ARCHIVO NACIONAL
COSTA RICA

XXXIV Congreso Archivístico Nacional

CONSTRUYENDO EN CONJUNTO
UNA NUEVA VISIÓN DEL SNA

Ciberseguridad en el manejo de los datos y su impacto en la gestión de documentos

Clasificación de datos

y la ciberdefensa de las organizaciones

ATTICYBER

$id

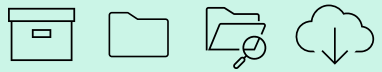
- Fundador y Jefe de Técnología en ATTICYBER
- Ingeniero de Sistemas Informáticos
- Máster en Gestión de Riesgo y Ciberseguridad
- Trabajé para Intel Security e IBM Security
- Ex Miembro Junta Directiva CPIC
- Full CV: www.estebanjimenez.com

Protección de la información
Activos digitales

- La **archivística**, **archivología** o **archivonomía** es una disciplina propia de las ciencias de la información, dedicada al estudio teórico y práctico de los principios, procedimientos y problemas concernientes a las funciones de los documentos y de las instituciones que los generan y los custodian, con el objetivo de potenciar el uso y servicio de ambos.

Archivística

- Funcionalidades
- Custodia
- Archivo
- Gestión
- Patrimonio
- Clasificación
- Historia
- Preservación
- Descripciones



Objetivos de aprendizaje

Clasificación de datos	Gobernanza de datos	Los datos maestros (MDM)	La metadata
Etiquetado digital	eDiscovery	Recovery Vaults	Electronic Archives

Seguridad de la Información

- “La seguridad de la información es algo que hacemos, no algo que compramos…”

Burton Group

- *“El ciberimen es el mayor riesgo para cualquier organización en el mundo”*

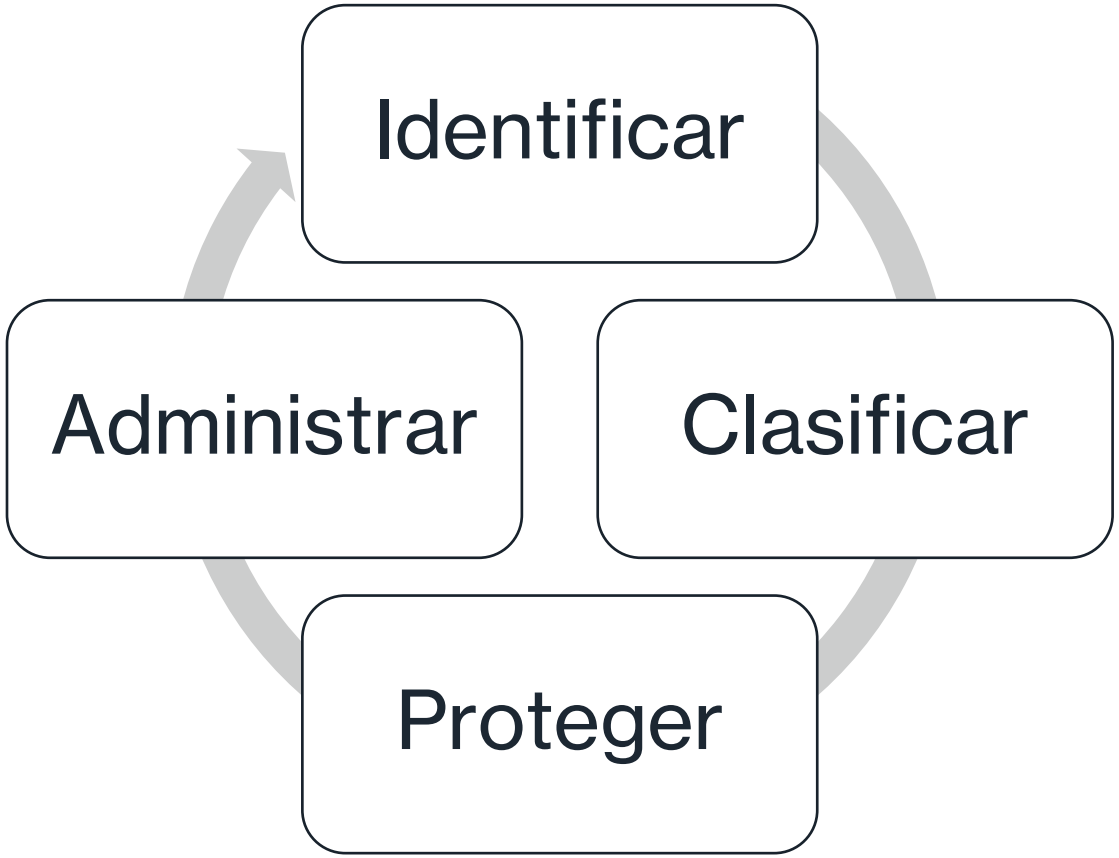
Ginny Rommeti

- *“Hay un ataque a los archivos de una organización cada 39 segundos”*

Universidad de Meryland

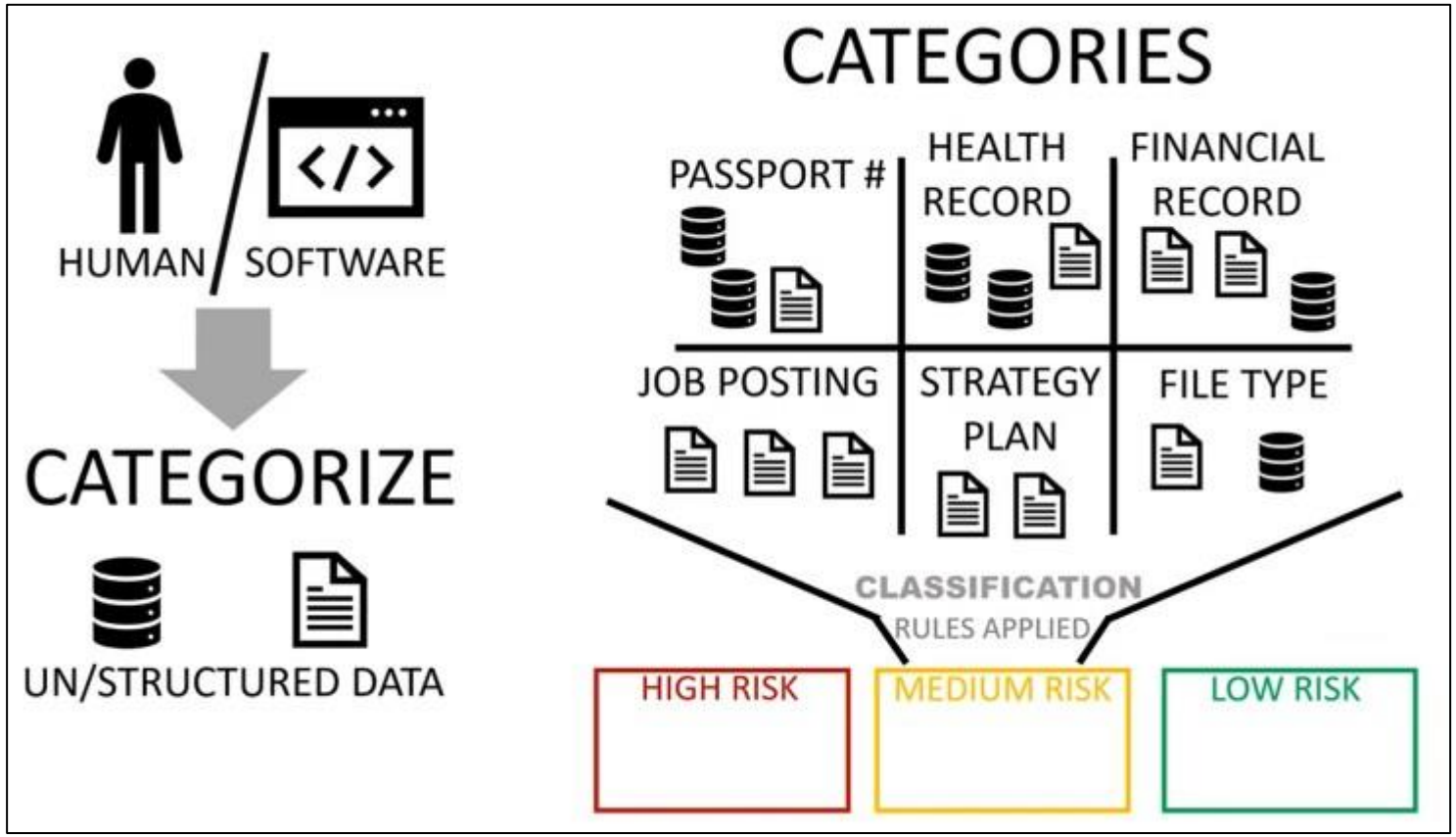
Clasificación de datos

- Es el proceso de análisis de datos estructurados y no estructurados que nos permite ordenar los datos según sus categorías, contenidos, tipos de archivos y otras características.



Importancia de la CD

- Permite lograr que los datos sean entendibles dentro de un contexto. No requerimos de conocer los contenidos necesariamente de un archivo para poder administrarlo de manera correcta según su clasificación.



ATTICYBER

Métodos de clasificación basados en el principio de defensa digital

Basado en Sensitividad

Basado en Contenido

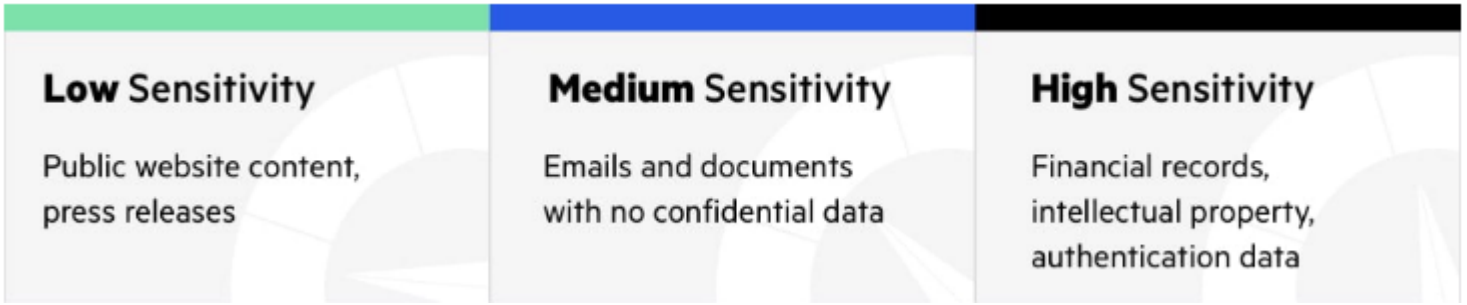
Modelos por sensitividad

Baja: Usualmente relacionado a documentos de uso público.

Alta: En caso de ser comprometidos el impacto contra la organización conlleva serias consecuencias.

Media: Documentos de uso interno, en caso de pérdida o robo no tendrán un impacto catastrófico en la organización.

Sensitividad	Modelo 1	Modelo 2
Alta	Confidencial	Restringido
Media	Uso Interno	Sensitivo
Baja	Público	Irrestricto



Modelos por contenido

Etiquetado dígital

- Permite colocar una marca en un archivo de manera programática según el contenido encontrado

Jerarquía Taxonómica

- Estructura por folders dentro de un medio de almacenamiento lógico usualmente divido por departamentos, usuarios, títulos, fechas con subsecciones o subfolders

Metadatos

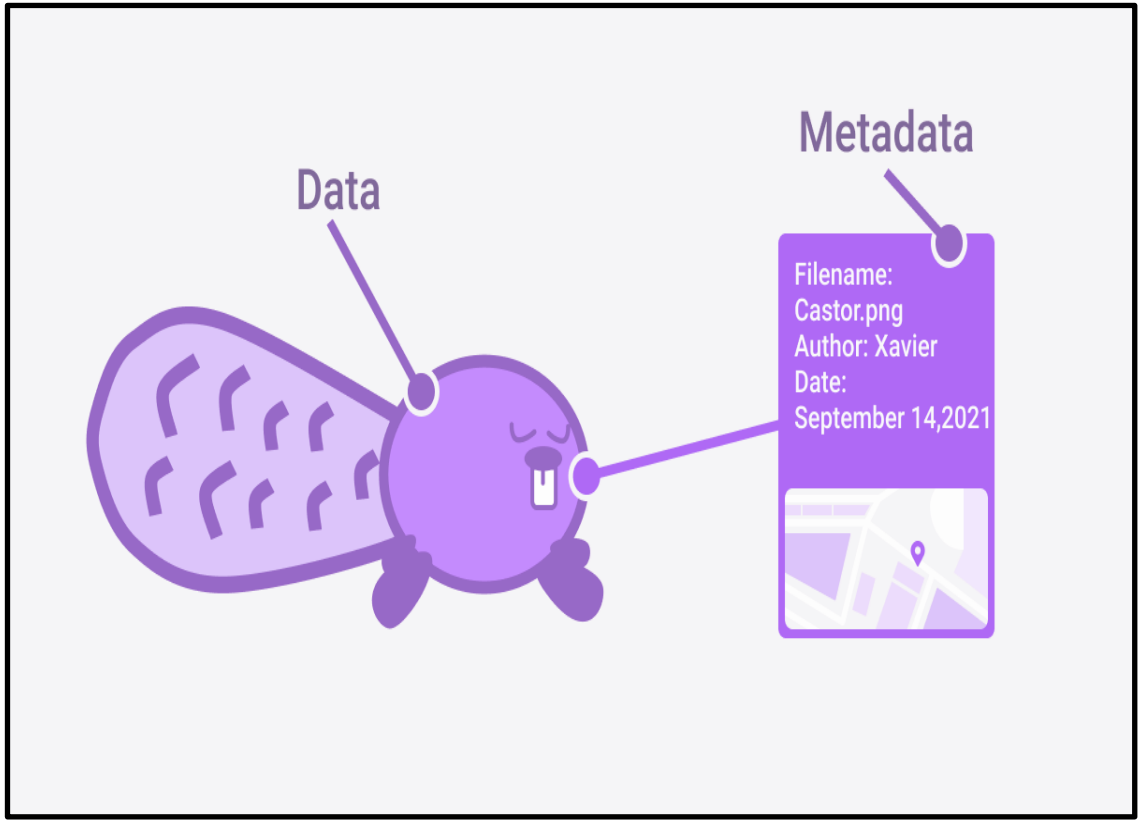
- Seríe de atributos relacionados a un archivo, datos estructurados que hacen referencia a otros datos como tamaño de archivo, fechas de creación, extension del archive, etc.

ATTICYBER

Ejemplo: Microsoft Purview

El desafío de la metadata

- La cantidad de datos que actualmente produce una organización es un ahora un problema de “Big Data”.
- Generalmente los sistemas solo serán capaces de procesar y clasificar información una vez que la calidad de la metadata así lo permita.
- Si la información no puede ser caracterizada de forma efectiva por sus atributos, la información difícilmente podrá ser encontrada por el usuario.



Estudio de la metadata: Tipos

Títulos, keywords, bibliografía

Reportes, porcentajes, compendios

Estructura, orden de elementos

Reglas de acceso, permisos, tamaño de archivo, requerimientos procesamiento

Trazabilidad de uso o procesamiento del archivo o dato, validación de errores

Licenciamiento, derechos, deberes, políticas de uso

Licenciamiento, derechos, deberes, políticas de uso

ATTICYBER

Common metadata standards

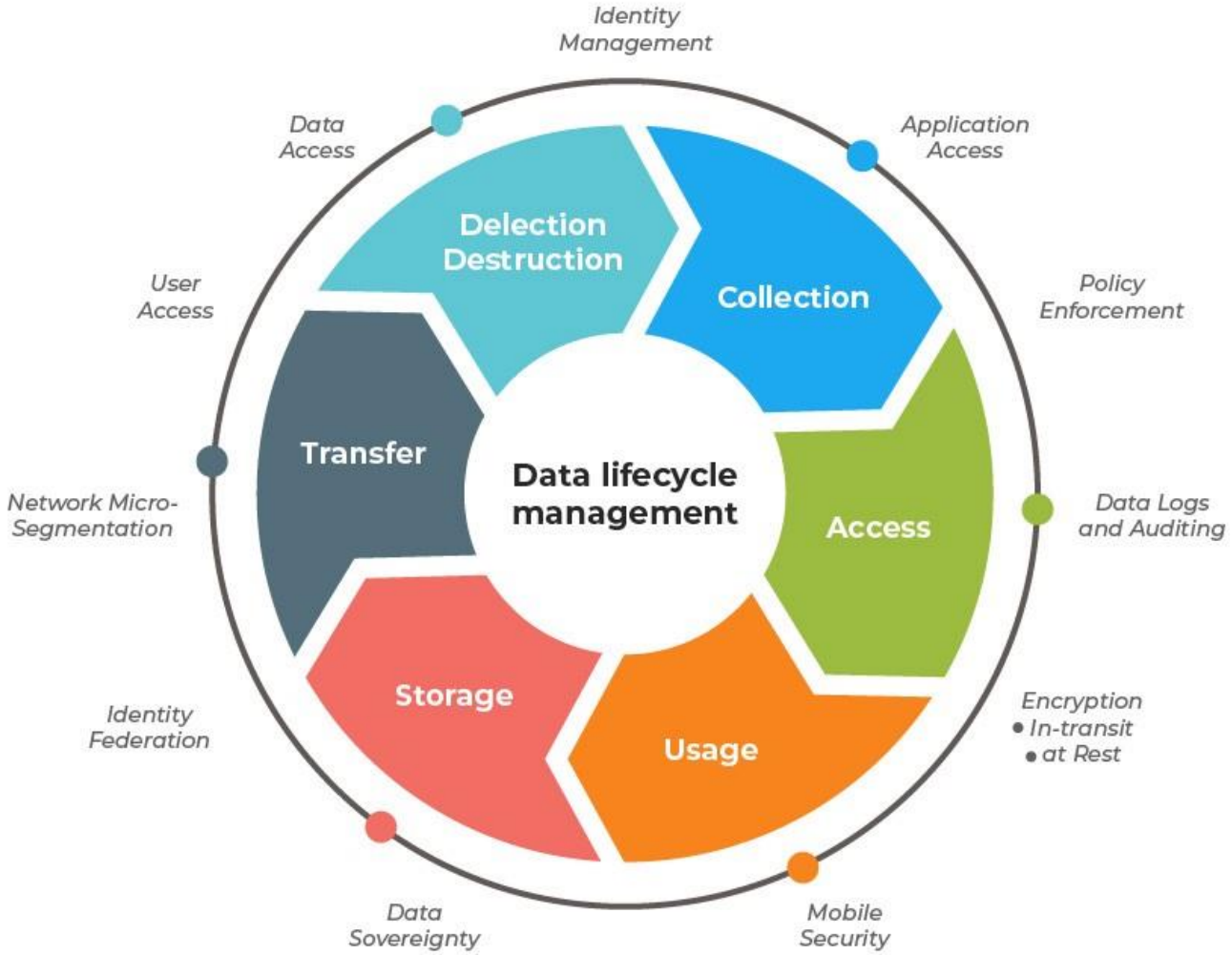
STANDARD	DESCRIPTION	SCHEMA
Dublin Core	Widely used for web-based digital metadata; adapted from physical library card indexing purposes.	Describes the attributes of 15 core data elements.
Metadata Objects Description Schema	Bibliographic metadata standard designed to replace 1960s-developed Machine-Readable Catalog standards	XML-based schema for libraries.
schema.org	Newer standard based on open source software collaboration.	Collection of metadata schema geared to structured digital data (e.g., internet data, email, etc.).

Otros esquemas

Industria	Estándar
Documentos de Artes y Humanidades	Text Encoding Initiative, VRA Core
Documentos de Cultura y Sociedades	Data Documentation Initiative, Open Archives Language Community
Documentos de Ciencias	Darwin Core, Ecological Metadata Language, Federal Geospatial Data Comittee

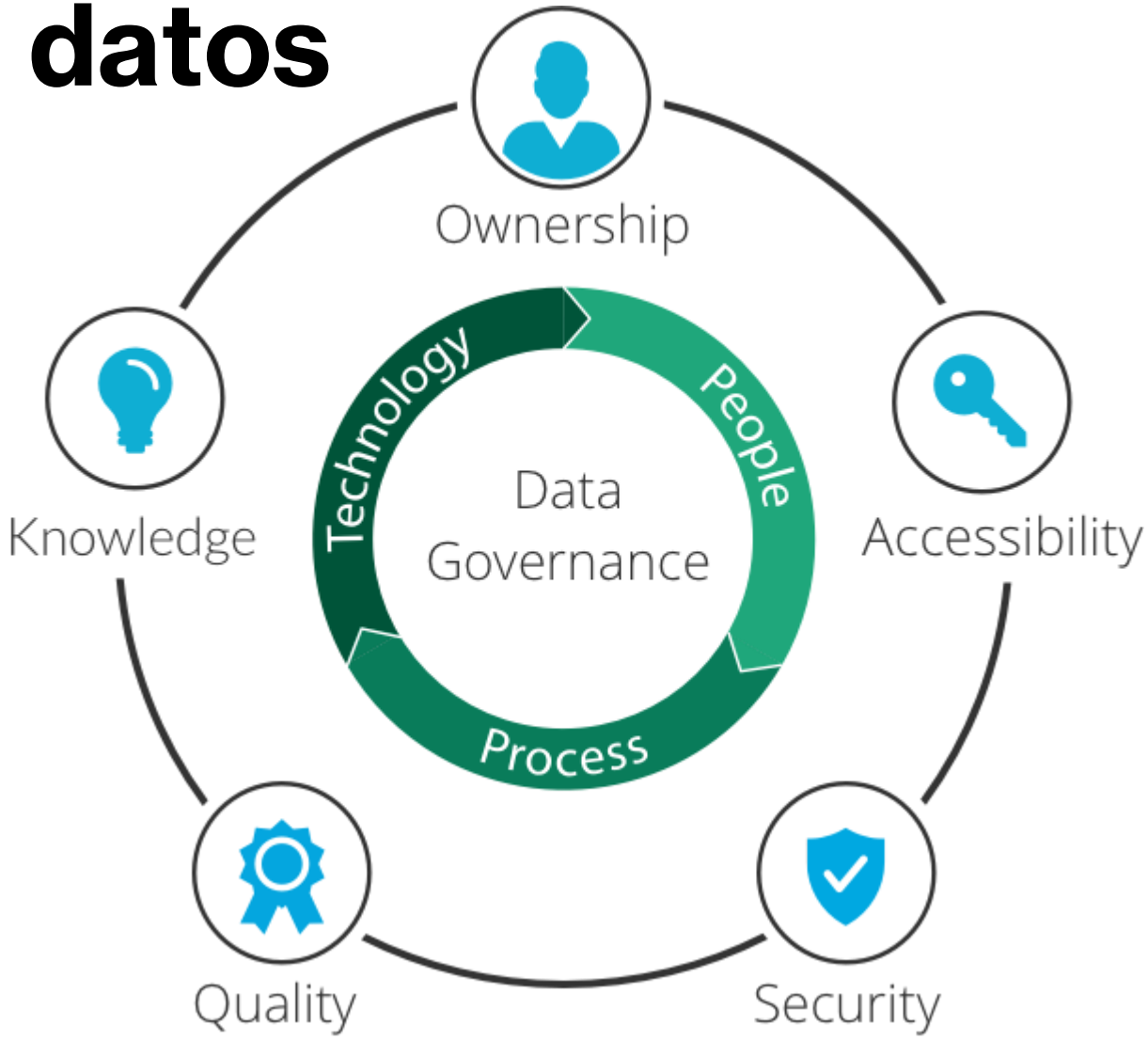
ATTICYBER

Data Lifecycle Management



Governanza de los datos

- Es una colección de procesos, roles, políticas, estándares y métricas para asegurar la efectividad del uso de la información en una organización.
- La gobernanza es el mecanismo mediante el cuál una organización define los procesos y responsabilidades dirigidos a mejorar la calidad y seguridad de los datos dentro de un esquema de clasificación y control de información.
- La gobernanza define quién puede tomar qué acción, con qué datos, en qué situaciones y por qué métodos.
- La gobernanza en el componente principal del data governance.



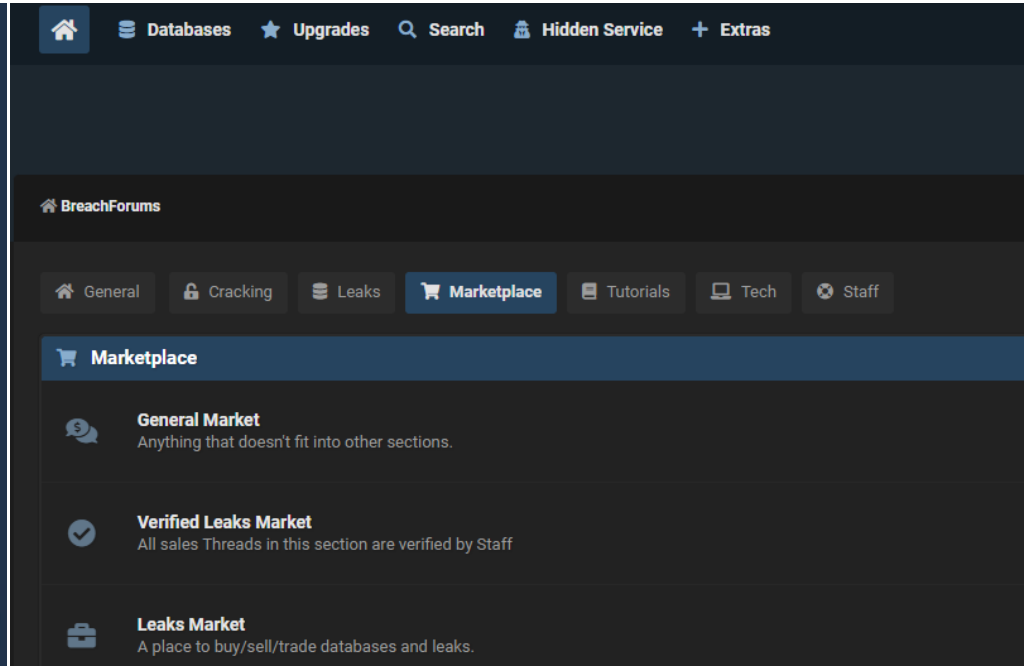
Master Data Management (MDM)

- Se enfoca en identificar las piezas de información madre para permitir la mejora de esta información. Transforma los datos en entidades como clientes, proveedores, sistemas y asegura la evolución y transformación de la información almacenada por una organización.

Ejemplo: SAP Master Data Governance

Vigilancia del MDM

https://www.dehashed.com/



https://breached.to/

ATTICYBER

eDiscovery

La clasificación de datos requiere conocer la ubicación, el volumen y el contexto de los datos. La mayoría de las empresas modernas almacenan grandes volúmenes de datos, que pueden distribuirse en varios repositorios:

- Bases de datos implementadas en las instalaciones o en la nube
- Big Data plataformas de datos
- Sistemas de colaboración como Microsoft SharePoint
- Servicios de almacenamiento en la nube como Dropbox y Google Docs
- Archivos como hojas de cálculo, PDF o correos electrónicos

ATTICYBER

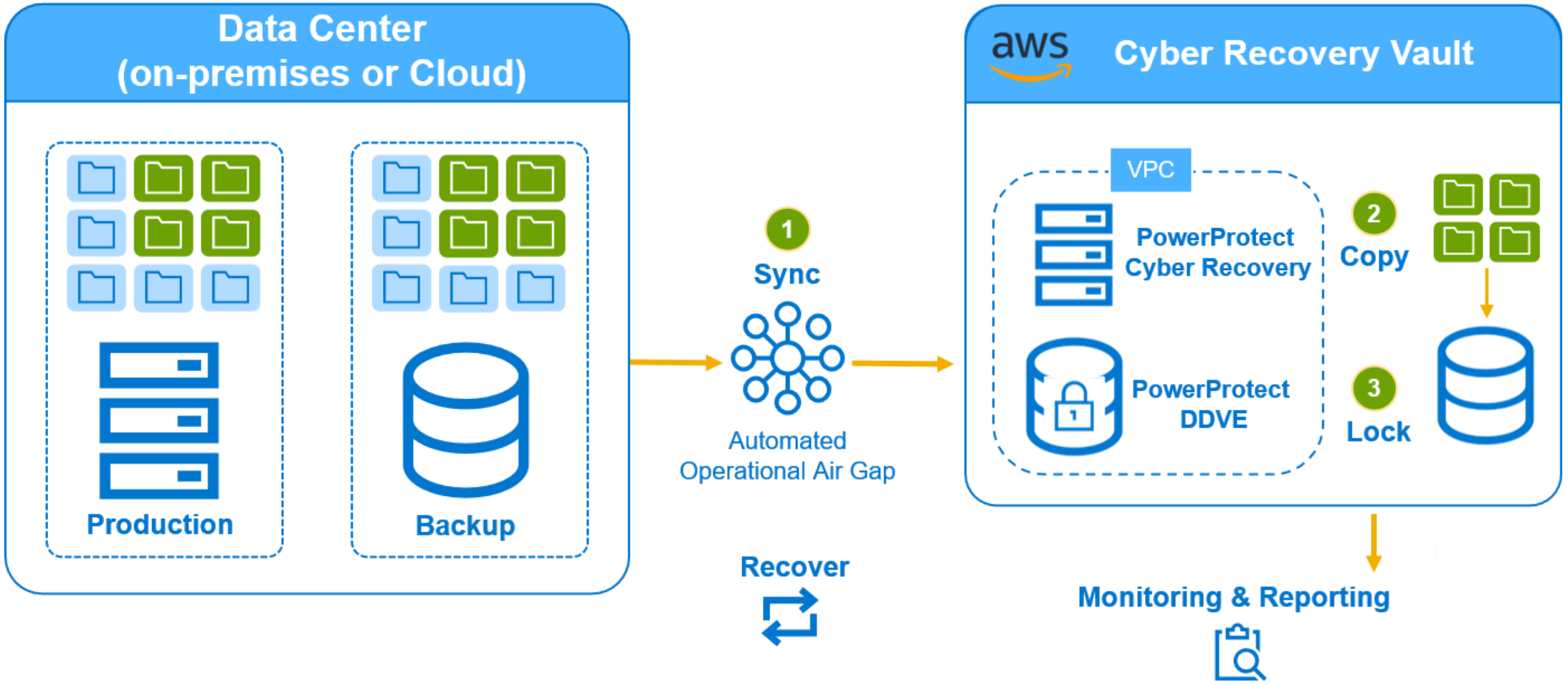
Ejemplo: Imperva Data Discovery

ATTICYBER

Data Recovery Vaults

- Una bóveda de recuperación cibernética es una defensa de varias capas contra los ataques cibernéticos. Esto se logra separando los datos críticos de la superficie de ataque. Está físicamente aislado, en una parte protegida de un centro de datos; el acceso requiere credenciales de seguridad únicas y autenticación multifactor (MFA).
  - La bóveda debe estar protegida por un espacio de aire,
  - La bóveda debe estar fuera del sitio y preferiblemente ser operada por una organización separada, y
  - La bóveda debe ejecutar análisis, diseñados para detectar posibles problemas de manera temprana.

ATTICYBER



Otras opciones: VERITAS Azure Backup veeAM

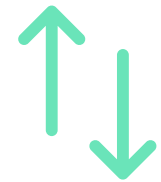
ATTICYBER

El mundo está cambiando y los ciberataques ahora son parte de la vida diaria. Y entre el arsenal electrónico disponible para protegerse contra estos riesgos de ciberseguridad, el archivo electrónico ocupa un lugar destacado.

ATTICYBER

La clasificación y preservación de los datos es nuestra mejor defensa

- La clasificación de datos garantiza que las organizaciones aprueben las obligaciones de cumplimiento normativo para desarrollar una seguridad centrada en los datos en todos los niveles de la empresa.
- Ayuda a las empresas a priorizar sus esfuerzos de protección de datos, mejorando la seguridad de los datos y el cumplimiento normativo. La clasificación también ayuda a reducir costos, aumentar la productividad del usuario y facilitar la toma de decisiones rápida al eliminar datos innecesarios.
- Además, la información confidencial debe almacenarse de forma segura (y a menudo debe hacerlo por ley) y eliminarse de las bases de datos de la empresa después de un período definido. Las empresas deben crear categorías de datos y aplicar reglas de seguridad para evitar infringir la ley.



ATTICYBER

Consejos: Seguridad de datos completa

La clasificación de datos ayuda a proteger sus datos valiosos y mejora la seguridad de los datos. Una vez que identifique los diferentes tipos de datos en su red, puede separar sus datos confidenciales de los datos generales. A su vez, esto le permite:

- Prioriza tus medidas de seguridad
- Ajuste sus controles de seguridad en función de la confidencialidad de los datos
- Descubra quién puede acceder, modificar o eliminar datos en su red
- Evalúe todos los riesgos y amenazas, como el impacto empresarial de una infracción o un ataque de ransomware, etc.


¡MUCHAS GRACIAS!
jan@core:~$ byzanz-record --delay=3 -d 30 elite.gif
jan@core:~$ y | hackertyper.sh -g -f -s 200; ./hack.exe google.com
Exploit-the
VIRUS
DROPPER
Nation's-Data
Reverse-
Engineering
HoM3-$w33t
Ur-Computer-
is-MY-Slave
H4x0r-HoM3-
127.0.0.1
|H4CK3R|
+WARNING+"Illegal_Network_Connections_Beyond_Login"
You are at the point of NO RETURN
Your Activities:Will_be_Keylogged_and_Timestamped "USER_BEWARE"
Hacking Sites: https://sites.google.com/site/lazyboxx * http://www.freebsd.org
Tasks: 94; 2 running
Load average: 1.38 1.44 1.14
Uptime: 3 days, 10:05:46
Hostname: core
USER PID NI S CPU% MEM% TIME+ Command
4:29/4:58 Hearts Burst Into Fire
[playing] Bullet For My Valentine (2008-01-23)
Vol: 22%
Playlist tems, length: 57 minutes, 11 seconds :: remaining: 4
Time Artist Title/Filename Album
4:27 Bullet For My Scream Aim Fire Scream Aim Fire
4:03 Bullet For My Eye Of The Storm Scream Aim Fire
4:58 Bullet For My Hearts Burst Into Fire Scream Aim Fire
4:08 Bullet For My Waking The Demon Scream Aim Fire
Terminal (5)
23:41.23