

Como no se cuenta con el personal capacitado para la resolución de incidentes, se debe generar un plan de formación transversal a la migración, se sugiere tener un equipo total de seis personas para la entrega final del proyecto.

Los equipos se van a conformar en grupos de dos personas y estos serán distribuidos así:

2 personas atenderán 2MFA y ZTNA.

2 personas atenderán PAM.

2 personas atenderán el Firewall.

Esta estrategia en pares permite que una persona esté configurando y otro aprendiendo al mismo tiempo, garantizando así que el conocimiento no solo se quede en una persona y así lograr tener habilidades cruzadas.

Este plan de formación busca pasar de tener conocimiento individual a el trabajo colaborativo. El plan de formación será liderado por el arquitecto de integración de ciberseguridad, este deberá de ser un líder servicial, ya que su función no es solamente enseñar, si no dar al equipo las herramientas necesarias para que comprenda la solución integral del producto. A medida que se vaya avanzando, la idea es generar una célula de ciberseguridad unificada, la cual puede atender las diferentes plataformas y así, ir generando un equipo capacitado, el cual pueda apoyar la solución integral de los servicios y mejorar los tiempos de respuesta y solución de incidentes.

Los insumos para este equipo serán los resultados de la matriz de habilidades de Robert Katz, se debe encontrar un equilibrio definido entre:

Habilidades Técnicas: Es el saber hacer, lo que implica un dominio completo de herramientas de ciberseguridad, configurar firewalls perimetrales, arquitectura de posturas de seguridad que garanticen una migración solida operativamente.

Habilidades Humanas: El saber ser y relacionarse desde una comunicación asertiva, con inteligencia emocional que permite negociar cambios, resolver conflictos y liderar equipos de trabajo que los lleve a cumplir los objetivos planteados.

Habilidades Conceptuales: Es conocer y analizar el proyecto de forma global, evaluando el impacto en cada ajuste técnico, más allá de una simple configuración.

En esta célula se busca trabajar bajo el principio de seguridad psicológica, y convirtiendo el error en oportunidad; así si un ingeniero comete un error en alguna de las fases, se analizará como fallo de la plataforma y no como fallo de una persona, buscando fomentar el aprendizaje continuo.

Kanban entonces va a ayudar a la reducción de tiempos de repuesta, visión total del proyecto y sinergia de los equipos de trabajo, convirtiendo así al equipo en administradores de ciberseguridad.

Planeación de la migración

Como ya se tiene un tiempo implementando una cultura de ciberseguridad, pero está separada por el uso de diferentes proveedores, en el proceso de unificación se va a iniciar por la migración de plataforma de mayor prioridad y complejidad, hacia la más “Fácil”, que se realizará hacía el cierre del proyecto.

Este proceso se realizará de la siguiente manera:

Identidad y acceso: Esta es la parte más crítica de la migración ya que se debe conocer quienes usan los servicios e identificar que son las personas correctas, una vez realizado esto se

unificarían las plataformas de ZTNA y 2MFA. Con esta integración ya se conocería quien se conecta, desde donde y que recursos utiliza.

Accesos Privilegiados: Se continua con la plataforma de administración de accesos privilegiados PAM, como ya se sabe quién está en la red, desde donde ingresan y a que ingresan, se van a garantizar esos accesos sin necesidad de conocer que usuario y que privilegios tiene en la plataforma, adicionalmente se tendrá control y monitoreo de la sesión durante la ejecución de las diferentes tareas en los servidores que se encuentran en la plataforma PAM.

Perímetro de Seguridad: Ahora que ya se tienen las plataformas unificadas, se debe garantizar que el uso es el correcto y que no están usando los recursos en otro tipo de actividades no correspondientes a su rol en la compañía, dado esto, se procederá a optimizar el perímetro, garantizando acceso a las plataformas y a los recursos, otorgando un acceso más seguro a internet, ya que hoy en día es un foco de infección. Al ser este el último paso, es el momento en el que el equipo ya conoce la forma de operación y las plataformas, brindando así la tranquilidad de una correcta operación.

Presentación del backlog y roadmap

Para garantizar el éxito de la unificación de las plataformas tecnológicas, se necesita tener una planeación más profunda para la gobernanza del proyecto, por ello se tendrá un backlog de producto al estilo Scrum diseñado para cubrir la complejidad de la migración que se va a llevar a cabo. “Tabla A1”. Esto se complementa con un roadmap visual estructurado como se realiza en Kanban bajo el modelo de flujo de valor (VSM).

Tabla 2. Backlog

Épica	Historia de Usuario / Tarea	Criterios de Aceptación (Definición de Hecho)	Prioridad
Diagnóstico y Auditoría	Como Arquitecto de Seguridad, quiero auditar las políticas actuales de Firewall y cuentas PAM para identificar qué reglas son obsoletas y no deben migrarse.	Inventario documentado de reglas útiles y cuentas activas.	Alta
Selección de Proveedor	Como Líder de Ciberseguridad, quiero evaluar a 3 proveedores mediante un formato RFP para seleccionar la herramienta que integre las 4 soluciones.	Matriz comparativa diligenciada con evaluación de latencia y costos.	Alta
Prueba de Concepto (PoC)	Como Especialista Técnico, quiero desplegar un entorno de pruebas con el proveedor elegido para validar la integración nativa entre 2MFA y ZTNA.	El proveedor demuestra bloqueo automático de un usuario sin 2MFA.	Alta
Diseño de Arquitectura	Como Arquitecto, quiero diseñar el Blueprint de la nueva red unificada para asegurar que cumple con la Arquitectura de Malla (CSMA).	Diagrama de red aprobado por los directivos de TI.	Alta
Plan de Comunicación	Como Scrum Máster, quiero enviar un plan de comunicación a la compañía para informar sobre el cambio en los métodos de acceso y evitar bloqueos masivos.	Correos enviados y manual de usuario final publicado en la intranet.	Media

Migración de Identidad	Como Usuario Final de GTD, quiero usar una única aplicación de 2MFA para acceder de forma sencilla a mis herramientas de trabajo diario.	100% de los usuarios migrados al nuevo token sin interrupción de servicio.	Alta
Despliegue ZTNA	Como Administrador de Red, quiero configurar las políticas de acceso remoto (ZTNA) para reemplazar las antiguas VPNs.	Conexiones remotas cifradas y validadas con latencia menor a 100ms.	Alta
Homologación PAM	Como Administrador de Servidores, quiero que mis accesos privilegiados estén en la nueva bóveda unificada para tener grabación de sesiones en un solo lugar.	Cuentas críticas migradas y directorio activo sincronizado.	Alta
Migración Firewall	Como Especialista de Seguridad, quiero traducir y migrar las reglas del perímetro al nuevo NGFW para unificar el monitoreo del tráfico.	El tráfico fluye por el nuevo firewall sin caída de aplicaciones core.	Alta
Capacitación Técnica	Como Miembro de la Célula de Ciberseguridad, quiero recibir entrenamiento en la nueva consola para administrar todas las tecnologías sin depender de terceros.	Todos los miembros de la célula aprueban la prueba de uso de la plataforma.	Media
Pruebas de Seguridad	Como Líder de Ciberseguridad, quiero ejecutar un Pentesting (Test de penetración) en la nueva arquitectura para garantizar que no hay vulnerabilidades post-migración.	Informe de vulnerabilidades entregado con cero hallazgos críticos.	Media
Apagado Legacy (Sunset)	Como Patrocinador del Proyecto, quiero apagar los servidores antiguos y cancelar las 4 licencias anteriores	Certificados de cancelación de	Baja

	para consolidar el ahorro financiero (ROI).		contratos previos y equipos apagados.

Nota: Autoría propia.

Estas herramientas permitirán transformar la naturaleza intangible de la ciberseguridad en un proceso medible, transparente y alineado con los objetivos estratégicos de la compañía.

Tabla 3. Roadmap 12 semanas

Fase / Sprint	**Semanas**	**Actividades de Implementación (El "Cómo")**	**Entregables y Artefactos**	**Métricas de Calidad**
Sprint 0: Inicio y Diagnóstico	1-2	Auditoría técnica de configuraciones actuales. Ejecución de proceso de negociación y selección de proveedor único.	Acta de Inicio, Matriz de Selección de Vendor.	% de reglas de firewall obsoletas identificadas.
Sprint 1: Identidad y Acceso	3-4	Configuración de la consola centralizada. Despliegue de la nueva plataforma de 2MFA y ZTNA en ambiente piloto.	Blueprint de Arquitectura, Prototipo de acceso remoto.	Tiempo de respuesta del token (< 3 segundos).
Sprint 2: Validación PoC	5-6	Ejecución de Pruebas de Concepto (PoC) con la Célula de Ciberseguridad para validar la interoperabilidad.	Informe de resultados PoC y ajustes técnicos.	Grado de ajuste a requisitos explícitos (100%).
Sprint 3: Privilegios Críticos	7-9	Migración escalonada de las cuentas con mayores privilegios de GTD a la	Log de migración de	% de cuentas críticas bajo

		plataforma de PAM integrada.	cuentas, Bóveda PAM activa.	control y grabación.
Sprint 4: Perímetro y Red	10-11	Consolidación de la seguridad perimetral (Next-Gen Firewall) y traducción de reglas de seguridad.	Reporte de conectividad y seguridad perimetral.	Reducción de latencia en el tráfico de red.
Sprint 5: Cierre y Transferencia	12	Apagado definitivo de plataformas antiguas. Capacitación final bajo el método de Peer Coaching.	Manuales operativos, Matriz de trazabilidad final.	100% de técnicos con test de uso aprobado.

Nota: Autoría propia.

Documentación y aprendizaje continuo

Como el sistema es altamente robusto se debe registrar cada paso de la migración, no solo se debe documentar como algo técnico, sino con el paso a paso de cómo se realizan los procesos de migración de cada plataforma y como el proceso de integración debe ir enfocado a mostrar la Gobernanza y el control de calidad.

Registro de errores: Se deben de identificar las fallas de integración y como se fueron resolviendo cada uno de ellos con el fin de ayudar el aprendizaje de la célula de ciberseguridad.

Tabla 4. Registro de errores

ID Error	Fase / Sprint	Descripción del hallazgo	Impacto (Negocio/Operación)	Acción Correctiva (Solución)	Lección Aprendida
ERR-01	Sprint 1: Identidad	Falla en sincronización entre AD y 2MFA.	Alto: Bloqueo total del acceso para el grupo piloto (Indisponibilidad del servicio).	Ajuste de certificados SSL y apertura de puertos.	Validar compatibilidad de versiones de TLS antes de migrar.
ERR-02	Sprint 3: Privilegios	Latencia >200ms en grabación de sesiones PAM.	Medio: Degradación de la experiencia de usuario y riesgo de pérdida de logs de auditoría.	Optimización de ancho de banda en el clúster PAM.	Las sesiones de video requieren priorización de tráfico (QoS).

Nota: Autoría propia. Muestra de un posible error y su impacto en la operación

Matriz de trazabilidad: Asegurar que cada requisito de ciberseguridad identificado en la plataforma original se cumpla en la nueva integración de servicios, esta nos dará la seguridad de que el proyecto cumpla con el alcance y la calidad definidos en el proyecto, su propósito es que ningún requisito se pierda durante la migración de la plataforma.

Tabla 5. Matriz de trazabilidad

ID Req.	Requisito de Seguridad Original	Categoría (ZTNA/PAM/FW)	Implementación en Nueva Plataforma	Estado de Validación	Métrica de Calidad Asociada
REQ-01	Autenticación de doble factor para acceso remoto.	Identidad	Módulo MFA Nativo con notificaciones Push.	Validado	Tiempo de respuesta < 3 seg.
REQ-02	Grabación de sesiones de usuarios con privilegios.	PAM	Bóveda centralizada con logs inalterables.	Validado	Ajuste al 100% de la política de auditoría.
REQ-03	Segmentación de tráfico por rol de usuario.	Perímetro	Reglas de Firewall basadas en ID de usuario (Identity-based).	Pendiente	Grado de modularidad de las reglas.

Nota: Autoría propia. Esta es una muestra de los resultados al evaluar cada requisito.

Conclusiones

La integración de plataformas en GTD no es solo un cambio de software, sino una evolución hacia un modelo de liderazgo Servicial donde la tecnología apoya al factor humano.

El uso de sprints y métricas de calidad permiten la tangibilidad de un proyecto de naturaleza intangible, reduciendo la incertidumbre para los patrocinadores.

La conformación de una célula de ciberseguridad de 4 personas garantiza la resiliencia operativa y la eliminación de los silos de conocimiento que afectaban a la compañía.

Referencias

Kanban y Scrum, dos metodologías ágiles diferentes. (2021, abril 12). Universidad Internacional de La Rioja. https://www.unir.net/revista/ingenieria/kanban-scrum-metodologias-agiles/

NIST Special Publication 800-63B. (s/f). Nist.gov. Recuperado el 15 de abril de 2026, de https://pages.nist.gov/800-63-3/sp800-63b.html

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. National Institute of Standards and Technology.

Sepúlveda, J. (2026). Módulo 2: Roles y Responsabilidades. Seminario Gestión de Proyectos y Habilidades Gerenciales. Corporación Universitaria Remington

(S/f-a). Paloaltonetworks.com. Recuperado el 15 de abril de 2026, de https://www.paloaltonetworks.com/cyberpedia/what-is-a-next-generation-firewall

(S/f-b). Gartner.com. Recuperado el 15 de abril de 2026, de https://www.gartner.com/en/documents/4017326

What is cybersecurity mesh? (s/f). Fortinet. Recuperado el 15 de abril de 2026, de https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity-mesh

Zero Trust security and strategy. (s/f). Microsoft.com. Recuperado el 15 de abril de 2026, de https://www.microsoft.com/en-us/security/business/zero-trust