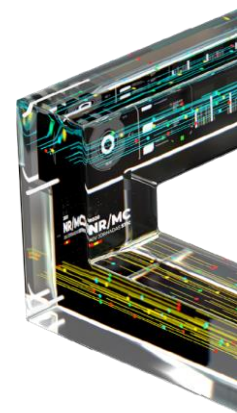
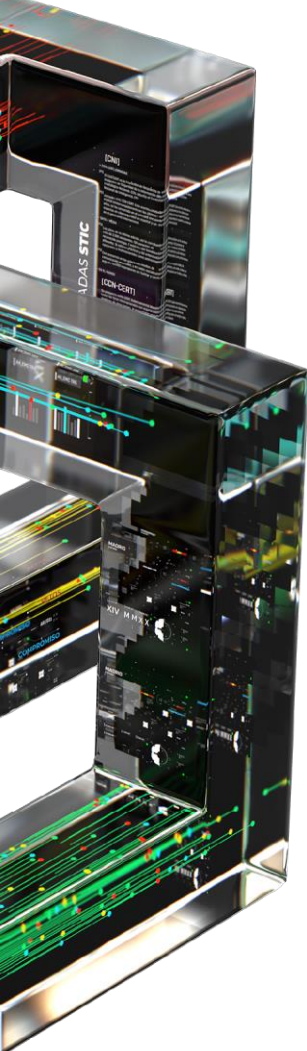


#XIVJORNADASCCNCERT

Automatización de seguridad en la nube





Borja Larrumbide Martinez

***Security Assurance
para Iberia***



***linkedin.com/in/borjal
ensccncert@amazon.com***



Javier Hijas

Cloud Security Partner



linkedin.com/in/javierhijas



Toni de la Fuente

***Senior Security Consultant
Autor de Prowler***



tonfuent@amazon.com

@ToniBlyx

Millones de clientes confían en AWS



Cientes con distintos perfiles de madurez

El conocimiento y la experiencia del cliente varia con el tiempo

1

2

3

Experimentación y POCs



Realojar y logros limitados



Expansión a la nube

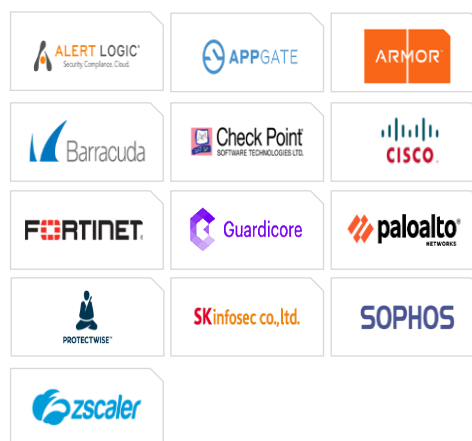


Cientes se apoyan en ...

AWS

- AWS Well-Architected Framework
- AWS Well-Architected tool
- AWS Cloud Adoption Framework
- AWS Trainings & Certifications
- AWS Professional Services
- AWS Support Services
- AWS Guidelines
- AWS Partners Solutions

Network & infrastructure security



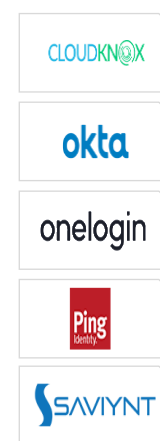
Host & endpoint security



Application security



Identity & access control



Vulnerability & configuration analysis



Logging, monitoring, SIEM, threat detection, & analytics



También en nuestros Partners Consultores

Security engineering

Governance, risk, & compliance

Security operations & automation

8K Miles

accenture
High performance. Delivered.

AllCloud

>CMD
SOLUTIONS

CLOUDZONE
by matrix

cloudten

Deloitte.

ECCOiii
华讯网络

escaia
24x7

FOGHORN

GuidePoint
SECURITY

HELECLOUD

Hewlett Packard
Enterprise

Itoc

lightstream

logicworks

NRI

pwc

Smartronix
CLOUD ASSURED

1

Eleven
Paths
"Advanced" cyber security company

VERSANT

direktgruppe

Booz | Allen | Hamilton

Cloudgotech

cavirin

CloudCheckr

CloudHealth[™]
by vmware[™]

CloudPassage

CALFIRE

DivvyCloud
Cloud Automation Reimagined

ECCOiii
华讯网络

Flux7
an NTT DATA Company

KindlyOps

OPTIV

pwc

lock

Telos

TREND
MICRO

turbot

wirewheel

direktgruppe

stackArmor

Cloudreach

ECCOiii
华讯网络

eCloud
valley

Mphasis
stelligent.
The Next Applied

pwc

SAMSUNG
SAMSUNG SDS

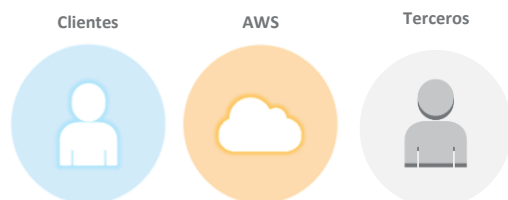
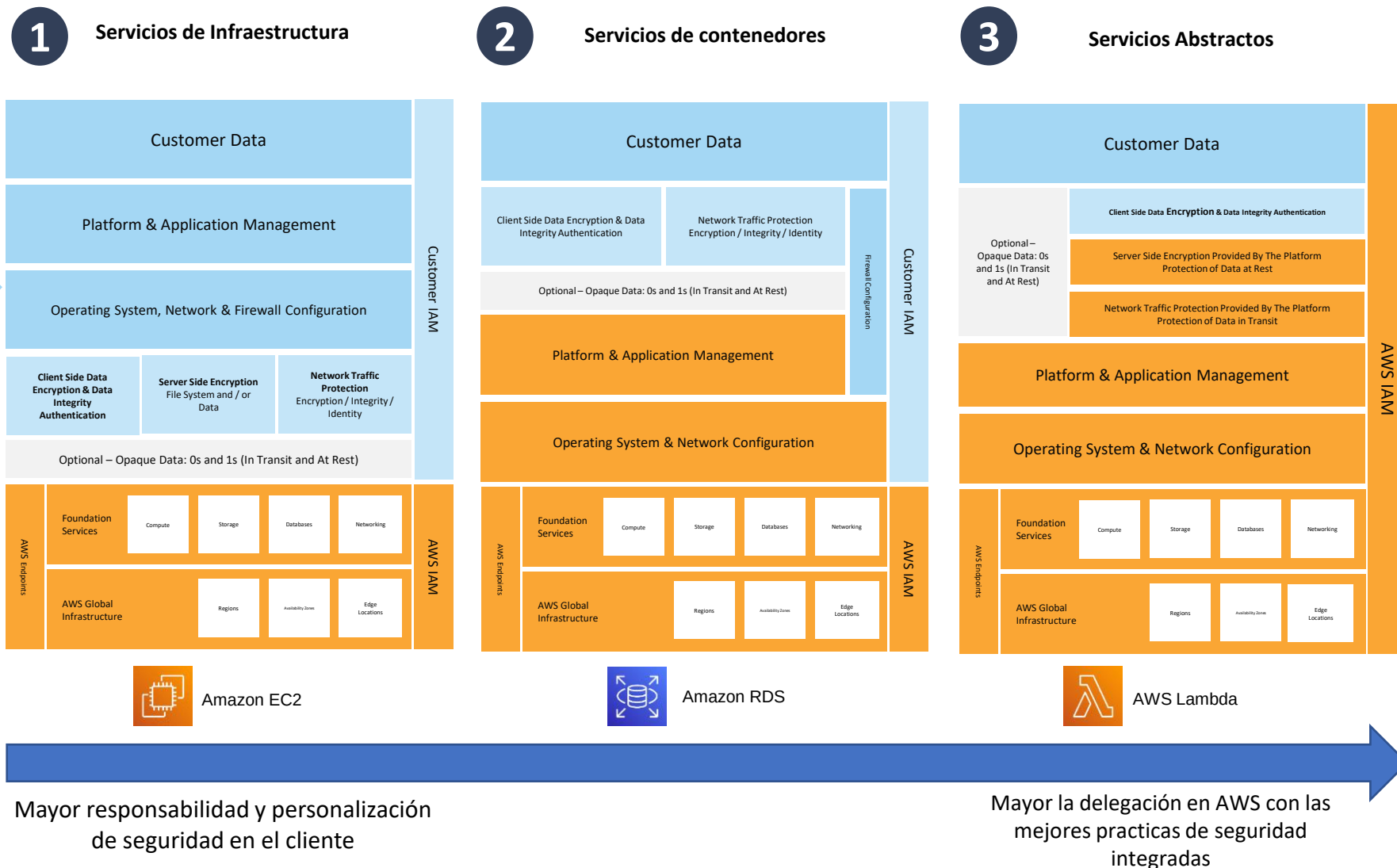
La responsabilidad es compartida y varía

“La forma en la que uno adapta su Seguridad y cumplimiento de los controles va a depender del modelo de responsabilidad compartida”

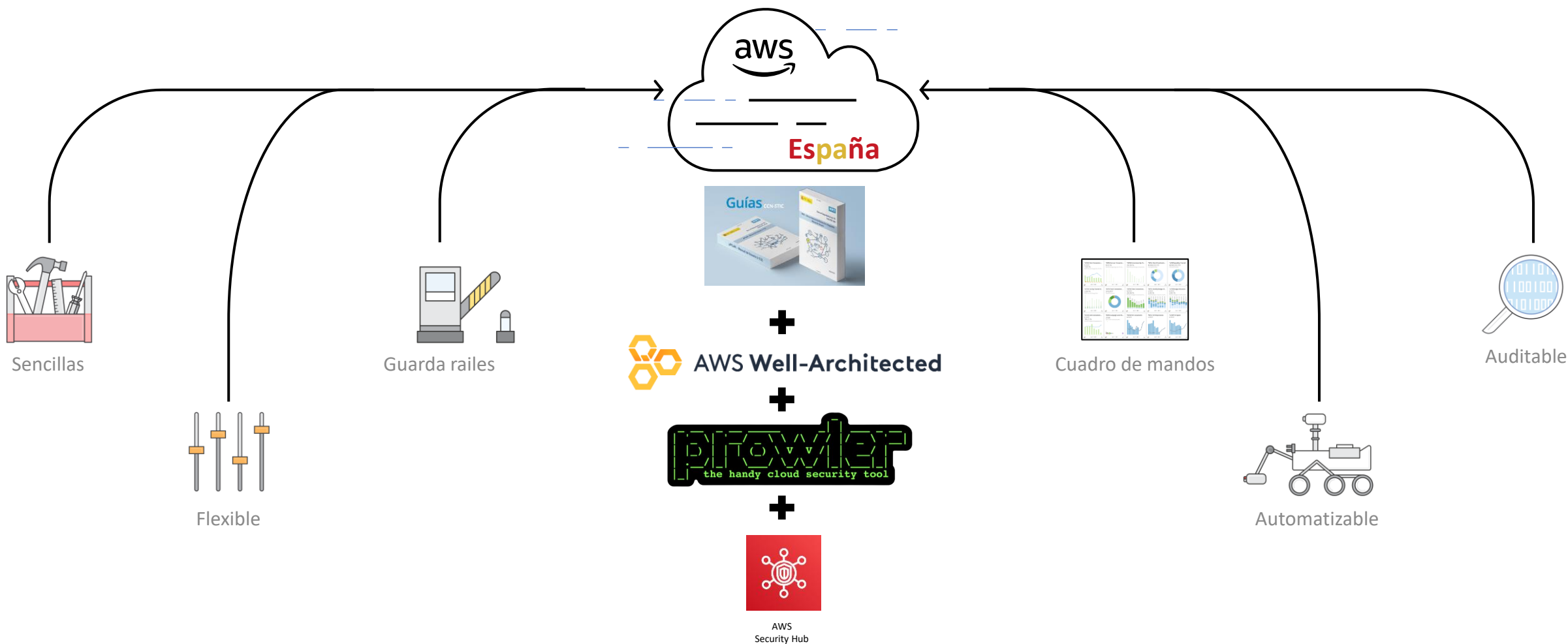
¿Que podemos ofrecer adicionalmente a nuestros clientes para ayudarles a cumplir con el ENS?



Nivel Alto



Guías STIC del ENS para AWS con ñ



Esto solo es el comienzo



AWS Security Hub
AWS Organizations



AWS Control Tower
AWS Trusted Advisor



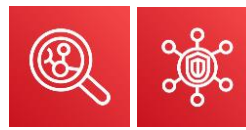
AWS Transit Gateway
Amazon VPC
AWS IoT Device Defender
Amazon Cloud Directory



Amazon VPC PrivateLink
AWS Direct Connect
Resource Access manager
AWS Directory Service



Amazon GuardDuty
Amazon Macie



Amazon Inspector
AWS Security Hub



Amazon CloudWatch
AWS Step Functions



AWS Systems Manager
AWS Lambda



AWS OpsWorks

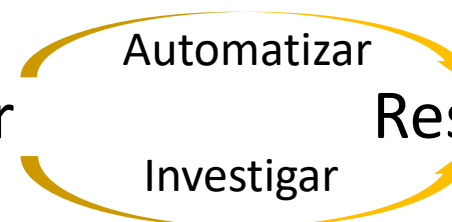


AWS CloudFormation

Identificar ➡

Proteger ➡

Detectar



Responder ➡

Recuperar



AWS Service Catalog
AWS Config



AWS Well-Architected Tool
AWS Systems Manager



AWS Shield



IAM



AWS Secrets Manager



KMS



Amazon Cognito



AWS WAF



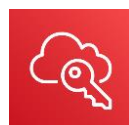
AWS Firewall Manager



AWS Certificate Manager



AWS CloudHSM



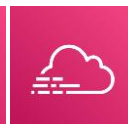
AWS Single Sign-On



Amazon Detective



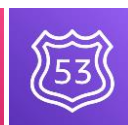
Amazon CloudWatch



AWS CloudTrail



Personal Health Dashboard



Amazon Route 53



Amazon S3 Glacier

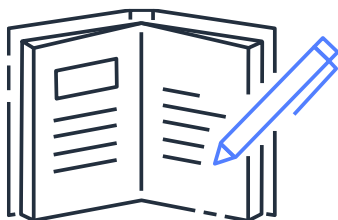


Snapshot



Archive

Regreso al futuro 1



Medidas de protección
de la información, de
servicios, de escenarios...



AWS
Security Hub



AWS Config



Cumplimiento
del ENS

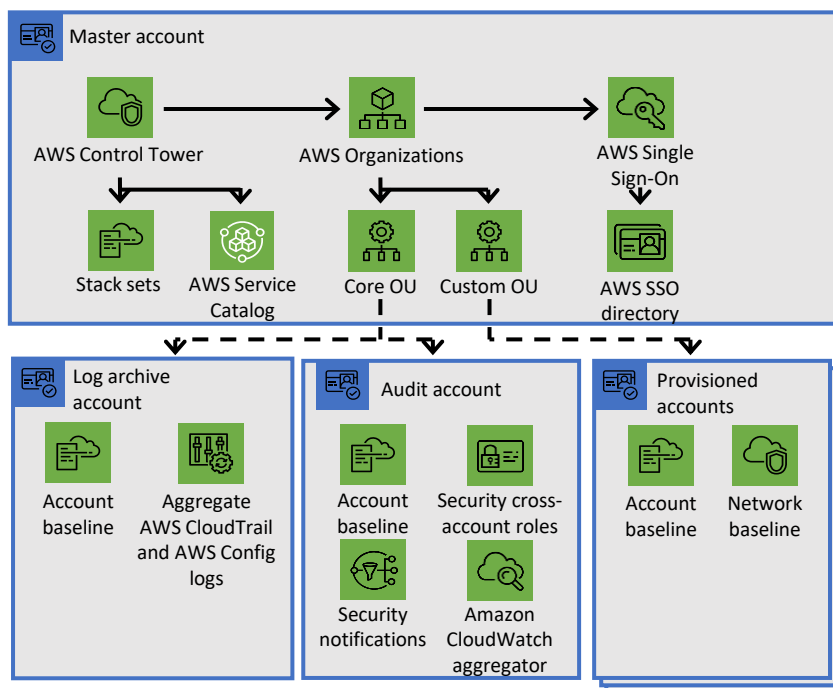


Regreso al futuro 2

Amazon
Machine Image

Amazon
CloudFormation

Containers



aws marketplace



AWS Quickstarts
cumplimiento
con el ENS

¿Estas interesado en participar o sugerir ideas?

Email: ensccncert@amazon.com

Regreso al futuro 3

- Guías del ENS
- Herramientas del ENS
- Certificados del ENS
- ENS Quickstarts y AMIs
- AWS Marketplace del ENS

Landing zone del ENS en AWS



The screenshot shows the AWS ENS landing page. At the top is the AWS navigation bar with links like 're:Invent', 'Productos', 'Soluciones', 'Precios', 'Documentación', 'Aprender', 'Red de socios', 'AWS Marketplace', 'Capacitación para clientes', and 'Más información'. Below this is a secondary navigation bar with 'Conformidad', 'Seguridad', 'Programas de conformidad', 'Recursos', 'Novedades', and 'Privacidad'. The main header features a large image of a classical building facade with columns and a statue, with the text 'Esquema Nacional de Seguridad (categoría Alta)' overlaid. The page is divided into two main sections: 'Información general' on the left and 'Recursos del ENS' on the right. The 'Información general' section includes a certification logo and a paragraph explaining that AWS has achieved high-level ENS certification, defining security standards for government agencies and public organizations. Below this are four expandable FAQ items: '¿Qué es la certificación de categoría alta del ENS?', '¿Quién creó el estándar de categoría alta del ENS?', '¿Qué regiones de AWS abarca la certificación de categoría alta del ENS?', and '¿Qué servicios de AWS abarca la certificación de categoría alta del ENS?'. The 'Recursos del ENS' section lists three resources: 'Certificado de categoría alta del ENS', 'ENS - Certificaciones del Esquema Nacional de Seguridad 27001', and 'Introducción del Centro Criptológico Nacional'.

Más novedades en el AWS INITIATE 2021



**Próximamente se anunciara AWS Initiate – Madrid
28 de Enero de 2021**

Con Pablo Lopez del CCN-CERT y Borja Larrumbide de AWS

davinci group

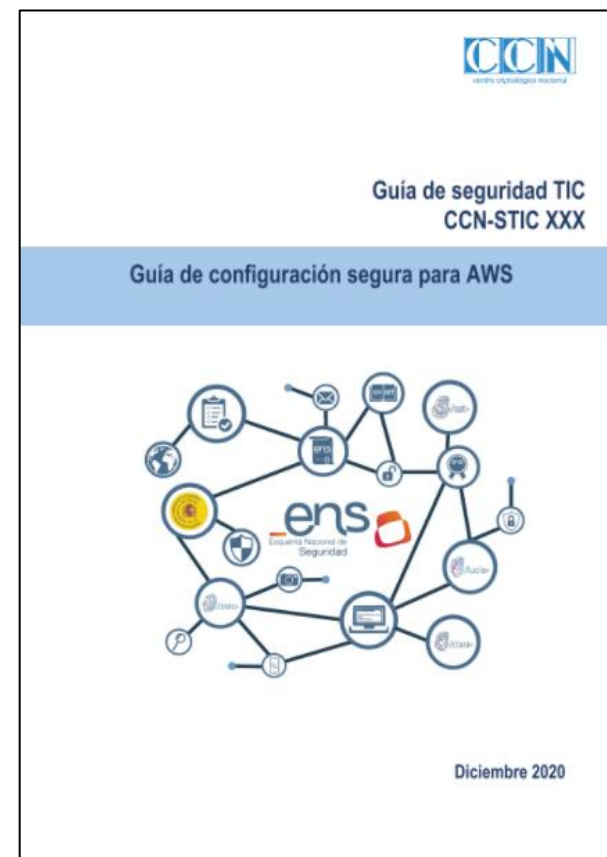


Secure Digital Cloud Platforms

Guías de configuración segura para AWS

Nuevas guías

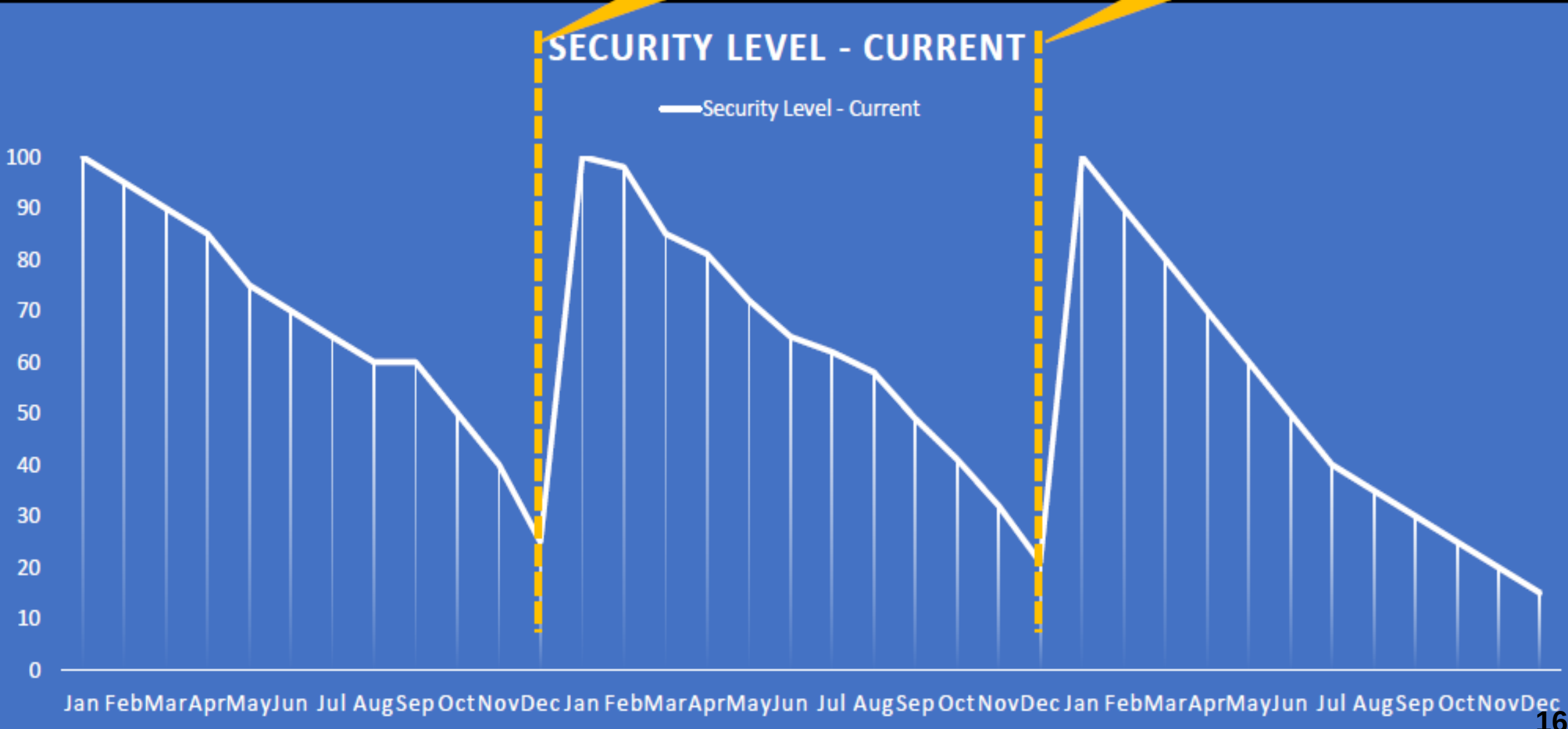
Nuevo concepto



Aproximación Tradicional a la seguridad

¡¡Nueva Auditoría!!

¡¡Nueva Auditoría!!



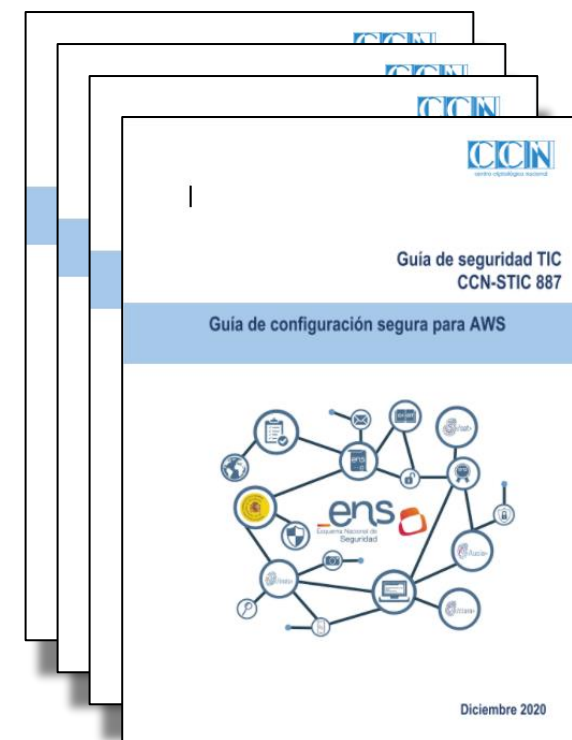
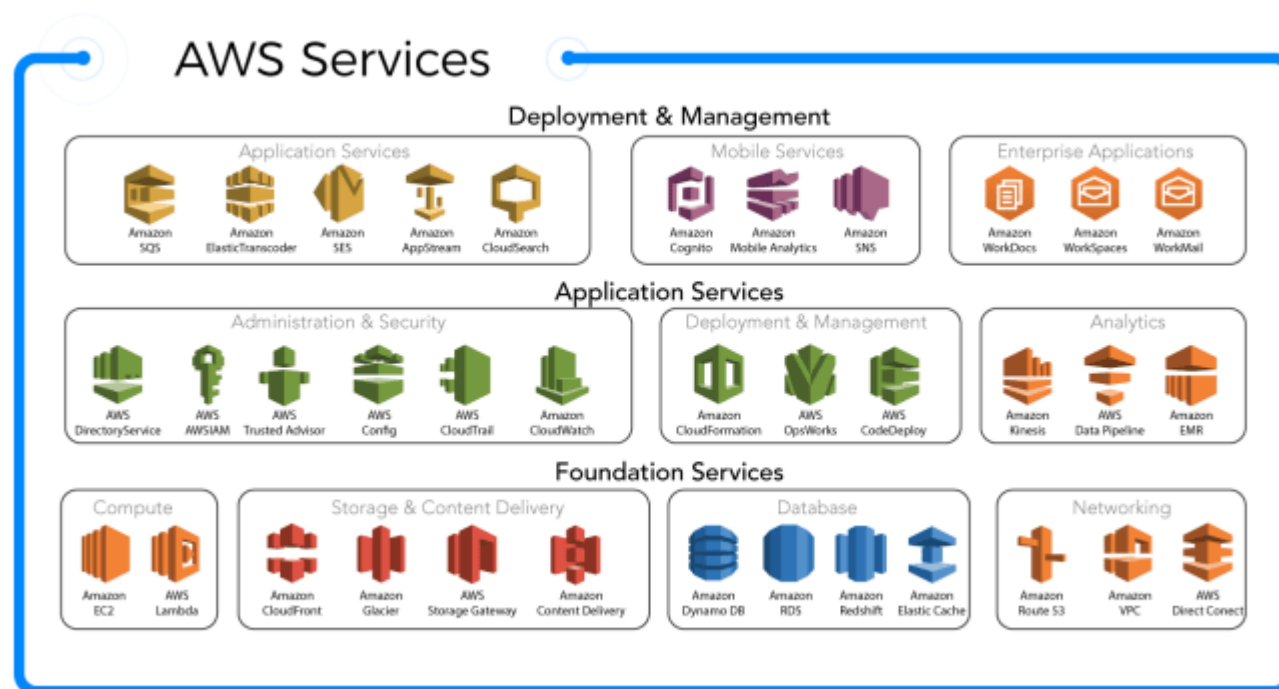
#XIVJORNADASCCNCERT

Medidas ENS y AWS Well-Architected

CCN-STIC XXX	ens	USO OFICIAL
Guía de configuración segura para AWS		
ÍNDICE		
1. GUÍA DE CONFIGURACIÓN SEGURA PARA AWS		7
1.1. DESCRIPCIÓN DEL USO DE ESTA GUÍA		7
1.2 DEFINICIÓN DEL SERVICIO		7
1.3 MODELO DE SEGURIDAD COMPARTIDA		7
1.4 FUNCIONALIDADES DEL SERVICIO DE AWS		9
2. DESPLIEGUE SEGURO PARA AWS		9
Información precisa de cuenta		10
Métodos de pago		10
Activación de servicios de seguridad		11
Entornos multi-cuenta		11
3. CONFIGURACIÓN SEGURA PARA AWS		11
3.1 MARCO OPERACIONAL		11
3.1.1 Control de Acceso		11
3.1.1.1 Identificación		12
3.1.1.2 Requisitos de acceso		14
3.1.1.3 Segregación de funciones y tareas		16
3.1.1.4 Proceso de gestión de derechos de acceso		17
3.1.1.5 Mecanismos de autenticación		18
3.1.1.6 Acceso Local y Remoto		21
3.1.2 Explotación		23
3.1.2.1 Inventario de activos		23
3.1.2.2 Mantenimiento		25
3.1.2.3 Registro de la actividad de los usuarios		27
3.1.2.4 Protección de los registros de actividad		29
3.1.2.5 Protección de claves criptográficas		30

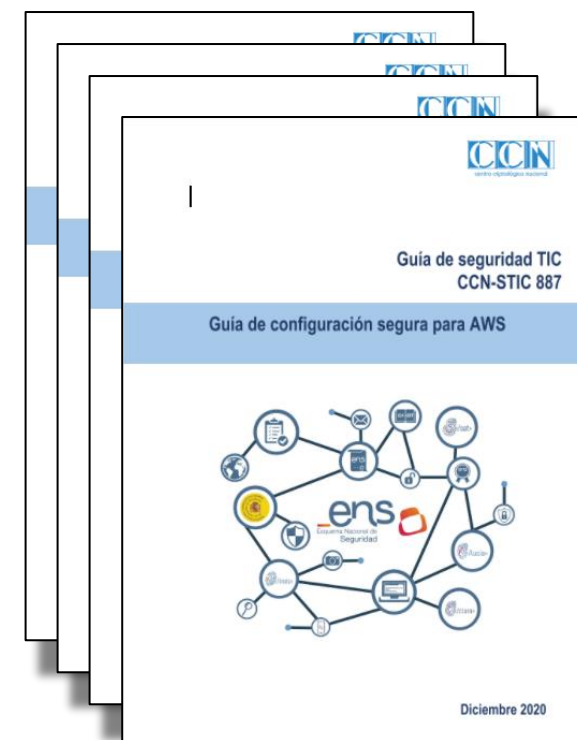


Servicios AWS y hoja de ruta



Servicios AWS y hoja de ruta

ANALYTICS ANALYTICS DATA EXCHANGE DATA LAKE DATA PIPELINES DATA WAREHOUSE ELASTICSEARCH STREAMING KTL HADOOP/SPARK INTERACTIVE SQL QUERIES VISUALIZATIONS	COMPUTE COMPUTE AUTO SCALING BATCH JOBS EVENT-DRIVEN SERVERLESS COMPUTING INSTANCE TYPES MANAGED VIRTUAL PRIVATE SERVERS MANAGED REPOSITORY FOR SERVERLESS APPS RUN & MANAGE WEB APPS SERVERLESS COMPUTE VIRTUAL SERVERS CONTAINERS CONTAINER SERVICE KUBERNETES STORE & RETRIEVE DOCKER IMAGES	END USER COMPUTING APP STREAMING DESKTOP COMPUTING MOBILE ACCESS STORAGE & COLLABORATION HYBRID ARCHITECTURE AWS SERVICES ON PREMISES DATA INTEGRATION INTEGRATED DEVICES & EDGE SYSTEMS INTEGRATED IDENTITY & ACCESS INTEGRATED NETWORKING INTEGRATED RESOURCE & DEPLOYMENT MANAGEMENT VMWARE CLOUD ON AWS	MACHINE LEARNING ML FRAMEWORKS DEEP LEARNING AMI & CONTAINERS HARDWARE ACCELERATION ML AT THE EDGE TENSORFLOW, PYTORCH, MXNET SAGEMAKER AUTOMATIC MODEL TUNING DATA LABELING HOSTED NOTEBOOKS ML MARKETPLACE MODEL HOSTING MODEL OPTIMIZATION MODEL TRAINING PRE-BUILT ALGORITHMS TOPIC MODELING DEEP LEARNING MODELS REINFORCEMENT LEARNING SPOT INSTANCES BATCH PREDICTIONS REAL-TIME PREDICTIONS CHATBOTS ENTITY EXTRACTION FACE ANALYTICS FACE SEARCH FORECASTING IMAGE LABELING NATURAL LANGUAGE PROCESSING PERSONALIZATION & RECOMMENDATION SENTIMENT ANALYSIS SPEECH TRANSCRIPTION TEXT & DATA EXTRACTION TEXT TO SPEECH TRANSLATION VIDEO & IMAGE ANALYSIS CONTENT MODERATION	MEDIA SERVICES LIVE VIDEO TRANSPORT MEDIA STORAGE TRANSCODING VIDEO ORIGINATOR & PACKAGING VIDEO PERSONALIZATION & MONETIZATION VIDEO PROCESSING & DELIVERY VIDEO STREAMING ANALYSIS MIGRATION & TRANSFER APPLICATION MIGRATION DATABASE MIGRATION EXABYTE-SCALE MIGRATION ONLINE DATA TRANSFER SCHEMA CONVERSION SERVER MIGRATION TRANSFER FOR SFTP	SATELLITE SATELLITE OPERATIONS SECURITY, IDENTITY, & COMPLIANCE ACCESS CONTROL ASSESSMENT & REPORTING CONFIGURATION COMPLIANCE DATA PROTECTION DDOS PROTECTION IDENTITY MANAGEMENT KEY MANAGEMENT & STORAGE MONITORING & LOGGING RESOURCE MANAGEMENT THREAT DETECTION WEB APPLICATION FIREWALL
AR + VR AR/VR EXPERIENCES	DATABASE REAL-TIME DATABASES HIGH-PERFORMANCE RELATIONAL DATABASE BUILT FOR THE CLOUD MANAGED MARIADB MANAGED MYSQL MANAGED ORACLE MANAGED POSTGRES MANAGED SQL SERVER PURPOSE-BUILT DATABASES DOCUMENT DATABASE GRAPH DATABASE IN-MEMORY CACHING KEY-VALUE STORE DATABASE LEDGER DATABASE TIME SERIES DATABASE	GAME TECH CROSS-PLATFORM 3D GAME ENGINE GAME SERVER HOSTING	INFRASTRUCTURE AVAILABILITY ZONES CUSTOM HARDWARE DATA CENTER INFRASTRUCTURE GLOBAL NETWORK BACKBONE POINTS OF PRESENCE POWER INFRASTRUCTURE REGIONS	MOBILE API GATEWAY DEVELOPMENT FRAMEWORK IDENTITY MOBILE ANALYTICS MOBILE APP TESTING SINGLE INTEGRATED CONSOLE SYNC TARGETED PUSH NOTIFICATIONS	STORAGE ARCHIVE STORAGE BACKUP & RESTORE BLOCK STORAGE DATA TRANSFER EDGE PROCESSING & COMPUTING FILE STORAGE HIGH-PERFORMANCE FILE SYSTEM HYBRID CLOUD STORAGE OBJECT STORAGE WINDOWS FILE SYSTEM
AWS COST MANAGEMENT ANALYZE AWS COSTS COST & USAGE BUDGETS COST & USAGE REPORTS RESERVED INSTANCES REPORTING	DEVELOPER TOOLS ANALYZE & DEBUG APPLICATION LIFECYCLE MANAGEMENT AUTHORIZING BUILD & TEST CONTAINERS DEVOPS RESOURCE MANAGEMENT ONE-CLICK APP DEVELOPMENT PATCHING PIPELINE ORCHESTRATION RESOURCE TEMPLATES TRIGGERS	INTERNET OF THINGS (IOT) RULES ENGINE DEVICE ANALYTICS DEVICE GATEWAY DEVICE SDK DEVICE SHADOWS EVENT DETECTION & RESPONSE LOCAL COMPUTE LOCAL DATA COLLECTION MANAGEMENT & SECURITY MICROCONTROLLER OPERATING SYSTEM REGISTRY VISUAL APPLICATIONS DEVELOPMENT	MANAGEMENT & GOVERNANCE ACTIVITY & API USAGE TRACKING CHATBOT CONFIGURATION TRACKING GOVERNANCE INVENTORY TRACKING LICENSE MANAGER MANAGE POLICIES MANAGE RESOURCES MONITORING PROVISIONING RESOURCE TEMPLATES SECURITY RECOMMENDATIONS SERVER MANAGEMENT SERVICE CATALOG SYSTEMS MANAGER	NETWORKING & CONTENT DELIVERY APPLICATION DELIVERY DEDICATED NETWORK CONNECTION DOMAIN NAME SYSTEM LOAD BALANCING MONITOR APIS MONITOR MICROSERVICES NETWORK TOPOLOGY NETWORKING HUB PRIVATE CONNECTION TO APPS SCALE VPC & ACCOUNT CONNECTIONS SERVICE DISCOVERY VIRTUAL PRIVATE CLOUD	CUSTOMER ENABLEMENT ACCOUNT MANAGEMENT DASHBOARD PERSONALIZATION ENTERPRISE SUPPORT EXPERTS MARKETPLACE OPTIMIZATION GUIDANCE PARTNER ECOSYSTEMS PROFESSIONAL SERVICES SECURITY & BILLING REPORTS SOLUTIONS MANAGEMENT TRAINING & CERTIFICATION
APPLICATION INTEGRATION EMAIL MESSAGE BROKER QUEUING & NOTIFICATIONS SEARCH TRANSCODING WORKFLOW	BLOCKCHAIN BLOCKCHAIN TEMPLATES LEDGER DATABASE MANAGED BLOCKCHAIN	MARKETPLACE ANALYTICS DATA PRODUCTS DATABASES DEVOPS IOT MACHINE LEARNING NETWORKING OPERATING SYSTEMS SECURITY STORAGE	ROBOTICS CLOUD ROBOTICS		



Automatización

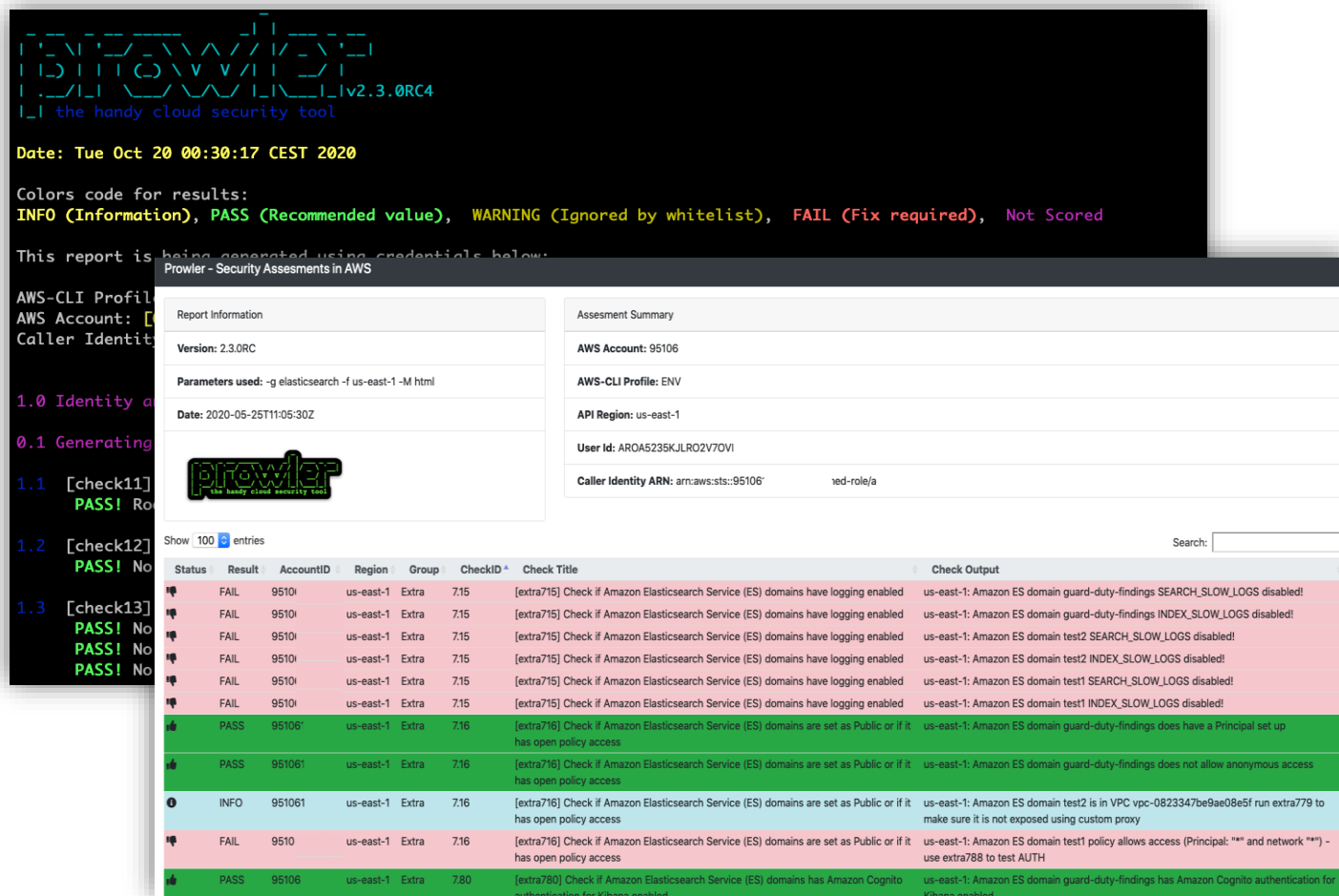


<https://github.com/toniblyx/prowler>

- Herramienta de Software Libre para realizar análisis de seguridad de la infraestructura en AWS
 - Seguridad EN la nube
- Permite realizar el análisis automático de recomendaciones de las nuevas guías del ENS para AWS
- Auditoría y buenas prácticas de seguridad
- Respuesta a incidentes
- Cumplimiento (ENS, PCI-DSS, GDPR, SOC2 y otros)

Automatización

- Integración en el ecosistema de servicios de seguridad de AWS
 - Security Hub
- Integración con API de Ana
- Mas de 170 controles
- Generar informes: html, pdf, texto
- Formatos: CSV, JSON, JSON-ASFF, Junit-xml
- Monitorización continua
- Análisis automático o manual
 - Completo o específico



The image shows the Prowler security assessment tool. On the left, a terminal window displays the ASCII art logo for Prowler, version 2.3.0RC4, and the date Tue Oct 20 00:30:17 CEST 2020. It also shows the colors code for results: INFO (Information), PASS (Recommended value), WARNING (Ignored by whitelist), FAIL (Fix required), and Not Scored. The terminal output shows the results of a security assessment for AWS account 95106, with checks 1.1, 1.2, and 1.3 all passing.

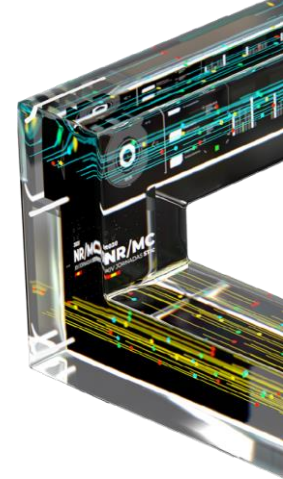
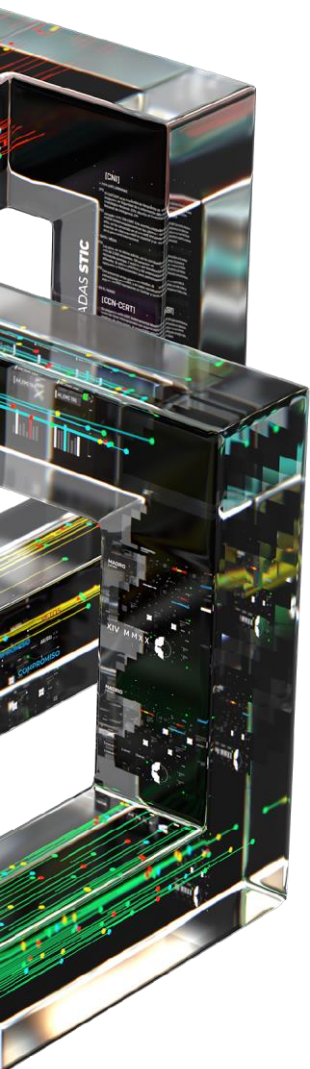
On the right, the Prowler web interface displays the assessment summary for AWS account 95106. The summary includes the AWS CLI Profile (ENV), API Region (us-east-1), User Id (AROAS23SKJLR02V70VI), and Caller Identity ARN (arn:aws:sts::95106:assumed-role/a). Below the summary, a table shows the results of the security assessment, with columns for Status, Result, AccountID, Region, Group, CheckID, Check Title, and Check Output.

Status	Result	AccountID	Region	Group	CheckID	Check Title	Check Output
FAIL	95106	us-east-1	Extra	7.15	[extra715] Check if Amazon Elasticsearch Service (ES) domains have logging enabled	us-east-1: Amazon ES domain guard-duty-findings SEARCH_SLOW_LOGS disabled!	
FAIL	95106	us-east-1	Extra	7.15	[extra715] Check if Amazon Elasticsearch Service (ES) domains have logging enabled	us-east-1: Amazon ES domain guard-duty-findings INDEX_SLOW_LOGS disabled!	
FAIL	95106	us-east-1	Extra	7.15	[extra715] Check if Amazon Elasticsearch Service (ES) domains have logging enabled	us-east-1: Amazon ES domain test2 SEARCH_SLOW_LOGS disabled!	
FAIL	95106	us-east-1	Extra	7.15	[extra715] Check if Amazon Elasticsearch Service (ES) domains have logging enabled	us-east-1: Amazon ES domain test2 INDEX_SLOW_LOGS disabled!	
FAIL	95106	us-east-1	Extra	7.15	[extra715] Check if Amazon Elasticsearch Service (ES) domains have logging enabled	us-east-1: Amazon ES domain test1 SEARCH_SLOW_LOGS disabled!	
FAIL	95106	us-east-1	Extra	7.15	[extra715] Check if Amazon Elasticsearch Service (ES) domains have logging enabled	us-east-1: Amazon ES domain test1 INDEX_SLOW_LOGS disabled!	
PASS	95106	us-east-1	Extra	7.16	[extra716] Check if Amazon Elasticsearch Service (ES) domains are set as Public or if it has open policy access	us-east-1: Amazon ES domain guard-duty-findings does have a Principal set up	
PASS	95106	us-east-1	Extra	7.16	[extra716] Check if Amazon Elasticsearch Service (ES) domains are set as Public or if it has open policy access	us-east-1: Amazon ES domain guard-duty-findings does not allow anonymous access	
INFO	95106	us-east-1	Extra	7.16	[extra716] Check if Amazon Elasticsearch Service (ES) domains are set as Public or if it has open policy access	us-east-1: Amazon ES domain test2 is in VPC vpc-0823347be9ae08e5f run extra779 to make sure it is not exposed using custom proxy	
FAIL	95106	us-east-1	Extra	7.16	[extra716] Check if Amazon Elasticsearch Service (ES) domains are set as Public or if it has open policy access	us-east-1: Amazon ES domain test1 policy allows access (Principal: "*" and network "*") - use extra788 to test AUTH	
PASS	95106	us-east-1	Extra	7.80	[extra780] Check if Amazon Elasticsearch Service (ES) domains has Amazon Cognito authentication for Kibana enabled	us-east-1: Amazon ES domain guard-duty-findings has Amazon Cognito authentication for Kibana enabled	

<https://github.com/toniblyx/prowler>

Demo





MUCHAS GRACIAS

#XIVJORNADASCCNCERT