LOGICALIS

Business and technology working as one

BU Seguridad

Retos GDPR

LOGICALIS Security

Resumen del Reglamento

Estrategia de seguridad tecnológica centralizada en prevenir brechas de seguridad basadas en "State of Art".

1 Protección de los datos

- Perímetro del tratamiento
- Período del tiempo de retención
- Limitar acceso y datos recogidos

2 Seguridad del tratamiento

- Trazabilidad de los datos
- Prevención de fugas
- Proteger la identidad de los usuarios y tratamiento de datos
- Protección de las aplicaciones

3 Notificación en 72h

- Descripción de la violación de los datos
- Consecuencias y medidas adoptadas
- Plan definido de respuesta ante incidentes

GDPR

4 Evaluación continua

- Gestión de riesgo de información e impacto
- Security by design
- Reforzar detección continua amenazas

5 Concienciación

- Cultura de seguridad
- Concienciación ciberseguridad

LOGICALIS
Business and technology working as one

Aproximación Seguridad Logicalis

Servicio de Adecuación a la GDPR

Análisis GAP

- Assessment Tecnológico

Diagnóstico de la situación actual frente a marcos normativos en materia de seguridad

Medidas Tecnológicas

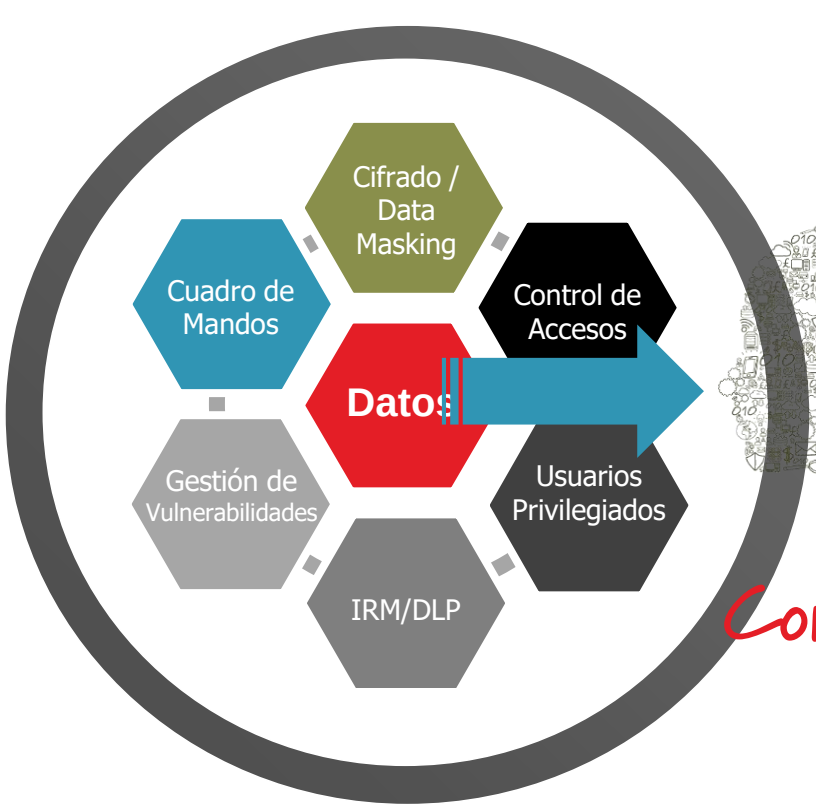
- Plan de Acción Tecnológico
- Análisis y definición de soluciones
- Implantación y adecuación tecnológica

Servicios Gestionados

- Soporte correctivo, preventivo y evolutivo
- Servicios Avanzados de Seguridad
- SOC

LOGICALIS
Business and technology working as one

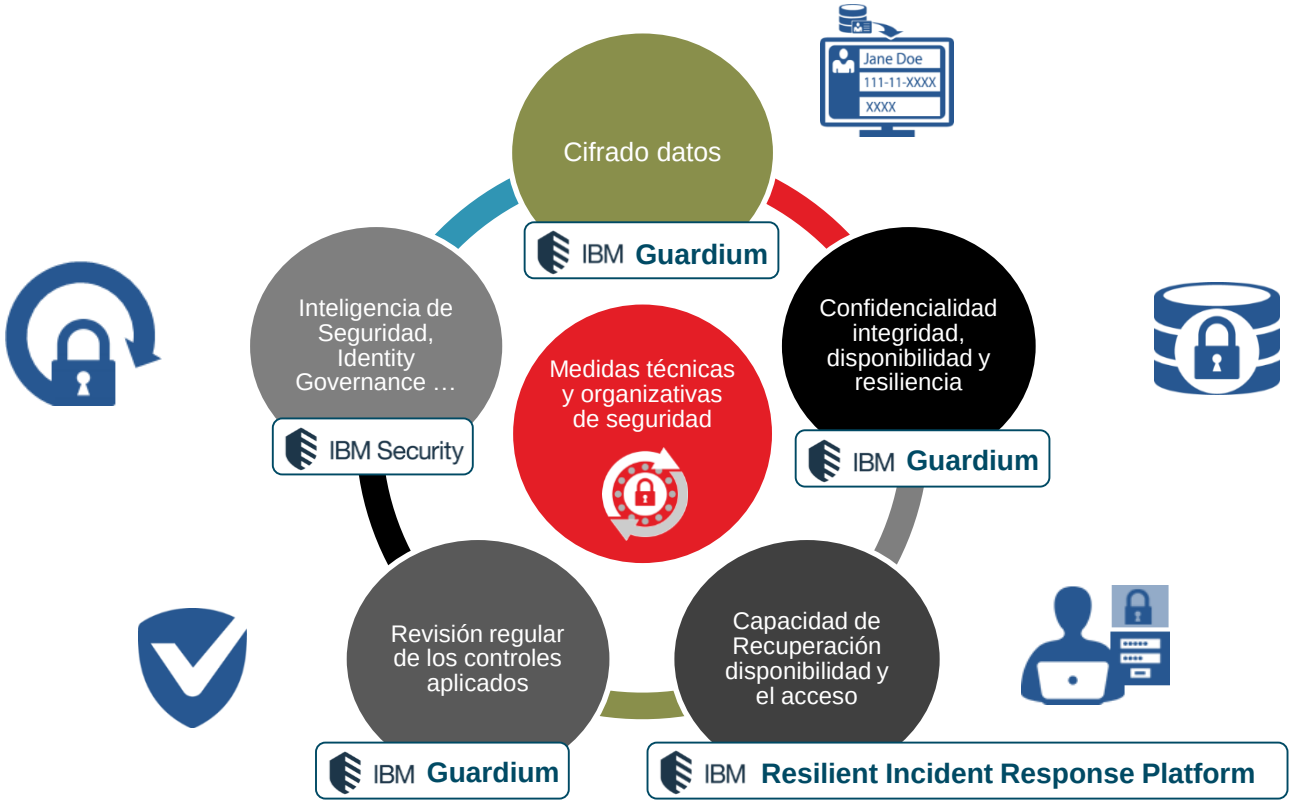
Medidas Tecnológicas



Concienciación

LOGICALIS
Business and technology working as one

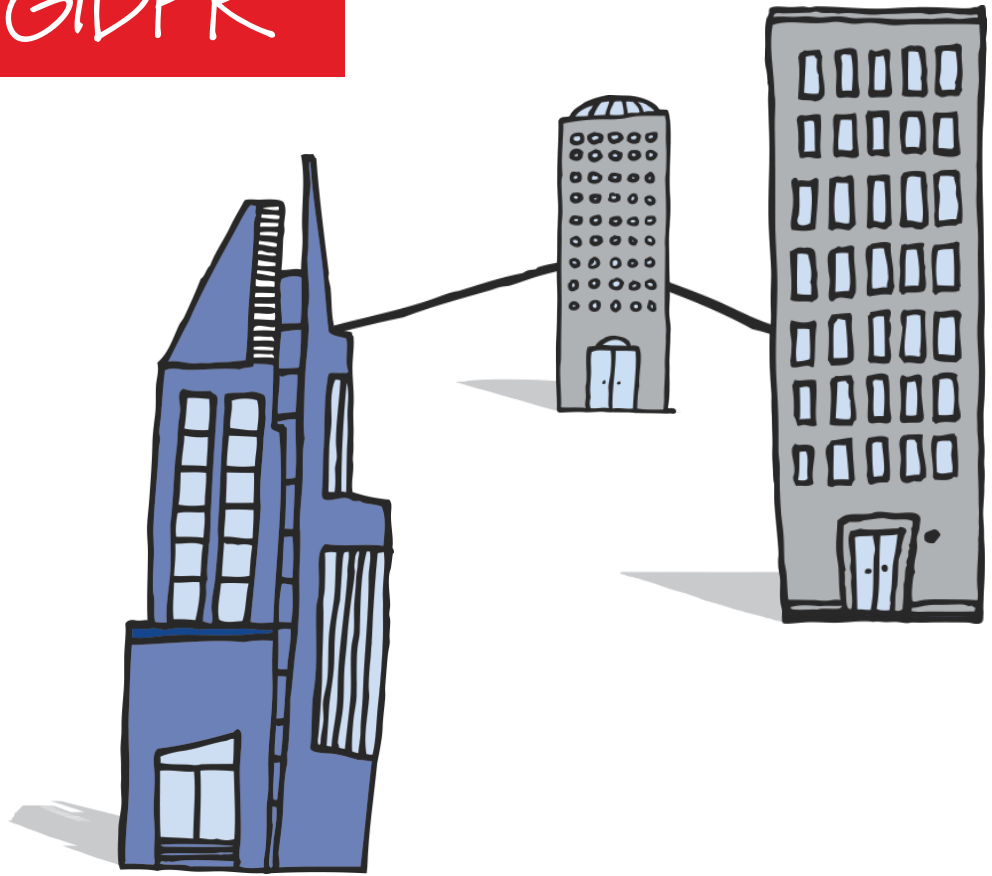
IBM Security GDPR Privacy



LOGICALIS
Business and technology working as one

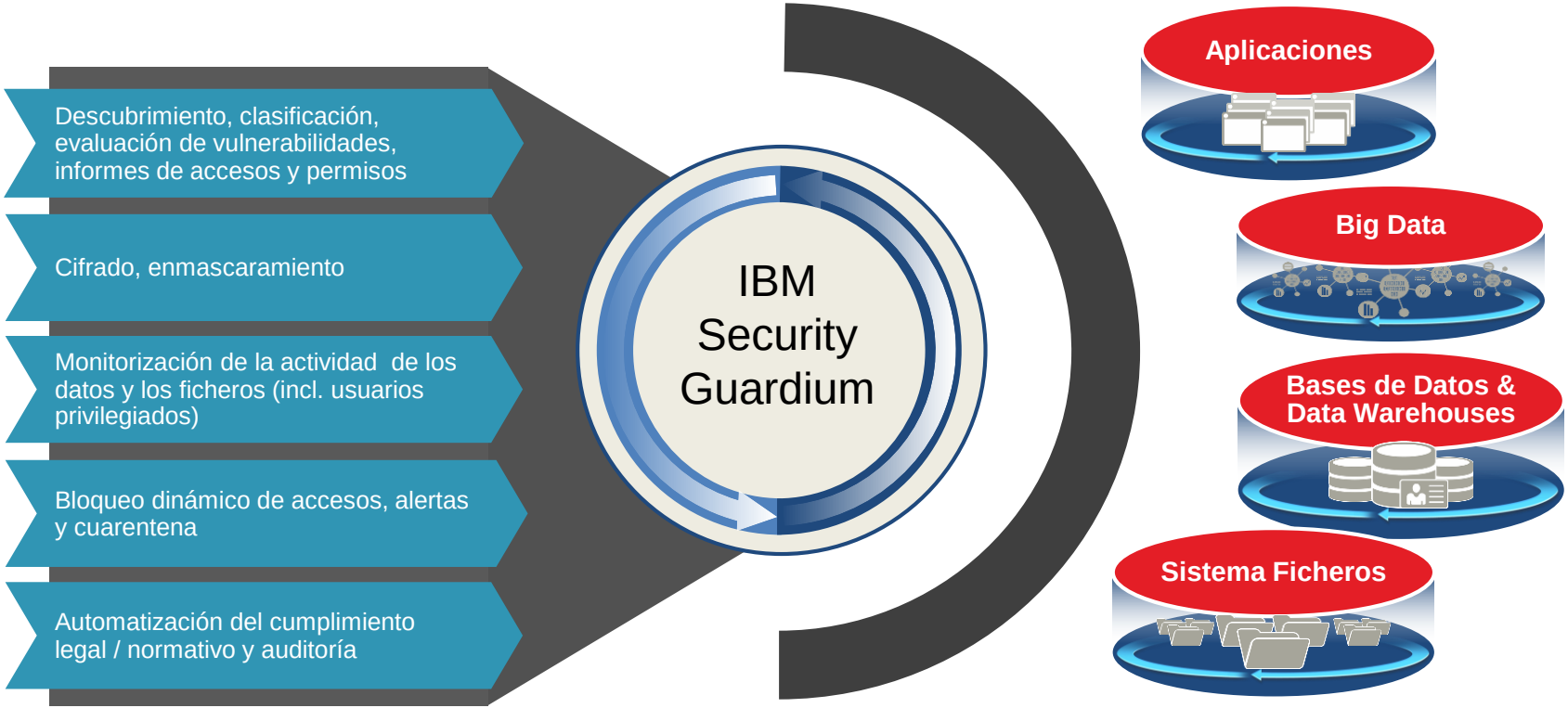
Soluciones GDPR

IBM



LOGICALIS
Business and technology working as one

Data Protection



Aproximación por fases

1

DESCUBRIMIENTO
Descubrir y clasificar los activos y sistemas con datos personales

Guardium GDPR Accelerator

Identificar vulnerabilidades

Guardium Vulnerability Assessment

2

DISEÑO
Definir políticas de Seguridad por diseño

Guardium Data **Protection**

Implementar controles de privacidad y protección

TRANSFORMACIÓN

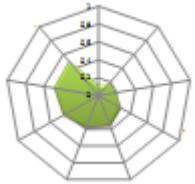
3

Guardium Data Protection

4

Monitorizar el acceso a datos personales dentro de la operativa de seguridad

OPERACIÓN



Guardium Data Protection

Demostrar el cumplimiento mediante el registro de accesos a datos personales y pistas de auditoría

5

CONFORMIDAD

Guardium GDPR Accelerator

LOGICALIS
Business and technology working as one

Data Protection. Ejemplos

Dónde están mis datos

Escaneo de vulnerabilidades

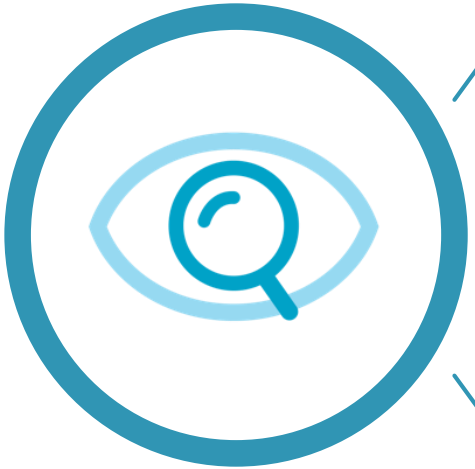
Monitorización y Auditoría

Guardium GDPR Accelerator

LOGICALIS
Business and technology working as one

Data Protection. Ejemplos (I)

Dónde están mis datos



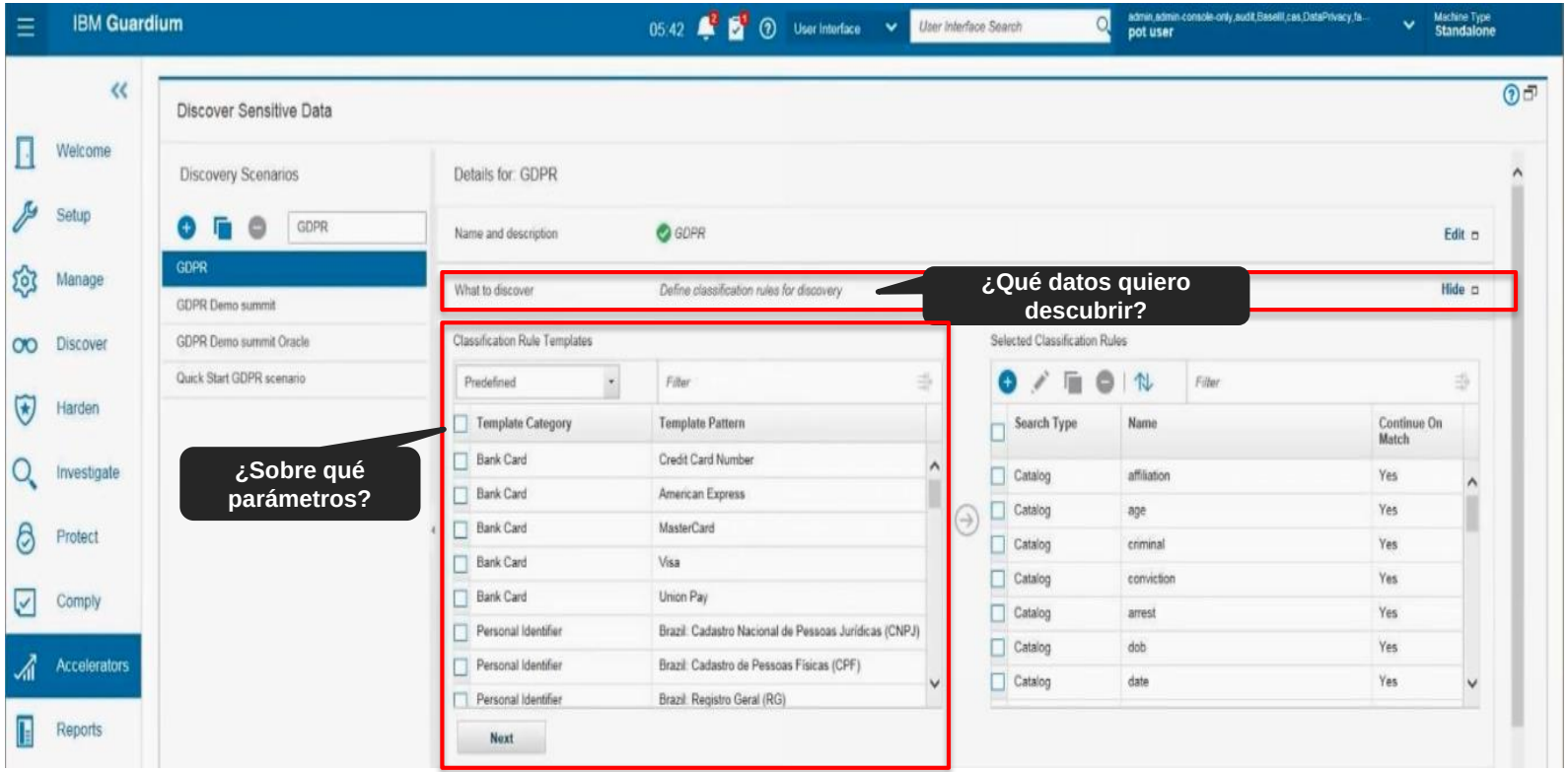
Soluciones al Desafío de Inventario

Descubrimiento de Activos de Base de Datos

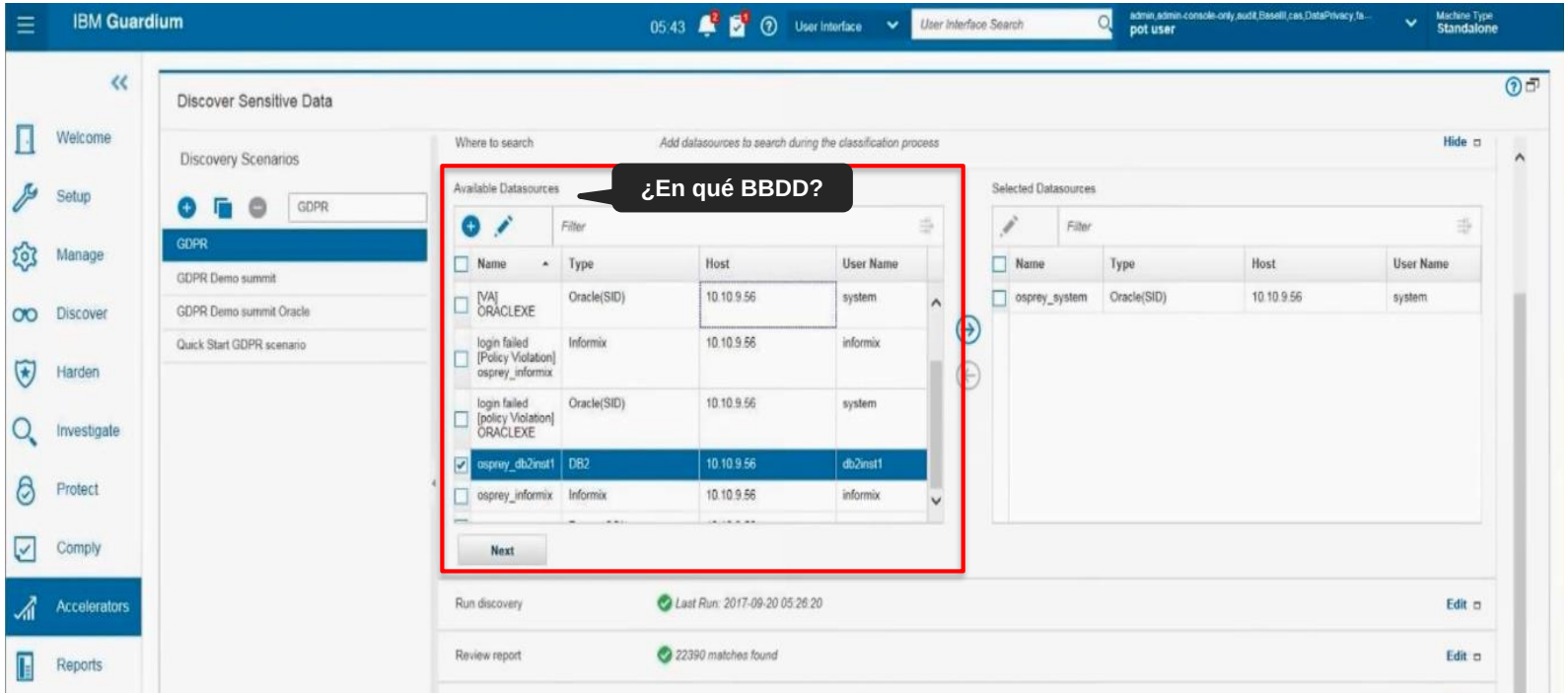
Descubrimiento de Datos Sensibles

LOGICALIS
Business and technology working as one

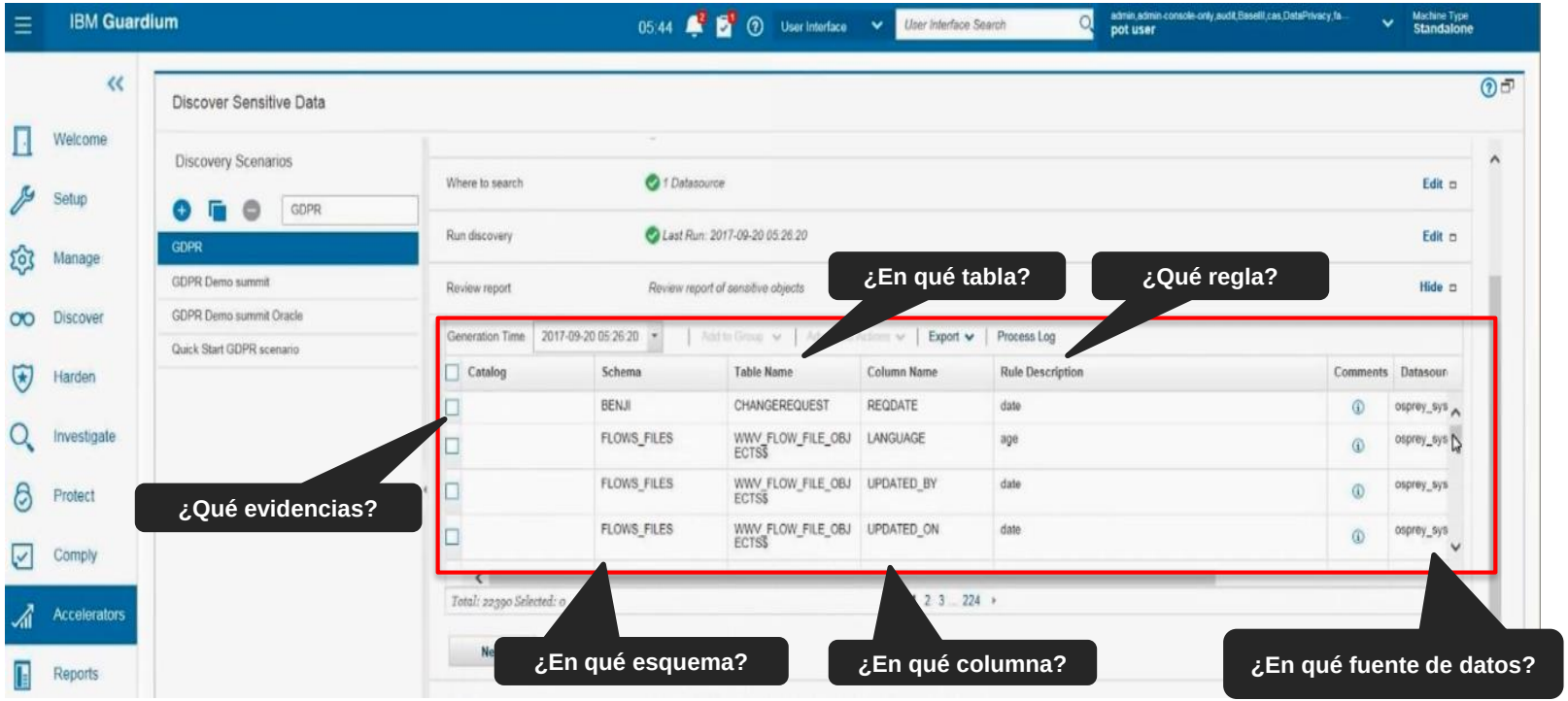
¿Dónde están mis datos? (1)



¿Dónde están mis datos? (2)



¿Dónde están mis datos? (3)

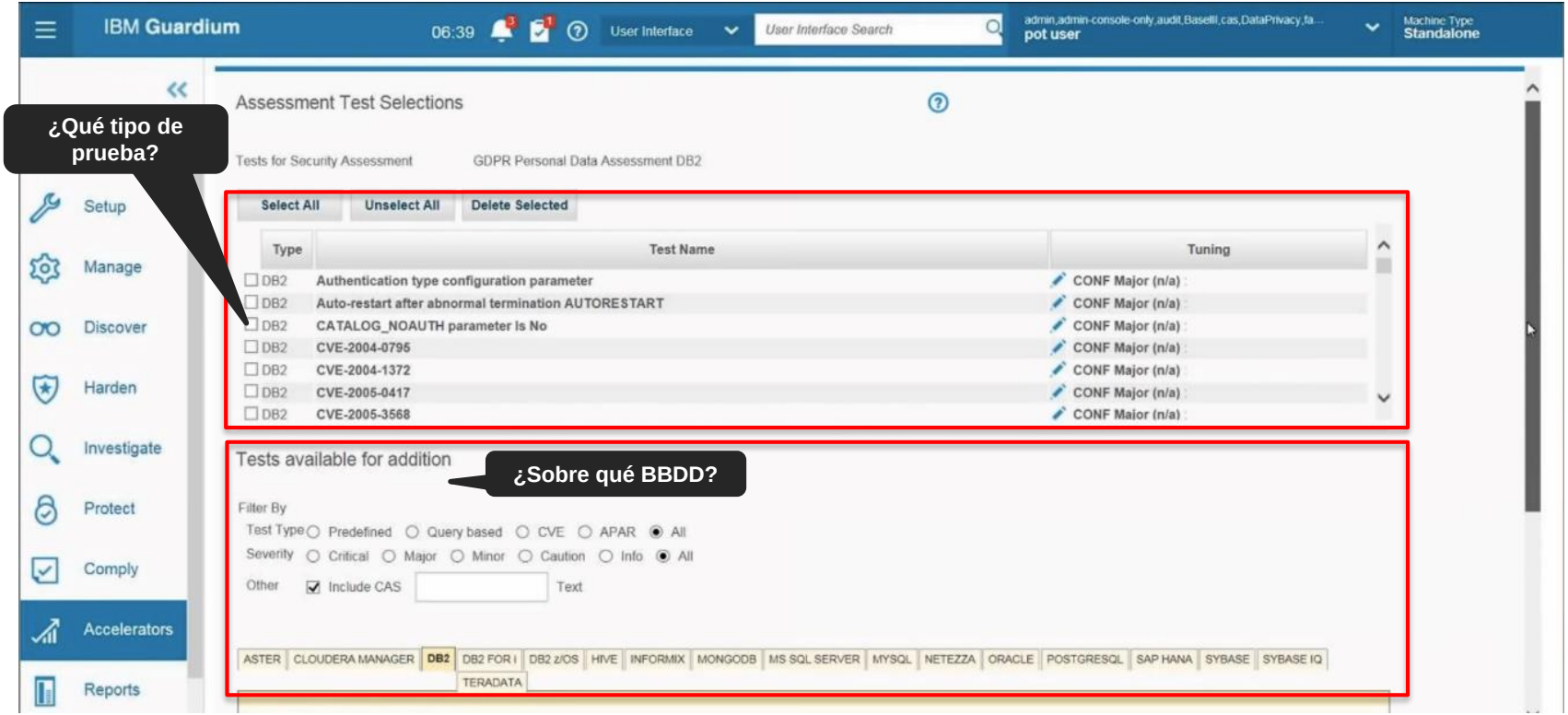


Data Protection. Ejemplos (II)

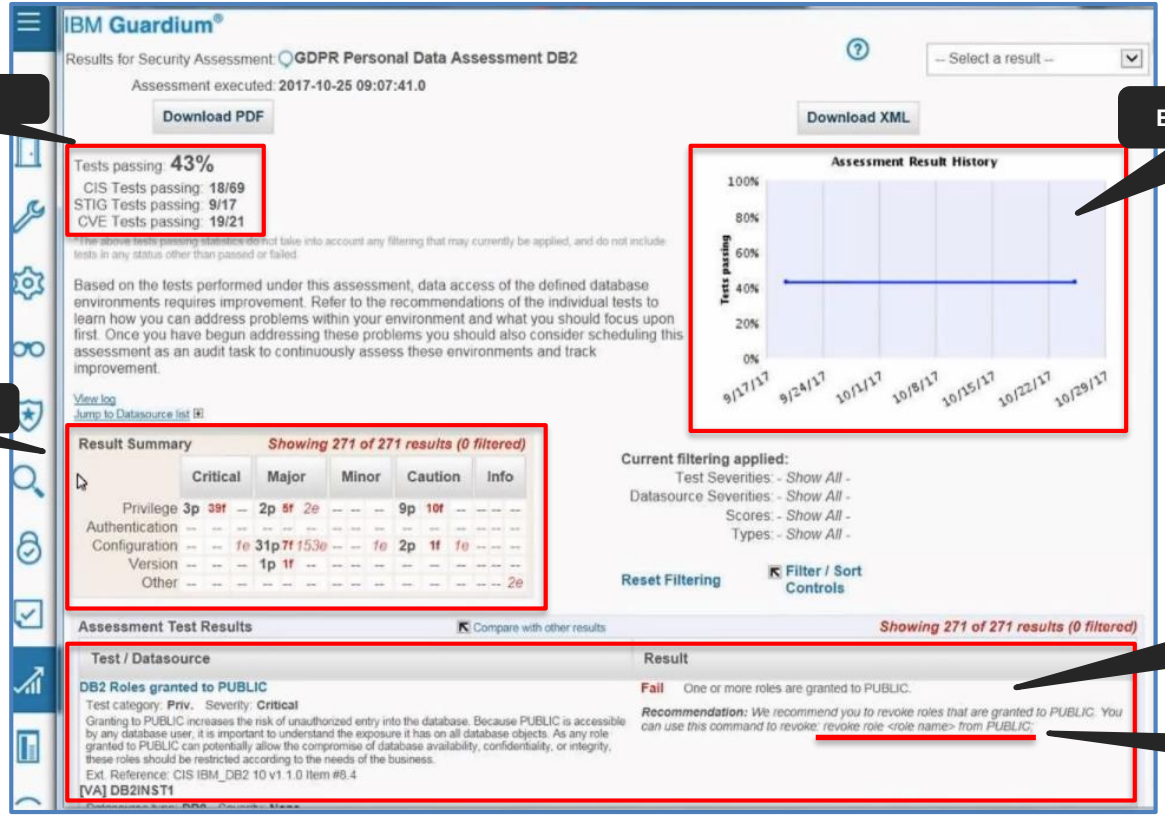
Escaneo de Vulnerabilidades

- Fallos de configuraciones
- Exceso de privilegios
- CVEs

Escaneo de Vulnerabilidades (1)



Escaneo de Vulnerabilidades (2)



Estado actual

Evolución del histórico

Detalle de severidad

Detalle de la Vulnerabilidad

Recomendaciones

LOGICALIS
Business and technology working as one

Data Protection. Ejemplos (III)

Monitorización y Auditoría

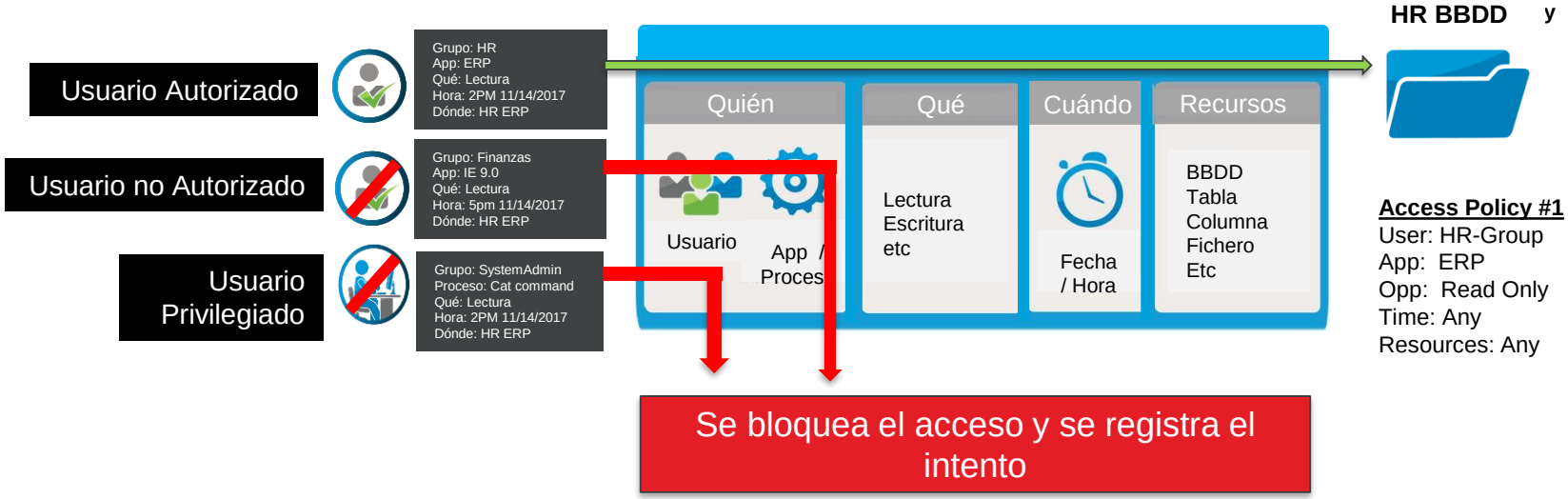
Caso de Uso: Data Breach

Políticas de Auditoría

Análisis de actividad de usuarios en tiempo real

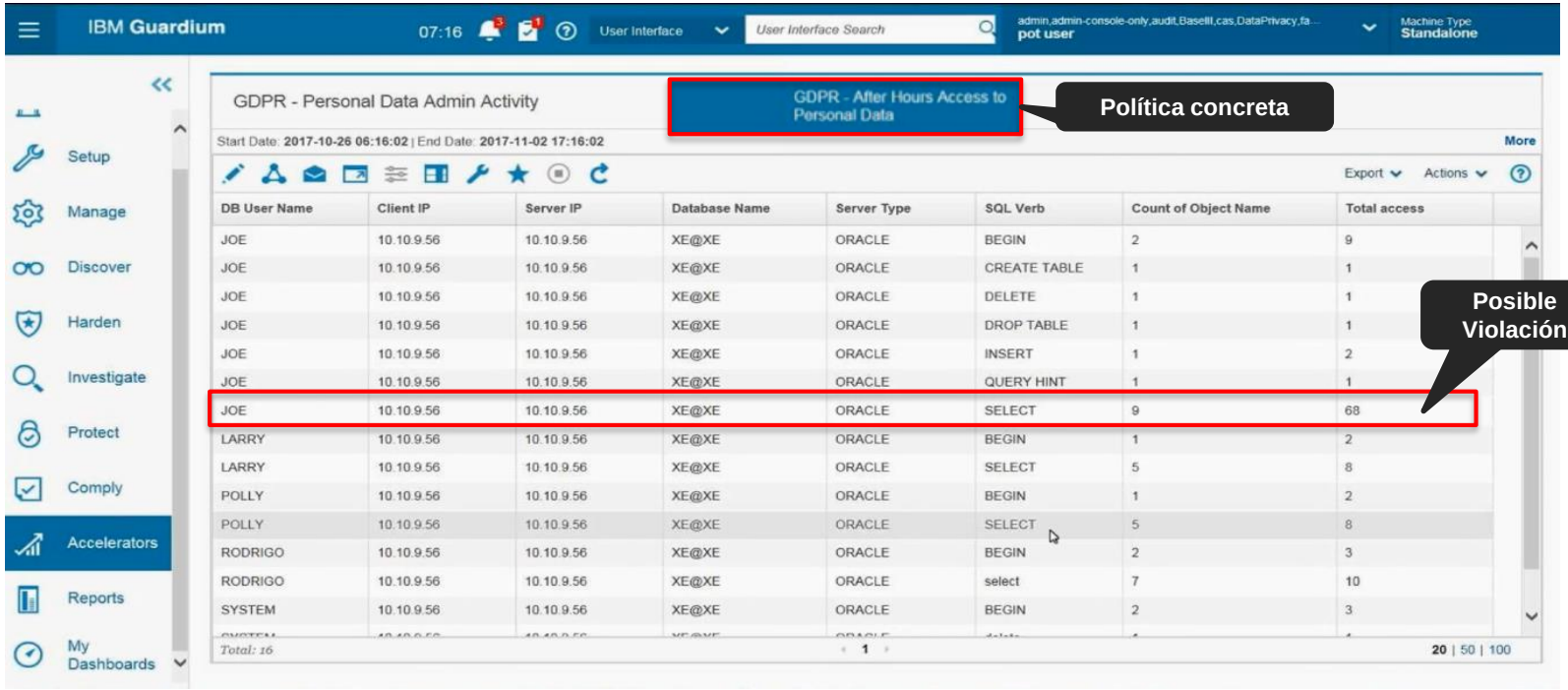
Violación de políticas. Enmascaramiento

Monitorización y Auditoría (1)

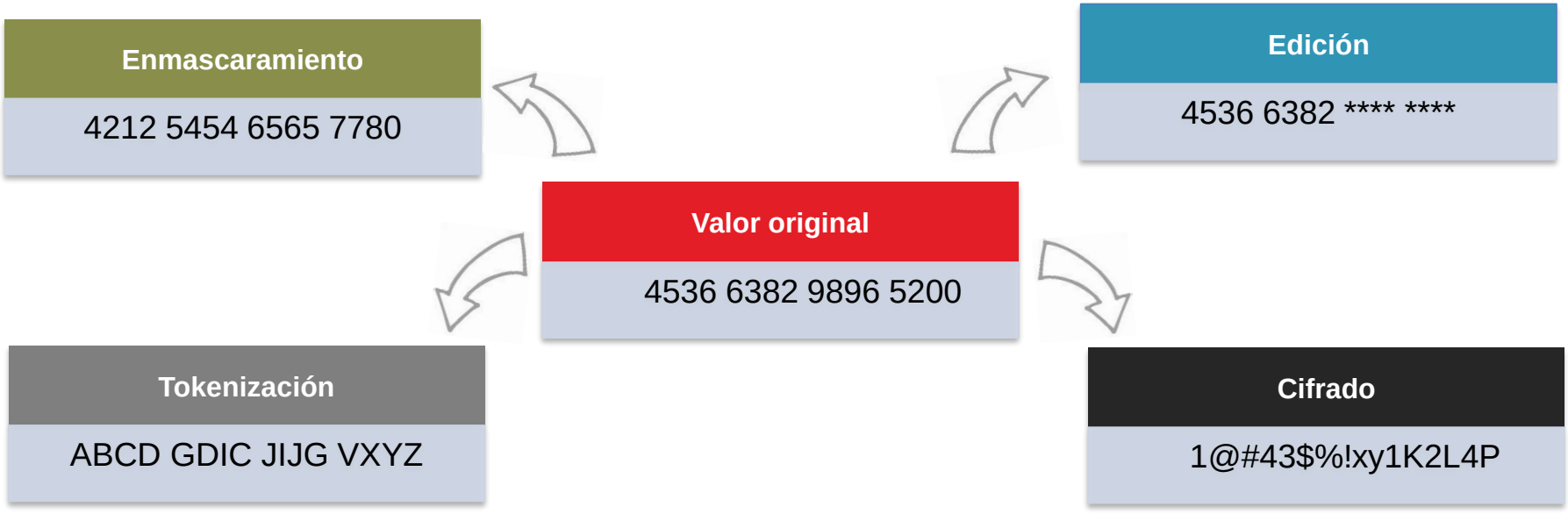


Toma de decisiones dinámica en base al comportamiento del usuario

Monitorización y Auditoría (2)

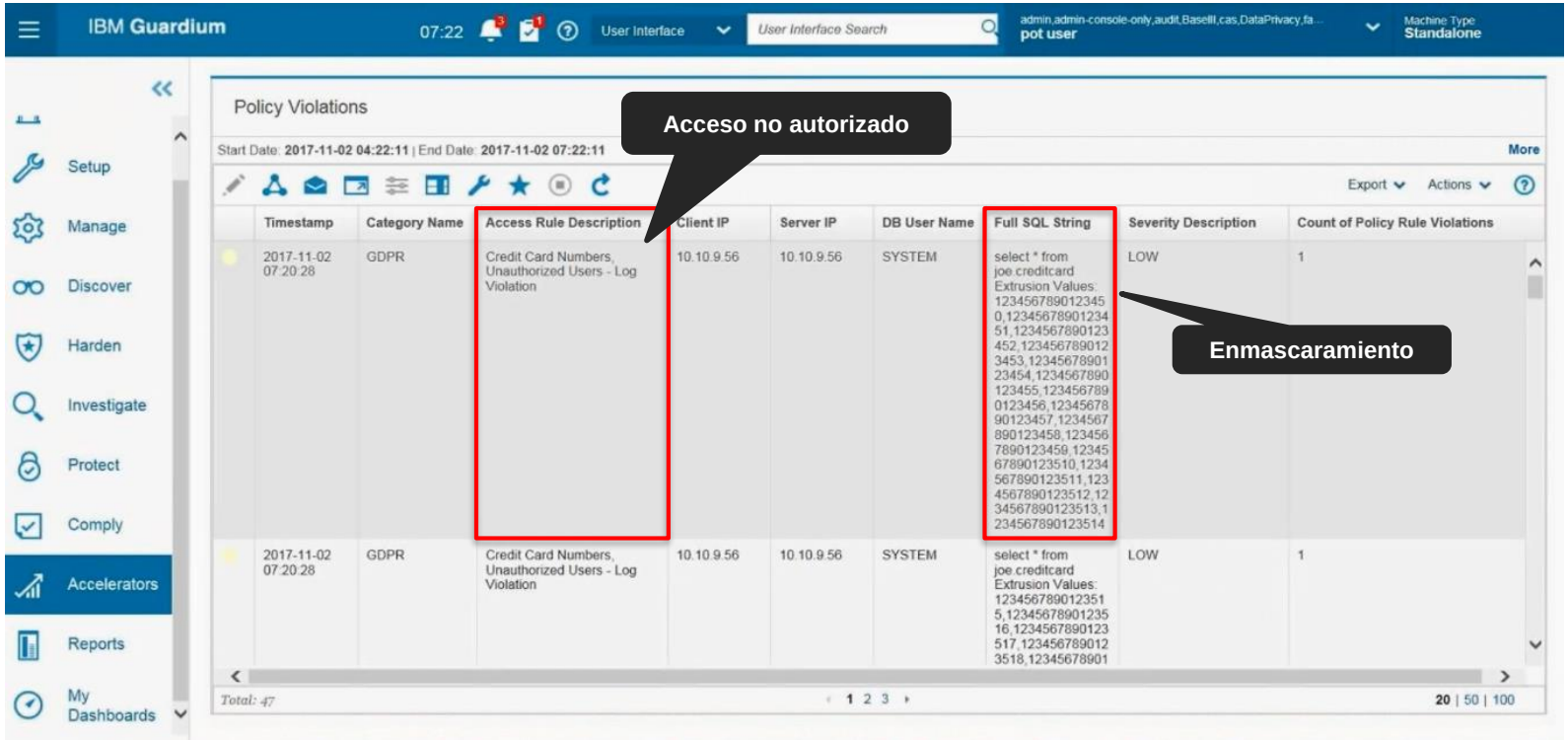


Monitorización y Auditoría (3)



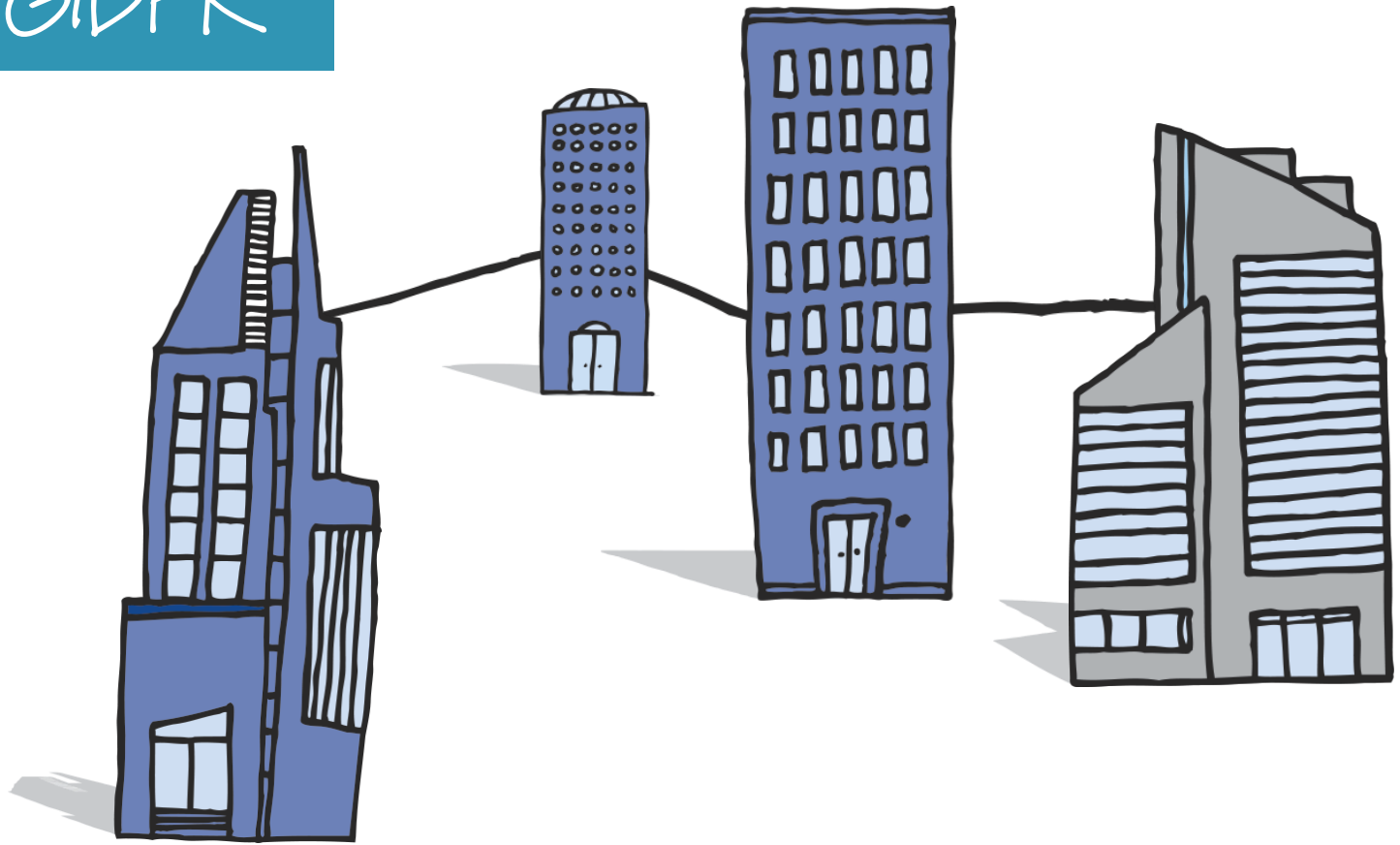
Toma de decisiones dinámica en base al comportamiento del usuario

Monitorización y Auditoría (4)



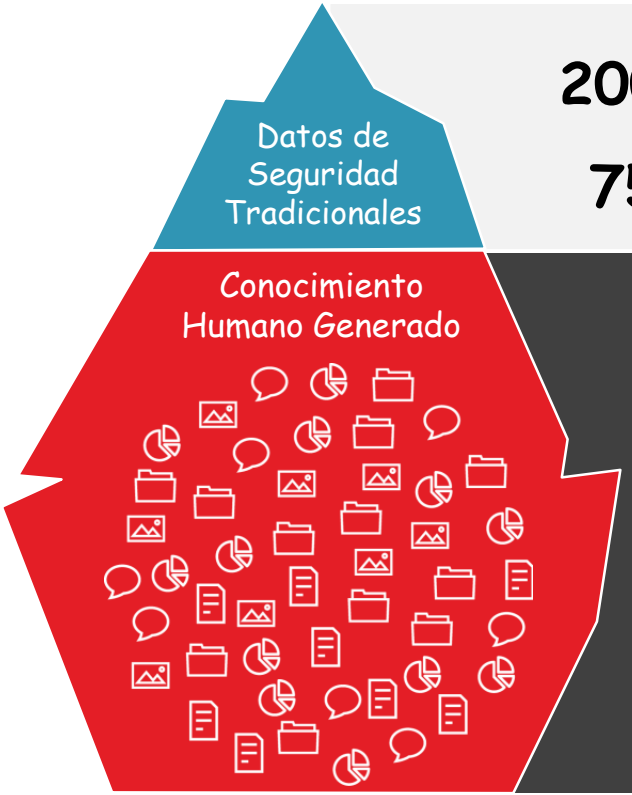
Soluciones GDPR

Integración



LOGICALIS
Business and technology working as one

Universo de Datos GDPR



200K+ Eventos de seguridad diarios

75K+ Vulnerabilidades de Software reportadas

- Eventos de Seguridad y Alertas
- Logs y datos de configuracion
- Actividad de Red y Usuarios
- Feeds de amenazas y Vulnerabilidades

Un universo de conocimiento de seguridad desconocido

8%

Las organizaciones típicas aprovechan solo el 8% de este contenido

720K blogs de seguridad / año

180K noticias y artículos de seguridad / año

10K investigaciones de seguridad / año

- Publicaciones industriales
- Información Forense
- Comentarios sobre amenanzas
- Informes de analistas
- Presentaciones de conferenciass
- Nuevas fuentes
- Newsletters
- Tweets
- Wikis

LOGICALIS
Business and technology working as one

Plataformas SIEM QRadar

Dispositivos de Seguridad

Servidores y Mainframes

Actividad de Red y Virtual

Actividad de Datos

Actividad de Aplicaciones

Información de Configuraciones

Vulnerabilidades y Amenazas

Usuarios e Identidades

Global threat intelligence

QRadar SIEM

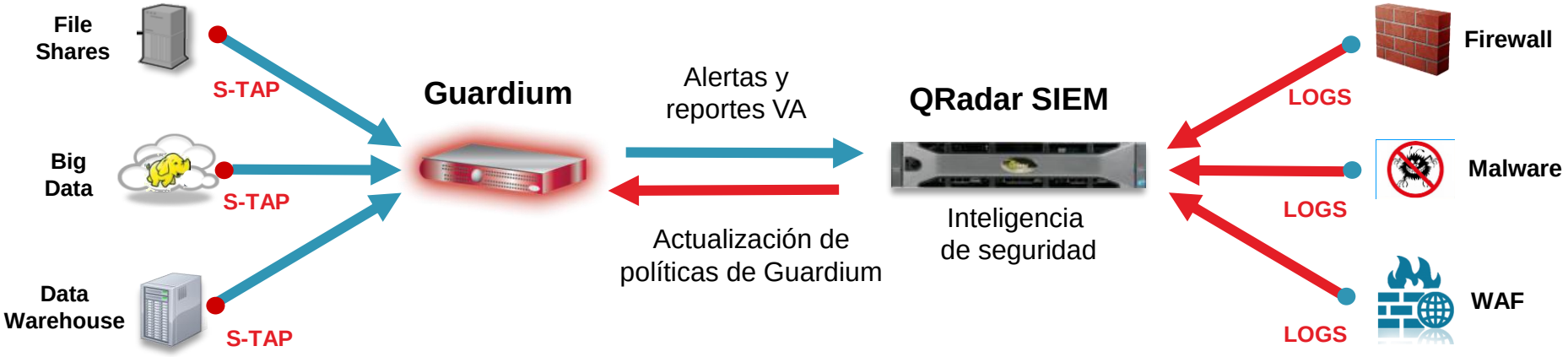
Identificación de Incidentes

- Amplia recopilación de datos, almacenamiento y análisis
- Correlación en tiempo real, anáisis de comportameinto, e inteligencia de amenazas
- Detección automática de activos, servicios y usuarios
- Línea base de actividades y detección de anomalías
- Implementacion fácil de casos de uso con App Exchange

Inteligencia de Seguridad

LOGICALIS
Business and technology working as one

Data Protection & SIEM (I)



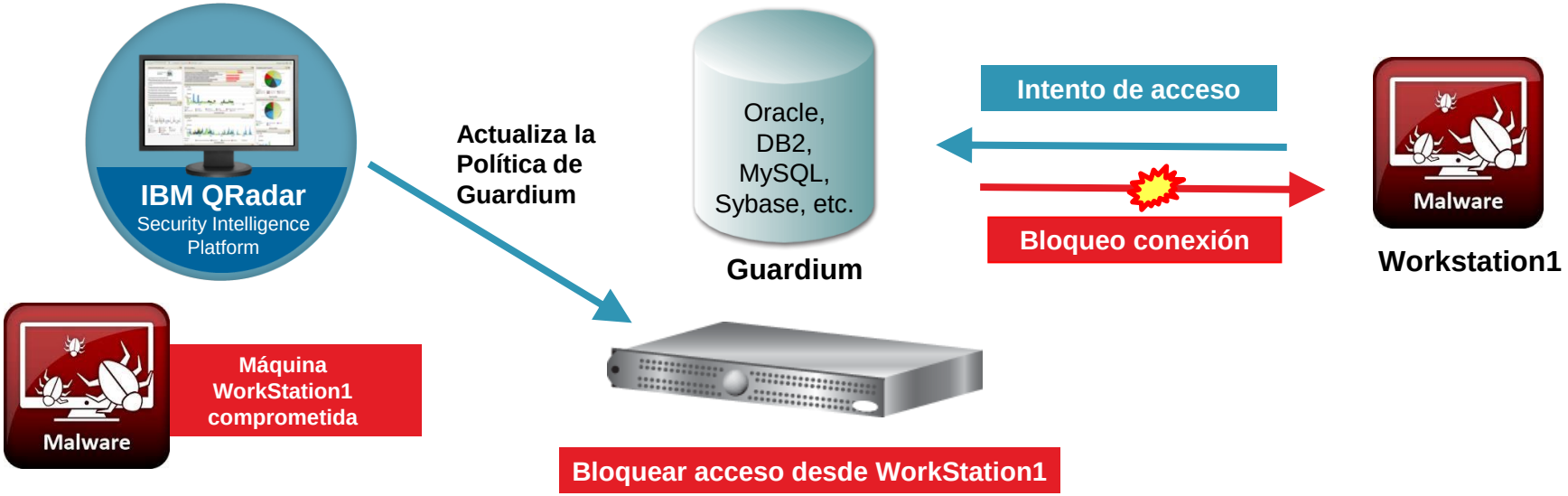
Es posible mantener las políticas de Guardium actualizadas en tiempo real y de forma automática en respuesta a eventos de seguridad de QRadar

Flujo de información bidireccional

Data Protection & SIEM (II)

Caso de Uso

- Detección de una máquina infectada con Malware y bloqueo automático del acceso



Respuesta Incidentes de Seguridad

Los desafíos en la comunicación de brechas de seguridad

*GDPR Obligará a reportar a las autoridades una brecha de seguridad en menos de **72 horas** y a notificar a los clientes afectados por las mismas. Lo que plantea un gran reto en los equipos de seguridad.*

Reduce tiempos, mejora la orquestación, facilita la recolección de evidencias

Permitirá a los equipos de seguridad orquestar los procesos de respuesta, y resolver incidentes más rápido y de forma más inteligente. Lo que antes se hacia en días/semanas ahora puede hacerse en horas/días.

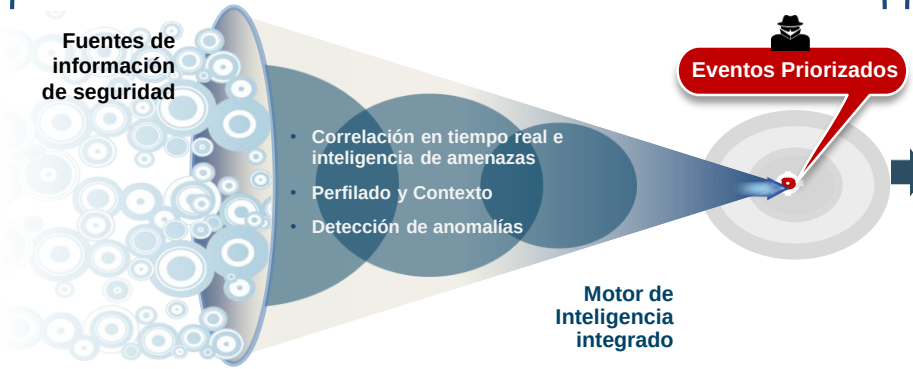
Se integra a la perfección con productos de IBM y de terceros

Además posee funcionalidades específicas para cumplimiento y seguimiento GDPR (GDPR Enhanced Privacy Module).

Respuesta Incidentes & SIEM

QRadar
Eventos priorizados de seguridad basados en logs, flujos, vulnerabilidades.

Procedimiento de respuesta a incidentes
Operaciones de seguridad en respuesta a amenazas brechas de datos, vulnerabilidades.



Creación del incidente → **Recopilación de contexto y tareas** → **Remediación / Cierre**

Base de conocimiento

Análisis continuo de la seguridad

Triaje de incidentes de seguridad

Reporte y notificación de incidentes

LOGICALIS
Business and technology working as one

QRadar Watson. Tiempo de Respuesta

Análisis Manual de Amenazas

Triaje de Incidentes → Investigación y Evaluación de Impacto → Remediación

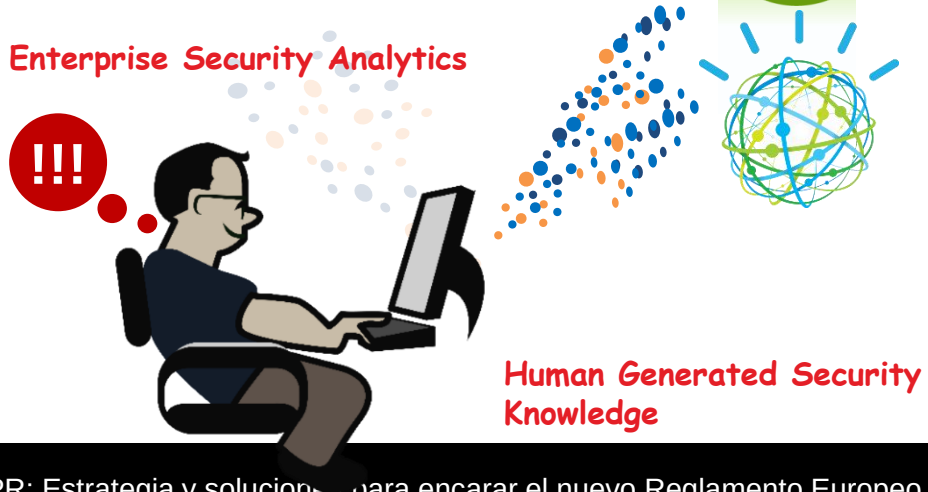
Días a Semanas

QRadar Advisor con Asistencia de Watson

Triaje de Incidentes → Investigación y Análisis de Impacto → Remediación

Minutos a Horas

Análisis rápido y preciso de las amenazas de seguridad, ahorrando tiempo y recursos valiosos



- **Acelera** el triaje de incidentes con más automatización y profundidad en el análisis
- **Alivia** presión en el gap de habilidades de Seguridad
- **Reduce** el riesgo de perder el análisis de enlaces ya descubiertos previamente
- **Aumenta** la contribución de los equipos de seguridad

Watson for CyberSecurity

LOGICALIS
Business and technology working as one

Respuesta End-to-End

QRadar → Alertas/ Anomalías → Watson → Causa raiz y comportamiento → Resilient → Acciones

- Amenazas
- Campañas
- Dominios
- IPs
- Hash
- Emails
- Ficheros
- Vulnerabilidades

Acciones

- Network Protection — Bloqueo Usuarios/ IPs / Dominios
- BigFix — Parches Vulnerabilidades
- Guar-dium — Protección Bases de Datos
- IAM — Modificar derechos de Usuario
- I2 …. — Investigación Forense …

Aproximación Seguridad Logicalis

Servicio de Adecuación a la GDPR

Análisis GAP
- Assessment Tecnológico

Diagnóstico de la situación actual frente a marcos normativos en materia de seguridad

Medidas Tecnológicas
- Plan de Acción Tecnológico
- Análisis y definición de soluciones
- Implantación y adecuación tecnológica

Servicios Gestionados
- Soporte correctivo, preventivo y evolutivo
- Servicios Avanzados de Seguridad
- SOC

Data Protection

- Descubrimiento, clasificación, evaluación de vulnerabilidades, informes de accesos y permisos
- Cifrado, enmascaramiento
- Monitorización de la actividad de los datos y los ficheros (incl. usuarios privilegiados)
- Bloqueo dinámico de accesos, alertas y cuarentena
- Automatización del cumplimiento legal / normativo y auditoría

IBM Security Guardium

- Aplicaciones
- Big Data
- Bases de Datos & Data Warehouses
- Sistema Ficheros

Retos GDPR

Respuesta End-to-End

QRadar → Alertas/ Anomalías → Watson → Causa raiz y comportamiento → Resilient → Acciones

- Amenazas
- Campañas
- Dominios
- IPs
- Hash
- Emails
- Ficheros
- Vulnerabilidades

Acciones:

- Network Protection: Bloqueo Usuarios/ IPs / Dominios
- BigFix: Parches Vulnerabilidades
- Guar-dium: Protección Bases de Datos
- IAM: Modificar derechos de Usuario
- I2 ….: Investigación Forense …

LOGICALIS
Business and technology working as one

Próximos pasos …

Gracias !!!

LOGICALIS Security