



Estudio de Ciberseguridad y Riesgos Informáticos

Empresa Ejemplo, S.L. · Informe de ejemplo con datos ficticios

ECRI-20260810-0142

Cliente: Empresa Ejemplo, S.L.

Jornada de trabajo: 4 de agosto de 2026

Emitido: 10 de agosto de 2026

1 Resumen ejecutivo

Veredicto. La organización sostiene la operativa diaria con un equipo de sistemas reducido y sin incidencias relevantes conocidas, pero el riesgo se concentra en dos frentes: la red no está segmentada, de modo que los sistemas que sostienen la expedición conviven con las oficinas, y la recuperación ante un cifrado masivo no está respaldada por ninguna prueba. Ninguno de los dos exige una inversión elevada para reducirse de forma sustancial.

Datos del mapeo de red

Recuentos obtenidos directamente del escaneo y mapeo de la red. [ESCANEO](#)

96

Hosts activos detectados

5

Segmentos de red identificados

238

Servicios expuestos en red interna

7

Sistemas fuera de soporte

4

Protocolos inseguros en uso

11

Paneles de administración accesibles

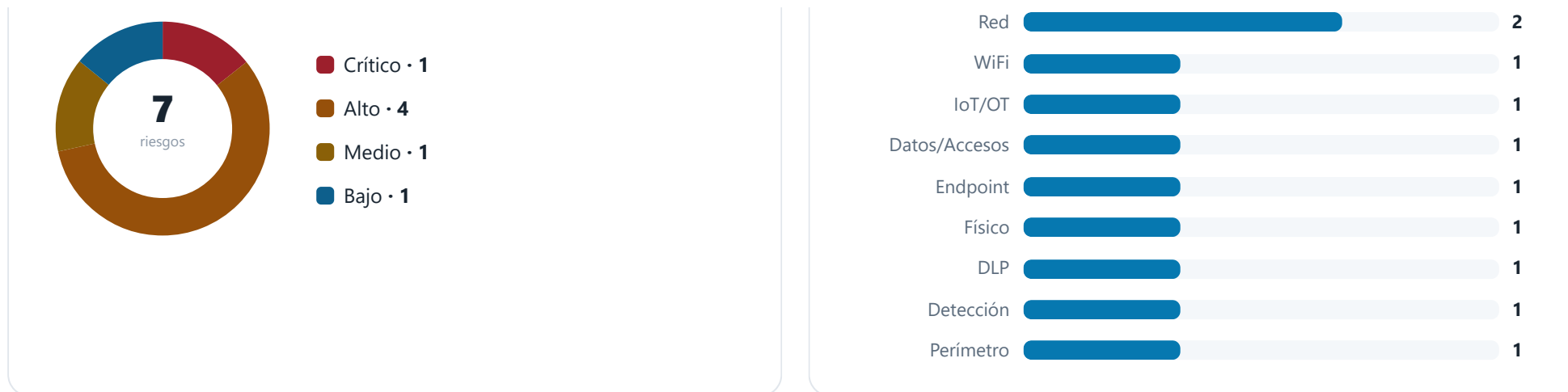
Riesgos y hallazgos

Riesgos por severidad

Hallazgos por categoría

Identidad/AD 3

Servicios 3



Continuidad de negocio

Objetivos y medios declarados por la organización. **ENTREVISTA** Contrastarlos mediante una prueba de restauración documentada es la primera actuación recomendada.

RTO DECLARADO 4 h Sin prueba que lo respalde	RPO DECLARADO 24 h Copia diaria nocturna	ÚLTIMA PRUEBA DE RESTAURACIÓN Nunca Recomendado: trimestral	COPIA AISLADA O INMUTABLE No Copias en NAS de la misma red
--	--	---	--

Madurez de los controles básicos

Valoración por dominio en cuatro niveles: **Inexistente** · **Inicial** · **Parcial** · **Establecido**. Cada dominio indica de qué actividad del estudio procede la valoración.

Copias de seguridad y recuperación		Inicial	ENTREVISTA
Gestión de identidades y accesos		Inicial	ENTREVISTA
Segmentación de red		Inexistente	ESCANEEO

Actualizaciones y ciclo de vida		Inicial	ESCANEAO
Protección del puesto de trabajo		Parcial	ENTREVISTA
Registro de eventos y detección		Inexistente	ENTREVISTA
Seguridad del perímetro		Parcial	ESCANEAO
Red inalámbrica		Inicial	ESCANEAO
Seguridad física de TI		Inicial	INSPECCIÓN
Concienciación y procedimientos		Inicial	ENTREVISTA

Observaciones verificadas

Comprobado de forma directa durante el estudio, no inferido de la documentación:

F1

Alta

Desde un único puesto de oficina se alcanzan los servidores de gestión, los terminales del almacén y la videovigilancia, sin filtrado intermedio.

F4

Crítica

El panel de administración del switch principal admite las credenciales de fábrica desde cualquier puesto de la red.

F2

Crítica

El servidor de gestión de almacén funciona sobre una versión sin soporte del fabricante.

F12

Media

El rack de comunicaciones está en el pasillo de muelles, abierto y con puertos libres activos.

Accesos rápidos por apartado

- Alcance y fuentes →
- Arquitectura de red →
- Inventario de activos →
- Matriz de riesgos →

Qué se ha hecho en la jornada y de dónde sale cada dato.

Topología y segmentos identificados en el mapeo.

Equipos localizados, con sus hallazgos y severidad.

Escenarios de riesgo por impacto y probabilidad.

Hallazgos técnicos →

Detalle de cada hallazgo, filtrable por categoría.

Tratamiento →

Proyectos de tratamiento con sus actuaciones y verificaciones de implantación.

Evidencias →

Fragmentos de escaneo y notas de entrevista e inspección.

Conclusiones

El riesgo no proviene de un fallo aislado sino de la combinación de una red sin segmentar con una recuperación no probada: cualquier incidente que entre por el acceso remoto tiene recorrido libre hasta los servidores de gestión, hasta los terminales del almacén y hasta las propias copias.

El impacto se mide en días de expedición detenida, no solo en información perdida. Los sistemas que sostienen la preparación y el etiquetado de pedidos están en el mismo espacio de red que las oficinas, y dos de ellos ya no reciben actualizaciones del fabricante.

Cuatro de las ocho actuaciones propuestas son de esfuerzo bajo y se pueden abordar de inmediato: copia aislada, doble factor en el acceso remoto, credenciales de la electrónica de red y cierre del rack. Reducen los dos escenarios de mayor impacto sin necesidad de proyecto previo.

La segmentación de la red es la única actuación que requiere planificación real, y es la que sostiene la mejora a medio plazo del resto de escenarios.

2 Alcance y fuentes de información

El estudio se apoya en tres fuentes de información complementarias, que permiten contrastar lo que la organización tiene definido con lo que la red muestra en la práctica. Cada hallazgo del informe indica de qué fuente procede.

ENTREVISTA

Entrevista con el responsable de IT

Recorrido sobre la organización de los sistemas, la estrategia de copias y su verificación, la gestión de identidades y accesos remotos, el mantenimiento del parque y los procedimientos ante incidentes.

ESCANEEO Escaneo y mapeo de la red

Descubrimiento de equipos y servicios activos, identificación de versiones y protocolos en uso, y comprobación del alcance real entre los distintos grupos de equipos.

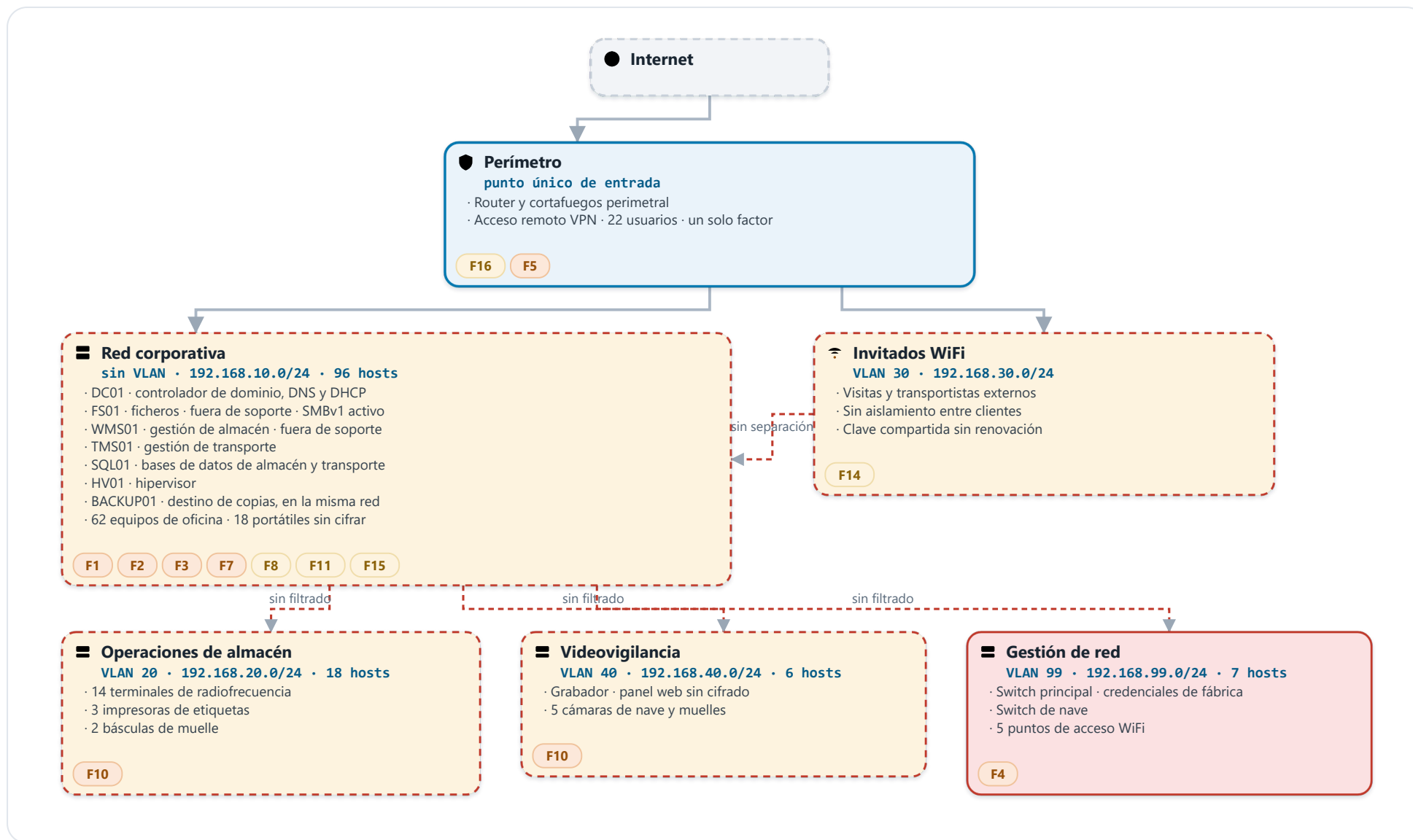
INSPECCIÓN Inspección remota de las instalaciones

Revisión asistida del emplazamiento y el estado del equipamiento de red, el control de acceso a los espacios técnicos y las condiciones de la instalación.

Los datos que la organización aporta en entrevista figuran identificados como declarados; el resto procede de comprobación directa sobre la red o las instalaciones. La distinción se mantiene a lo largo de todo el informe.

3 Arquitectura de red

Topología reconstruida a partir del mapeo de la red. El alcance obtenido desde un puesto de oficina abarca, en la práctica, la totalidad de la instalación: no se encontró filtrado entre las oficinas, los servidores de gestión, los sistemas de almacén y la videovigilancia. El catálogo detallado de equipos está en el apartado siguiente.



Cada caja es un **segmento de red** y enumera dentro los equipos que contiene. Las etiquetas azules son los hallazgos que afectan a ese segmento: púlsalas para ir a su ficha. :: Arrastra cualquier segmento para reordenar el esquema.

 Perímetro
 Segmento con hallazgos abiertos
 Segmento crítico
 --- Alcance sin filtrado entre segmentos

Segmentos identificados

VLAN	NOMBRE	RANGO	FUNCIÓN	ESTADO
sin VLAN	Red corporativa	192.168.10.0/24	Puestos de oficina, servidores de gestión y controlador de dominio en el mismo dominio de difusión	Sin segmentar
VLAN 20	Operaciones de almacén	192.168.20.0/24	Terminales de radiofrecuencia, impresoras de etiquetas y básculas de muelle	Accesible desde corporativa
VLAN 30	Invitados WiFi	192.168.30.0/24	Visitas y transportistas externos en zona de muelles	Sin aislamiento de cliente
VLAN 40	Videovigilancia	192.168.40.0/24	Grabador y cámaras de nave y muelles	Accesible desde corporativa
VLAN 99	Gestión	192.168.99.0/24	Administración de switches, puntos de acceso y router perimetral	Accesible desde corporativa

4

Inventario de activos

▼

Activos localizados durante el estudio, agrupados por función. Pulsa la etiqueta de un hallazgo para ir a su ficha. Pulsa el título de un grupo para plegarlo.

TIPO	ACTIVO	OBSERVACIÓN	HALLAZGOS	SEVERIDAD
▼ PERÍMETRO Y ELECTRÓNICA DE RED · 5				
Router / FW	Router perimetral	Firmware con actualizaciones pendientes · concentra la VPN	F16	Media
Switch	Switch principal 48 puertos	Panel web con credenciales de fábrica	F4	Crítica
Switch	Switch de nave 24 puertos	Sin VLAN configuradas	F1	Alta
WiFi	Puntos de acceso de nave (4)	Cobertura de terminales de radiofrecuencia	F10	Alta
WiFi	Punto de acceso de oficinas	Red de invitados sin aislamiento	F14	Media
▼ SERVIDORES · 7				
Servidor	DC01 · Controlador de dominio	AD, DNS y DHCP	F6 F8	Media
Servidor	FS01 · Servidor de ficheros	Windows Server 2012 R2 · SMBv1 activo	F2 F3	Crítica
Servidor	WMS01 · Gestión de almacén	Windows Server 2012 R2 · sostiene la preparación de pedidos	F2 F11	Crítica
Servidor	TMS01 · Gestión de transporte	Escritorio remoto abierto a toda la red	F11	Media
Servidor	SQL01 · Base de datos	Bases de datos de almacén y transporte	F11	Media
Servidor	HV01 · Hipervisor	Administración en la misma red que los puestos	F1	Alta
NAS	BACKUP01 · Destino de copias	En la misma red · sin copia inmutable	F7	Alta
▼ PUESTOS Y ACCESOS · 3				
Equipos	62 equipos de sobremesa	Oficinas y administración de almacén	F15	Media

TIPO	ACTIVO	OBSERVACIÓN	HALLAZGOS	SEVERIDAD
Portátiles	18 portátiles	Comercial y tráfico · sin cifrado de disco generalizado	F15	Media
Accesos	22 usuarios con VPN	Delegaciones y comercial · un solo factor	F5	Alta
▼ OPERACIONES DE ALMACÉN · 4				
Terminales	14 terminales de radiofrecuencia	Preparación de pedidos · sin actualizaciones recientes	F10	Alta
Impresoras	3 impresoras de etiquetas	Etiquetado de expediciones	F10	Alta
Básculas	Básculas de muelle (2)	Pesaje y control de carga	F10	Media
CCTV	Grabador de videovigilancia	Panel web sin cifrado · alcanzable desde oficinas	F10 F4	Alta
▼ INSTALACIONES · 2				
Rack	Rack de comunicaciones	Pasillo oficinas-muelles · sin cierre · puertos libres	F12	Media
SAI	SAI de rack	Operativo · sin monitorización remota	—	Baja

5 Matriz de riesgos

Clasificación de **escenarios de riesgo** por **impacto potencial para el negocio** y **probabilidad de explotación**. Cada escenario está habilitado por uno o varios hallazgos técnicos.

Escala cualitativa MAGERIT: MB (muy bajo/a) · B (bajo/a) · M (medio/a) · A (alto/a) · MA (muy alto/a)

PROBABILIDAD →

		Muy baja (MB)	Baja (B)	Media (M)	Alta (A)	Muy alta (MA)
↑ IMPACTO	Muy alto (MA)			⌵ R-02	⌵ R-01	
	Alto (A)			⌵ R-03	⌵ R-04	
	Medio (M)			⌵ R-06	⌵ R-05	
	Bajo (B)		⌵ R-07			
	Muy bajo (MB)					

NIVEL DE RIESGO:

Crítico

Alto

Medio

Bajo

⌵ Arrastra cada ficha a otra celda si, al releer el análisis, crees que su probabilidad o impacto deberían reclasificarse — el cambio se recuerda en este navegador. Pasa el ratón sobre una ficha para ver el resumen del escenario sin salir de la matriz.

Inventario de riesgos

Cada riesgo es un escenario de lo que podría llegar a ocurrir, construido a partir de los hallazgos que lo hacen posible. Marca un hallazgo como remediado para ver cómo baja la probabilidad residual del escenario y cómo se mueve su ficha en la matriz.

REF	ESCENARIO DE RIESGO	HALLAZGOS	IMPACTO	PROB.	ZONA	COMPROBACIÓN DE REMEDIACIÓN
R-01	Cifrado masivo de sistemas con recuperación no garantizada ▾ Ver análisis DESCRIPCIÓN DEL ESCENARIO Un cifrado que entre por el acceso remoto o por un servidor sin soporte se propaga por una red sin segmentar, alcanza la gestión de almacén y de transporte, y llega también al destino de las copias, que está en la misma red y nunca se ha probado. La expedición diaria quedaría detenida durante un plazo que hoy no se puede estimar, porque no hay evidencia de que la restauración funcione. REQUISITOS PARA SU MATERIALIZACIÓN 1. Obtener una credencial válida de acceso remoto, que solo pide un factor, o alcanzar uno de los servidores sin soporte del fabricante. 2. Moverse hasta el segmento de servidores: inmediato, al no existir segmentación ni filtrado intermedio. 3. Alcanzar el destino de copias, accesible desde la misma red y sin copia aislada que quede fuera del alcance del cifrado. RECOMENDACIÓN • PT-1 · Continuidad y recuperación • PT-2 · Control de accesos e identidad • PT-4 · Mantenimiento y ciclo de vida	F2 F3 F7 F5	Muy alto	Alta	Crítico	☐ F2 remediado ☐ F3 remediado ☐ F7 remediado ☐ F5 remediado 0/4 hallazgos remediados

REF	ESCENARIO DE RIESGO	HALLAZGOS	IMPACTO	PROB.	ZONA	COMPROBACIÓN DE REMEDIACIÓN
R-02	Parada de la operativa de almacén y expediciones ▾ Ver análisis DESCRIPCIÓN DEL ESCENARIO Un incidente que empiece en un equipo de oficina alcanza los terminales de radiofrecuencia, las impresoras de etiquetas y las básculas de muelle, que comparten espacio de red con la gestión. Sin ellos no se puede preparar ni etiquetar pedidos: el impacto es la detención de la expedición, con incumplimiento de los plazos comprometidos con los clientes. REQUISITOS PARA SU MATERIALIZACIÓN 1. Un incidente en cualquier equipo de la red de oficina. 2. Alcance a 192.168.20.0/24 desde ese equipo, hoy disponible sin ningún filtrado. 3. Terminales, impresoras y básculas con servicios de gestión abiertos y sin actualizaciones recientes del fabricante. RECOMENDACIÓN • PT-3 · Arquitectura de red y aislamiento • PT-4 · Mantenimiento y ciclo de vida	F1 F10	Muy alto	Media	Alto	☐ F1 remediado ☐ F10 remediado 0/2 hallazgos remediados

REF	ESCENARIO DE RIESGO	HALLAZGOS	IMPACTO	PROB.	ZONA	COMPROBACIÓN DE REMEDIACIÓN
R-03	Toma de control del dominio desde un puesto de oficina ▾ Ver análisis DESCRIPCIÓN DEL ESCENARIO Partiendo de un puesto cualquiera, la combinación de electrónica con credenciales de fábrica, ausencia de bloqueo por intentos fallidos, escritorio remoto abierto entre equipos y un grupo de administradores más amplio de lo necesario permite escalar hasta el control del dominio. REQUISITOS PARA SU MATERIALIZACIÓN - Acceso a un puesto de la red, físico o remoto. - Obtener una credencial con permisos elevados: la falta de bloqueo por intentos fallidos permite probar de forma sistemática, y existen cuentas compartidas de turno. - Saltar entre equipos mediante el escritorio remoto, accesible sin restricción de origen. - Un grupo de administradores de dominio amplio, que multiplica las cuentas cuyo compromiso basta para culminar el escenario. RECOMENDACIÓN PT-2 · Control de accesos e identidad PT-3 · Arquitectura de red y aislamiento PT-4 · Mantenimiento y ciclo de vida	F4 F6 F8 F11	Alto	Media	Alto	☐ F4 remediado ☐ F6 remediado ☐ F8 remediado ☐ F11 remediado 0/4 hallazgos remediados

REF	ESCENARIO DE RIESGO	HALLAZGOS	IMPACTO	PROB.	ZONA	COMPROBACIÓN DE REMEDIACIÓN
R-04	Acceso remoto no autorizado con credenciales legítimas ▾ Ver análisis DESCRIPCIÓN DEL ESCENARIO Una credencial de dominio obtenida fuera de la organización, por reutilización en un servicio ajeno o por engaño al usuario, da entrada directa a la red interna. Con 22 accesos remotos activos entre delegaciones y personal comercial, no hay segundo factor que lo frene, ni segmentación que limite el alcance, ni registro que lo evidencie. REQUISITOS PARA SU MATERIALIZACIÓN 1. Una credencial de dominio válida obtenida fuera de la organización. 2. Ausencia de segundo factor en el acceso remoto. 3. Ninguna restricción por origen ni registro centralizado que permita detectar el acceso. RECOMENDACIÓN • <u>PT-2 · Control de accesos e identidad</u>	<u>F5 F16</u>	Alto	Alta	Alto	☐ F5 remediado ☐ F16 remediado 0/2 hallazgos remediados

REF	ESCENARIO DE RIESGO	HALLAZGOS	IMPACTO	PROB.	ZONA	COMPROBACIÓN DE REMEDIACIÓN
R-05	Incidente que permanece sin detectar durante semanas ▾ Ver análisis DESCRIPCIÓN DEL ESCENARIO Sin registro centralizado ni alertas, la organización solo se enteraría de que algo ocurre cuando el efecto sea visible: una parada de expediciones o una reclamación de un cliente. Para entonces los registros locales se habrán sobrescrito y no será posible reconstruir lo sucedido ni acreditarlo ante terceros. REQUISITOS PARA SU MATERIALIZACIÓN 1. Actividad que no produzca un efecto inmediatamente visible para los usuarios. 2. Ausencia de recolección centralizada de registros y de alertas configuradas. 3. Retención local por defecto, que se sobrescribe de forma cíclica antes de que nadie la revise. RECOMENDACIÓN • PT-5 · Visibilidad y protección de la información	<u>F9 F14</u>	Medio	Alta	Alto	☐ F9 remediado ☐ F14 remediado 0/2 hallazgos remediados

REF	ESCENARIO DE RIESGO	HALLAZGOS	IMPACTO	PROB.	ZONA	COMPROBACIÓN DE REMEDIACIÓN
R-06	Fuga de información comercial y de clientes	F13 F15	Medio	Media	Medio	☐ F13 remediado ☐ F15 remediado 0/2 hallazgos remediados
	▾ Ver análisis DESCRIPCIÓN DEL ESCENARIO Listados de clientes, rutas y tarifas salen de la organización en portátiles sin cifrar y en memorias USB sin control ni registro. Puede ocurrir por descuido o de forma deliberada, y en ninguno de los dos casos quedaría constancia de qué información ha salido. REQUISITOS PARA SU MATERIALIZACIÓN 1. Información comercial o de clientes almacenada en un portátil sin cifrar o copiada a un soporte extraíble. 2. Pérdida, robo o salida deliberada del soporte. 3. Ausencia de registro que permita determinar qué información ha salido. RECOMENDACIÓN • PT-5 · Visibilidad y protección de la información					

REF	ESCENARIO DE RIESGO	HALLAZGOS	IMPACTO	PROB.	ZONA	COMPROBACIÓN DE REMEDIACIÓN
R-07	Manipulación física de la electrónica de red ▾ Ver análisis DESCRIPCIÓN DEL ESCENARIO El rack accesible en el pasillo que comunica oficinas y muelles permite conectar un equipo no autorizado a la red o interrumpir el servicio sin superar ningún control lógico. Requiere presencia física, lo que limita la probabilidad, pero por esa zona circula a diario personal externo. REQUISITOS PARA SU MATERIALIZACIÓN 1. Acceso físico a la zona de paso donde se ubica el rack, hoy de tránsito común para personal externo. 2. Rack sin cierre operativo. 3. Puertos de red activos y disponibles en el switch. RECOMENDACIÓN • PT-5 · Visibilidad y protección de la información	F12	Bajo	Baja	Bajo	☐ F12 remediado 0/1 hallazgos remediados

6

Hallazgos técnicos

Cada ficha indica su categoría, su severidad y la actividad del estudio de la que procede. Usa los filtros para acotar por categoría.

Todas las categorías

Identidad/AD

Servicios

Red

WiFi

IoT/OT

Datos/Accesos

Endpoint

Físico

DLP

Detección

Perímetro

Índice de hallazgos

REF ↕	HALLAZGO ↕	CATEGORÍA ↕	ORIGEN ↕	SEVERIDAD ↕
F1	Red corporativa sin segmentación	Red	ESCANEEO	Alta
F2	Servidores con sistema operativo fuera de soporte	Servicios	ESCANEEO	Crítica
F3	Protocolo de compartición obsoleto habilitado	Servicios	ESCANEEO	Alta
F4	Electrónica de red con credenciales de fábrica	Red	ESCANEEO	Crítica
F5	Acceso remoto sin segundo factor de autenticación	Identidad/AD	ENTREVISTA	Alta
F6	Política de contraseñas sin bloqueo por intentos fallidos	Identidad/AD	ENTREVISTA	Media
F7	Copias de seguridad sin copia aislada ni prueba de restauración	Datos/Accesos	ENTREVISTA	Alta
F8	Exceso de cuentas con privilegios de administración de dominio	Identidad/AD	ENTREVISTA	Media
F9	Sin registro centralizado de eventos	Detección	ENTREVISTA	Media
F10	Sistemas de almacén y videovigilancia en la misma red que la gestión	IoT/OT	ESCANEEO	Alta
F11	Escritorio remoto accesible entre todos los equipos internos	Servicios	ESCANEEO	Media
F12	Rack de comunicaciones sin cierre en zona de paso	Físico	INSPECCIÓN	Media
F13	Sin control de uso de dispositivos extraíbles	DLP	ENTREVISTA	Baja
F14	Red WiFi de invitados sin aislamiento entre clientes	WiFi	ESCANEEO	Media
F15	Portátiles sin cifrado de disco	Endpoint	ENTREVISTA	Media

REF ↑	HALLAZGO ↑	CATEGORÍA ↑	ORIGEN ↑	SEVERIDAD ↑
F16	Router perimetral con firmware desactualizado	Perímetro	ESCANEAO	Media

Detalle por hallazgo

F1 Alta ESCANEAO Red

Red corporativa sin segmentación

▼ Descripción

Oficinas, sistemas de almacén, videovigilancia y servidores comparten el mismo espacio de red, sin ningún control que limite quién puede comunicarse con quién. Un problema en cualquier punto tiene recorrido libre hasta los servidores que sostienen la operativa.

▼ Detalle técnico

El segmento 192.168.10.0/24 reúne 96 hosts: puestos de oficina, servidores de gestión de almacén y transporte, controlador de dominio, hipervisor y las direcciones de gestión de la electrónica de red. Desde un puesto de oficina se alcanzan además 192.168.20.0/24 (operaciones de almacén), 192.168.40.0/24 (videovigilancia) y 192.168.99.0/24 (gestión) sin ningún filtrado intermedio.

▼ Comprobación

Desde un puesto de oficina, comprobar el alcance a tres destinos: dirección de gestión del switch, un terminal de radiofrecuencia del almacén y la consola del hipervisor. Una vez remediado, los tres deben quedar inalcanzables desde ese origen.

▼ Remediación

Separar la red en VLAN por función (servidores, oficinas, operaciones de almacén, videovigilancia, gestión e invitados) y aplicar listas de control entre ellas. Priorizar el aislamiento de operaciones y del segmento de servidores.

F2

Crítica

ESCANEO

Servicios

Servidores con sistema operativo fuera de soporte

▼ Descripción

El servidor de ficheros y el que sostiene la gestión de almacén funcionan sobre una versión que el fabricante ya no actualiza. Las vulnerabilidades que se publiquen a partir de ahora no tendrán corrección disponible.

▼ Detalle técnico

FS01 (192.168.10.24) y WMS01 (192.168.10.26) responden como Windows Server 2012 R2 6.3.9600, sin soporte del fabricante desde octubre de 2023. El escaneo identifica 7 equipos en situación equivalente, incluidos dos puestos de administración del almacén.

▼ Comprobación

Inventariar versión y fecha de fin de soporte de cada servidor y contrastarla con el calendario del fabricante. Una vez remediado, ningún sistema en producción debe figurar fuera de soporte.

▼ Remediación

Planificar la migración a versiones con soporte, empezando por el servidor de gestión de almacén por su papel en la operativa diaria. Mientras se ejecuta, restringir el acceso a esos servidores por origen y reforzar la vigilancia sobre ellos.

F3

Alta

ESCANEEO

Servicios

Protocolo de compartición obsoleto habilitado

▼ Descripción

El servidor de ficheros sigue aceptando la primera versión del protocolo de compartición de Windows, retirada por el fabricante, y no exige firma del tráfico. Es el mecanismo que han usado las familias de cifrado masivo de propagación automática.

▼ Detalle técnico

FS01 (192.168.10.24) negocia SMBv1 además de SMBv2 y SMBv3. El escaneo devuelve *message_signing: enabled but not required*, por lo que la firma del tráfico es opcional.

▼ Comprobación

En el servidor, ejecutar `Get-SmbServerConfiguration | Select EnableSMB1Protocol, RequireSecuritySignature`. El resultado correcto es False y True respectivamente.

▼ Remediación

Deshabilitar SMBv1 y exigir firma del tráfico por directiva de grupo, comprobando antes qué equipos antiguos, terminales de almacén o impresoras de etiquetas dependen de la versión obsoleta.

F4

Crítica

ESCANEEO

Red

Electrónica de red con credenciales de fábrica

▼ Descripción

El panel de administración del switch principal es accesible desde cualquier puesto de la red y mantiene el usuario y la contraseña que traía de fábrica. No hace falta ninguna credencial corporativa para reconfigurar la red.

▼ Detalle técnico

El switch principal (192.168.10.2) publica interfaz web en el puerto 80 y consola Telnet en el 23, ambos sin cifrado. El panel acepta las credenciales por defecto del fabricante. Se localizan 11 paneles de administración accesibles en total, incluidos los del grabador de videovigilancia y los puntos de acceso del almacén.

▼ Comprobación

Desde un puesto de oficina, intentar acceder al panel del switch. Una vez remediado, las credenciales de fábrica deben ser rechazadas y el panel no debe responder desde fuera de la VLAN de gestión.

▼ Remediación

Cambiar las credenciales de todos los paneles localizados, deshabilitar la consola sin cifrado, mover la administración a una VLAN de gestión separada y limitar el acceso a las direcciones del equipo de sistemas.

F5

Alta

ENTREVISTA

Identidad/AD

Acceso remoto sin segundo factor de autenticación

▼ Descripción

El acceso remoto a la red se resuelve únicamente con usuario y contraseña de dominio. Una sola credencial filtrada basta para entrar en una red que además no está segmentada.

▼ Detalle técnico

Se declaran unos 22 usuarios con acceso VPN entre personal comercial, tráfico y delegaciones, todos con autenticación de un solo factor contra el directorio. No hay restricción por origen ni registro específico de los accesos remotos.

▼ Comprobación

Autenticar en la VPN con unas credenciales válidas: el sistema debe solicitar un segundo factor antes de conceder acceso a la red.

▼ Remediación

Activar segundo factor en el acceso remoto para todos los usuarios, empezando por las cuentas con permisos administrativos y por los accesos de delegaciones.

Política de contraseñas sin bloqueo por intentos fallidos

▼ Descripción

La directiva de dominio no bloquea temporalmente una cuenta tras varios errores seguidos, lo que permite probar contraseñas de forma sistemática sin ninguna traba.

▼ Detalle técnico

La directiva de dominio mantiene una longitud mínima de 8 caracteres sin requisitos adicionales y el umbral de bloqueo de cuenta está a 0, es decir, desactivado. Existen cuentas de uso compartido en el turno de almacén.

▼ Comprobación

Ejecutar net accounts en un controlador de dominio y revisar la directiva aplicada. El umbral de bloqueo debe ser distinto de 0 y la longitud mínima acorde a la política acordada.

▼ Remediación

Fijar bloqueo temporal tras varios intentos fallidos, elevar la longitud mínima, contrastar las contraseñas nuevas contra listas de credenciales filtradas y sustituir las cuentas compartidas de turno por cuentas nominales.

Copias de seguridad sin copia aislada ni prueba de restauración

▼ Descripción

Las copias se guardan en un equipo accesible desde la misma red que los servidores, no existe ninguna copia fuera de línea y nunca se ha probado una restauración completa. El objetivo de recuperación declarado no está respaldado por ninguna evidencia.

▼ Detalle técnico

Destino de copias: NAS BACKUP01 (192.168.10.40), en el mismo segmento que los servidores. Frecuencia diaria en ventana nocturna, incluyendo las bases de datos de gestión de almacén y de transporte. Sin copia inmutable ni fuera de línea. RTO declarado 4 h y RPO declarado 24 h, sin registro de pruebas de restauración.

▼ Comprobación

Ejecutar una restauración completa del servidor de gestión de almacén sobre un entorno aislado y medir el tiempo hasta recuperar el servicio. Ese tiempo medido es el RTO real y debe contrastarse con las 4 h declaradas.

▼ Remediación

Incorporar una copia aislada, fuera de línea o inmutable, y programar una prueba de restauración documentada al menos trimestral, priorizando los sistemas que sostienen la expedición diaria.

Exceso de cuentas con privilegios de administración de dominio

▼ Descripción

Hay más cuentas con control total del dominio de las que el tamaño del equipo justifica, y una de ellas es compartida. Comprometer cualquiera equivale a controlar el dominio, y lo compartido no se puede atribuir a nadie.

▼ Detalle técnico

Se declaran 7 cuentas en el grupo de administradores del dominio para un equipo de IT de 2 personas. El grupo incluye cuentas de servicio de la aplicación de transporte, una cuenta compartida por el equipo y una cuenta de un proveedor externo.

▼ Comprobación

Ejecutar `Get-ADGroupMember "Domain Admins"` y revisar el resultado. Solo deben figurar las cuentas nominales estrictamente necesarias, sin cuentas compartidas ni de proveedores con acceso permanente.

▼ Remediación

Reducir el grupo al mínimo, dar a cada administrador una cuenta nominal separada de su cuenta de usuario habitual, retirar la cuenta compartida y conceder el acceso de proveedores solo durante la intervención.

Sin registro centralizado de eventos

▼ Descripción

Los registros quedan solo en cada equipo, con la retención por defecto y sin que nadie los revise. Un incidente puede pasar semanas sin detectarse y, cuando se detecte, no habrá rastro suficiente para reconstruir lo ocurrido.

▼ Detalle técnico

No existe recolector de registros ni sistema de correlación. La retención es la local por defecto de cada equipo, que se sobrescribe de forma cíclica. No hay ninguna alerta configurada, tampoco sobre el uso de cuentas administrativas ni sobre los accesos remotos.

▼ Comprobación

Comprobar que los eventos de inicio de sesión de los controladores de dominio llegan al recolector y que existe una alerta que se dispara al usar una cuenta administrativa.

▼ Remediación

Centralizar al menos los registros de controladores de dominio, servidores de gestión, perímetro y accesos remotos, con retención mínima de 6 meses y un conjunto reducido de alertas sobre uso administrativo.

F10**Alta****ESCANE0**

IoT/OT

Sistemas de almacén y videovigilancia en la misma red que la gestión

▼ Descripción

Los terminales de radiofrecuencia, las impresoras de etiquetas, las básculas de muelle y el grabador de videovigilancia conviven con los servidores de gestión y son alcanzables desde cualquier puesto. Son equipos que rara vez reciben actualizaciones y que, comprometidos, permanecen dentro de la red sin que nadie los vigile.

▼ Detalle técnico

Desde 192.168.10.180 se alcanzan los 18 hosts de 192.168.20.0/24 (terminales de radiofrecuencia, impresoras de etiquetas y básculas) y los 6 de 192.168.40.0/24 (videovigilancia). El grabador expone panel de administración web sin cifrado y varios terminales mantienen servicios de gestión abiertos sin autenticación.

▼ Comprobación

Desde un puesto de oficina, comprobar el alcance a los terminales del almacén y al grabador de videovigilancia. Una vez remediado, no deben ser alcanzables salvo desde los equipos expresamente autorizados.

▼ Remediación

Llevar operaciones de almacén y videovigilancia a VLAN propias y permitir únicamente los flujos estrictamente necesarios hacia los servidores de gestión, desde equipos identificados.

Escritorio remoto accesible entre todos los equipos internos

▼ Descripción

Cualquier equipo de la red puede abrir sesión remota contra cualquier servidor. Con unas credenciales válidas se puede ir saltando de equipo en equipo hasta alcanzar los sistemas que sostienen la operativa.

▼ Detalle técnico

El puerto 3389/tcp responde en FS01 (192.168.10.24), SQL01 (192.168.10.25), WMS01 (192.168.10.26) y TMS01 (192.168.10.30), alcanzable desde cualquier puesto del segmento, sin restricción por origen ni pasarela intermedia.

▼ Comprobación

Desde un puesto de usuario, comprobar si el puerto 3389 de los servidores responde. Una vez remediado, solo debe responder desde los equipos de administración designados.

▼ Remediación

Restringir el escritorio remoto por origen mediante el cortafuegos del sistema y concentrar el acceso administrativo en equipos designados.

F12

Media

INSPECCIÓN

Físico

Rack de comunicaciones sin cierre en zona de paso

▼ Descripción

El armario que concentra la electrónica de red está en un pasillo de acceso común junto a la zona de muelles, abierto y con puertos libres activos. Permite conectar un equipo no autorizado o dejar la red sin servicio sin superar ningún control lógico.

▼ Detalle técnico

La inspección remota sitúa el rack principal en el pasillo que comunica oficinas con la zona de muelles, de acceso común para personal propio y transportistas externos. La puerta está abierta y sin cerradura operativa. Se observan 8 puertos libres accesibles y activos en el switch. El SAI está operativo pero sin monitorización remota.

▼ Comprobación

Inspección visual: el rack debe estar cerrado con llave, con registro de accesos, y los puertos no utilizados desactivados en la configuración del switch.

▼ Remediación

Instalar cierre con llave y registro de acceso, desactivar en el switch los puertos que no estén en uso y valorar el traslado del rack a un espacio sin tránsito de personal externo.

F13

Baja

ENTREVISTA

DLP

Sin control de uso de dispositivos extraíbles

▼ Descripción

No hay ninguna directiva que limite el uso de memorias USB ni registro de lo que se copia en ellas. Los listados de clientes, rutas y tarifas pueden salir de la organización sin dejar rastro.

▼ Detalle técnico

No existe directiva de control de soportes extraíbles en el dominio ni registro de eventos de escritura en ellos. El intercambio de documentación con clientes y transportistas se realiza por correo y por memorias USB.

▼ Comprobación

Conectar un dispositivo extraíble en un puesto y verificar que se aplica la directiva prevista y que la operación queda registrada.

▼ Remediación

Definir una directiva de uso de soportes extraíbles, dejando permiso de escritura solo donde el proceso lo exija, y habilitar el registro de esos eventos.

F14

Media

ESCANE0

WiFi

Red WiFi de invitados sin aislamiento entre clientes

▼ Descripción

Los dispositivos conectados a la red de invitados se ven entre sí y la red no está realmente separada del direccionamiento interno. La usan visitas y transportistas externos en la zona de muelles, por lo que la rotación de dispositivos ajenos es alta.

▼ Detalle técnico

La red de invitados (192.168.30.0/24) no tiene activado el aislamiento de clientes. Los dispositivos asociados se alcanzan entre sí y el segmento no está separado del resto del direccionamiento interno mediante filtrado. La clave de acceso es compartida y no se renueva.

▼ Comprobación

Con dos dispositivos conectados a la red de invitados, comprobar que no se alcanzan entre sí ni llegan a ninguna dirección de la red interna.

▼ Remediación

Activar el aislamiento de clientes, llevar la red de invitados a una VLAN sin acceso a la red interna y renovar la clave de acceso de forma periódica.

F15

Media

ENTREVISTA

Endpoint

Portátiles sin cifrado de disco

▼ Descripción

Los equipos que salen de las instalaciones no tienen el disco cifrado de forma generalizada. La pérdida o el robo de uno de ellos expone directamente la información que contenga, con las implicaciones de protección de datos que eso conlleva.

▼ Detalle técnico

De los 18 portátiles declarados, repartidos entre personal comercial y responsables de tráfico, el cifrado de disco no está activado de forma generalizada ni gestionado desde una consola central, por lo que tampoco hay custodia centralizada de las claves de recuperación.

▼ Comprobación

Ejecutar `manage-bde -status` en cada portátil. Todos los volúmenes de sistema deben aparecer cifrados y la consola central debe custodiar la clave de recuperación.

▼ Remediación

Activar el cifrado de disco en todos los portátiles y en los equipos que salgan de las instalaciones, con custodia centralizada de las claves de recuperación.

F16

Media

ESCANE0

Perímetro

Router perimetral con firmware desactualizado

▼ Descripción

El equipo que conecta la organización con el exterior tiene actualizaciones de seguridad pendientes. Es el primer elemento expuesto y por él pasan además los accesos remotos de delegaciones y personal comercial.

▼ Detalle técnico

El equipo perimetral presenta una versión de firmware con actualizaciones de seguridad publicadas por el fabricante y pendientes de aplicar. Es también el concentrador del acceso remoto.

▼ Comprobación

Comparar la versión de firmware instalada con la última publicada por el fabricante. Una vez remediado, deben coincidir o estar dentro de la ventana de mantenimiento acordada.

▼ Remediación

Aplicar la actualización de firmware en ventana planificada y establecer una revisión periódica de versiones del equipamiento perimetral.

7 Proyectos de tratamiento de riesgos

Las recomendaciones se agrupan en proyectos de tratamiento: cada proyecto persigue un objetivo de riesgo concreto y reúne las actuaciones que lo hacen posible. Cada actuación indica los hallazgos que cierra y las verificaciones que permiten dar por implantada la medida.

PT-1 Continuidad y recuperación

Plazo: Inmediato

Esfuerzo: Bajo

Objetivo. Garantizar que la organización puede volver a operar en un plazo conocido y acreditado tras un incidente que afecte a los sistemas de gestión.

Riesgos que trata: **R-01** · 2 actuaciones

▼ 1. Copia aislada e inmutable

Incorporar una copia fuera de línea o inmutable que quede fuera del alcance de un cifrado que se propague por la red de producción.

HALLAZGOS QUE CIERRA

F7

VERIFICACIÓN DE IMPLANTACIÓN

- Existe al menos una copia que no es accesible ni modificable desde la red de producción.
- Simulado el borrado de la copia en el NAS, se conserva una copia reciente recuperable.
- La ventana entre copias cumple el RPO comprometido.

▼ 2. Prueba de restauración documentada

Restaurar los sistemas de gestión de almacén y transporte sobre un entorno aislado y dejar constancia del tiempo real hasta recuperar el servicio.

HALLAZGOS QUE CIERRA

F7

VERIFICACIÓN DE IMPLANTACIÓN

- Existe acta de restauración con fecha, alcance y tiempo medido hasta servicio.
- El tiempo medido se ha contrastado con el RTO comprometido y, si no lo cumple, se ha revisado el objetivo o los medios.
- La prueba está planificada con periodicidad al menos trimestral.

PT-2 Control de accesos e identidad

Plazo: 1 mes

Esfuerzo: Bajo

Objetivo. Que una única credencial filtrada no sea suficiente para entrar en la red ni para escalar privilegios dentro del dominio.

Riesgos que trata: **R-04 R-03 R-01** · 3 actuaciones

▼ 1. Doble factor en el acceso remoto

Activar segundo factor en los accesos remotos de delegaciones y personal comercial, empezando por las cuentas con permisos administrativos.

HALLAZGOS QUE CIERRA

F5

VERIFICACIÓN DE IMPLANTACIÓN

- La autenticación con credenciales válidas solicita un segundo factor.
- Los accesos remotos activos están cubiertos, sin excepciones permanentes.
- Las cuentas con permisos administrativos no pueden acceder sin segundo factor.

▼ 2. Higiene de cuentas privilegiadas

Reducir el grupo de administradores de dominio, separar cuentas nominales de cuentas de usuario, retirar la cuenta compartida de turno y acotar el acceso de proveedores.

HALLAZGOS QUE CIERRA

F8

VERIFICACIÓN DE IMPLANTACIÓN

- El grupo de administradores del dominio contiene solo cuentas nominales necesarias.
- No queda ninguna cuenta compartida ni cuenta de proveedor con acceso permanente.
- Cada administrador dispone de una cuenta separada de su cuenta de usuario habitual.

▼ 3. Endurecimiento de la política de contraseñas

Fijar bloqueo temporal por intentos fallidos, elevar la longitud mínima y sustituir las cuentas compartidas de turno por cuentas nominales.

HALLAZGOS QUE CIERRA

F6

VERIFICACIÓN DE IMPLANTACIÓN

- La directiva de dominio aplica un umbral de bloqueo por intentos fallidos distinto de 0.
- La longitud mínima y los requisitos de contraseña se corresponden con la política acordada.
- El personal de almacén accede con cuentas nominales, no compartidas por turno.

PT-3 Arquitectura de red y aislamiento

Plazo: 1-3 meses

Esfuerzo: Medio

Objetivo. Limitar el recorrido de un incidente para que un problema en oficinas no alcance los sistemas que sostienen la expedición.

Riesgos que trata: **R-02 R-03** · 4 actuaciones

▼ 1. Segmentación en VLAN por función

Separar servidores, oficinas, operaciones de almacén, videovigilancia, gestión e invitados, con reglas de filtrado entre segmentos y una matriz de flujos documentada.

HALLAZGOS QUE CIERRA

F1

VERIFICACIÓN DE IMPLANTACIÓN

- Desde un puesto de oficina no se alcanzan la gestión de la electrónica de red, los terminales de almacén ni la videovigilancia.
- Existe matriz de flujos permitidos entre segmentos, aprobada y aplicada.
- La operativa de almacén sigue funcionando con los flujos autorizados.

▼ 2. Gestión segura de la electrónica de red

Cambiar las credenciales de todos los paneles de administración, deshabilitar los protocolos sin cifrado y trasladar la administración a la VLAN de gestión.

HALLAZGOS QUE CIERRA

F4

VERIFICACIÓN DE IMPLANTACIÓN

- Ningún panel de administración acepta las credenciales de fábrica.
- Los paneles no responden desde fuera de la VLAN de gestión.
- Las consolas sin cifrado están deshabilitadas en todos los equipos.

▼ 3. Aislamiento de la red de invitados

Activar el aislamiento entre clientes, separar la red de invitados del direccionamiento interno y establecer una renovación periódica de la clave.

HALLAZGOS QUE CIERRA

F14

VERIFICACIÓN DE IMPLANTACIÓN

- Dos dispositivos conectados a la red de invitados no se alcanzan entre sí.
- Desde la red de invitados no se alcanza ninguna dirección de la red interna.
- Existe procedimiento de renovación periódica de la clave de acceso.

▼ 4. Restricción del acceso remoto interno

Limitar el escritorio remoto por origen y concentrar el acceso administrativo en equipos designados.

HALLAZGOS QUE CIERRA

F11

VERIFICACIÓN DE IMPLANTACIÓN

- El puerto de escritorio remoto de los servidores no responde desde puestos de usuario.
- El acceso administrativo solo es posible desde los equipos designados.

PT-4 Mantenimiento y ciclo de vida

Plazo: 3-6 meses

Esfuerzo: Medio

Objetivo. Eliminar de la red los sistemas y protocolos que ya no reciben correcciones del fabricante, y evitar que vuelvan a acumularse.

Riesgos que trata: R-01 R-02 R-03 · 4 actuaciones

▼ 1. Migración de sistemas fuera de soporte

Planificar y ejecutar la migración de los sistemas sin soporte, priorizando el servidor de gestión de almacén por su papel en la operativa diaria.

HALLAZGOS QUE CIERRA

F2

VERIFICACIÓN DE IMPLANTACIÓN

- Ningún sistema en producción figura fuera de soporte del fabricante.
- El servidor de gestión de almacén opera sobre una versión con soporte vigente.
- Existe inventario de versiones con fecha de fin de soporte y revisión periódica.

▼ 2. Retirada de protocolos obsoletos

Deshabilitar el protocolo de compartición obsoleto y exigir firma del tráfico, tras resolver las dependencias de equipos antiguos e impresoras de etiquetas.

HALLAZGOS QUE CIERRA

F3

VERIFICACIÓN DE IMPLANTACIÓN

- La consulta de configuración del servidor devuelve el protocolo obsoleto deshabilitado y la firma de tráfico como obligatoria.
- Los terminales e impresoras que dependían del protocolo antiguo funcionan con la configuración nueva.

▼ 3. Actualización del equipamiento perimetral

Aplicar las actualizaciones pendientes en el equipo perimetral y establecer una revisión periódica de versiones.

HALLAZGOS QUE CIERRA

F16

VERIFICACIÓN DE IMPLANTACIÓN

- La versión instalada coincide con la última publicada por el fabricante o está dentro de la ventana de mantenimiento acordada.
- Existe procedimiento documentado de revisión periódica de versiones.

▼ 4. Endurecimiento de equipos de almacén y videovigilancia

Cambiar credenciales por defecto, cerrar los servicios de gestión innecesarios y aplicar las actualizaciones que ofrezca el fabricante en terminales, impresoras, básculas y grabador.

HALLAZGOS QUE CIERRA

F10

VERIFICACIÓN DE IMPLANTACIÓN

- Ningún equipo de almacén o videovigilancia mantiene credenciales por defecto.
- Los paneles de administración de esos equipos no son accesibles desde oficinas.
- Existe inventario de estos equipos con versión de firmware y responsable.

PT-5 Visibilidad y protección de la información

Plazo: 1-3 meses

Esfuerzo: Medio

Objetivo. Poder detectar un incidente antes de que su efecto sea visible, y evitar que la información salga de la organización sin control.

Riesgos que trata: R-05 R-06 R-07 · 4 actuaciones

▼ 1. Registro centralizado y alertas

Recoger los registros de controladores de dominio, servidores de gestión, perímetro y accesos remotos, con retención suficiente y un conjunto reducido de alertas.

HALLAZGOS QUE CIERRA

F9

VERIFICACIÓN DE IMPLANTACIÓN

- Los eventos de inicio de sesión de los controladores de dominio llegan al recolector.
- La retención efectiva es de al menos 6 meses.
- Una prueba controlada de uso de cuenta administrativa dispara la alerta prevista.

▼ 2. Cifrado del puesto de trabajo

Activar el cifrado de disco en los portátiles de comercial y tráfico, con custodia centralizada de las claves de recuperación.

HALLAZGOS QUE CIERRA

F15

VERIFICACIÓN DE IMPLANTACIÓN

- Todos los portátiles muestran el volumen de sistema cifrado.
- La consola central custodia la clave de recuperación de cada equipo.
- El cifrado se aplica automáticamente a los equipos nuevos.

▼ 3. Control de soportes extraíbles

Definir una directiva de uso de soportes extraíbles, con permiso de escritura solo donde el proceso lo exija, y habilitar el registro de esos eventos.

HALLAZGOS QUE CIERRA

F13

VERIFICACIÓN DE IMPLANTACIÓN

- La conexión de un soporte extraíble aplica la directiva prevista.
- Las operaciones de escritura en soportes extraíbles quedan registradas.
- Las excepciones están documentadas y asociadas a una necesidad concreta.

▼ 4. Aseguramiento físico del equipamiento de red

Instalar cierre y registro de acceso en el rack, desactivar los puertos libres y valorar su traslado fuera de la zona de tránsito externo.

HALLAZGOS QUE CIERRA

F12

VERIFICACIÓN DE IMPLANTACIÓN

- El rack permanece cerrado con llave y existe registro de accesos.
- Los puertos no utilizados están desactivados en la configuración del switch.
- Se ha valorado y decidido documentalmente el emplazamiento definitivo del rack.

El plazo y el esfuerzo son estimaciones relativas para ordenar la ejecución, no un presupuesto. Las verificaciones están redactadas como comprobaciones observables, de modo que puedan usarse como criterio de cierre de cada actuación.

8 Evidencias

Fragmentos representativos de lo obtenido en cada actividad: salidas del escaneo, datos recogidos en la entrevista y notas de la inspección remota. Se omiten los ficheros completos y cualquier dato que no sea necesario para sostener el hallazgo.

ESCANEADO Sistema fuera de soporte y SMBv1 en el servidor de ficheros F2 F3

```
Host: 192.168.10.24 (FS01)
OS fingerprint : Windows Server 2012 R2 Standard 6.3.9600
445/tcp open  microsoft-ds
    smb-protocols : SMBv1 (habilitado), SMBv2, SMBv3
    smb-security  : message_signing: enabled but not required
139/tcp open  netbios-ssn
```

ESCANEEO Panel de administración del switch principal F4

```
Host: 192.168.10.2 (switch principal)
80/tcp  open  http    Web management interface
http-title  : Switch Management Console
http-auth   : credenciales de fábrica aceptadas
23/tcp  open  telnet  (protocolo sin cifrado)
```

ESCANEEO Alcance desde un único punto de conexión de oficina F1 F10

```
Origen: 192.168.10.180 (puesto de oficina)
Alcanzables sin filtrado intermedio:
192.168.10.0/24  96 hosts  (puestos, servidores, AD, hipervisor)
192.168.20.0/24  18 hosts  (terminales RF, impresoras de etiquetas, básculas)
192.168.40.0/24   6 hosts  (grabador y cámaras)
192.168.99.0/24   7 hosts  (gestión de electrónica de red)
Grabador 192.168.40.10 : 80/tcp panel web sin cifrado
```

ESCANEEO Escritorio remoto accesible entre equipos internos F11

```
3389/tcp open  ms-wbt-server  192.168.10.24  (FS01)
3389/tcp open  ms-wbt-server  192.168.10.25  (SQL01)
3389/tcp open  ms-wbt-server  192.168.10.26  (WMS01)
3389/tcp open  ms-wbt-server  192.168.10.30  (TMS01)
Alcanzables desde cualquier puesto del segmento, sin restricción por origen.
```

ENTREVISTA Esquema de copias recogido en entrevista F7

Destino : NAS BACKUP01, 192.168.10.40 (misma red que los servidores)
Alcance : ficheros + bases de datos de almacén y transporte
Frecuencia : diaria, ventana nocturna
Copia fuera de línea o inmutable : no
Última restauración completa probada : sin registro
RTO declarado : 4 h · RPO declarado : 24 h

INSPECCIÓN Inspección remota del rack de comunicaciones F12

Ubicación : pasillo de comunicación entre oficinas y zona de muelles
Tránsito : personal propio y transportistas externos
Cierre : puerta abierta, sin cerradura operativa
Puertos : 8 puertos libres accesibles y activos en el switch
Entorno : SAI operativo, sin monitorización remota