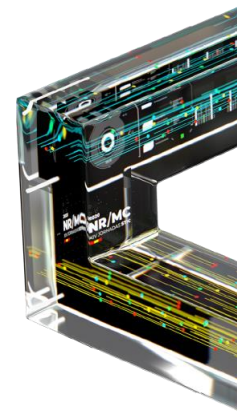


#XIVJORNADASCCNCERT

Modelos de adecuación a la nube





Iván González Vilaboa

Plain Concepts

igonzalez@plainconcepts.com

El reto....

La seguridad de la nube es una Responsabilidad Compartida

2016/2018



#XIVJORNADASCONCERT

Responsibility	SaaS	PaaS	IaaS	On-prem
Data governance & rights management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account & access management	Customer	Customer	Customer	Customer
Identity & directory infrastructure	Customer	Customer	Customer	Customer
Application	Customer	Customer	Customer	Customer
Network controls	Customer	Customer	Customer	Customer
Operating system	Customer	Customer	Customer	Customer
Physical hosts	Microsoft	Microsoft	Microsoft	Customer
Physical network	Microsoft	Microsoft	Microsoft	Customer
Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

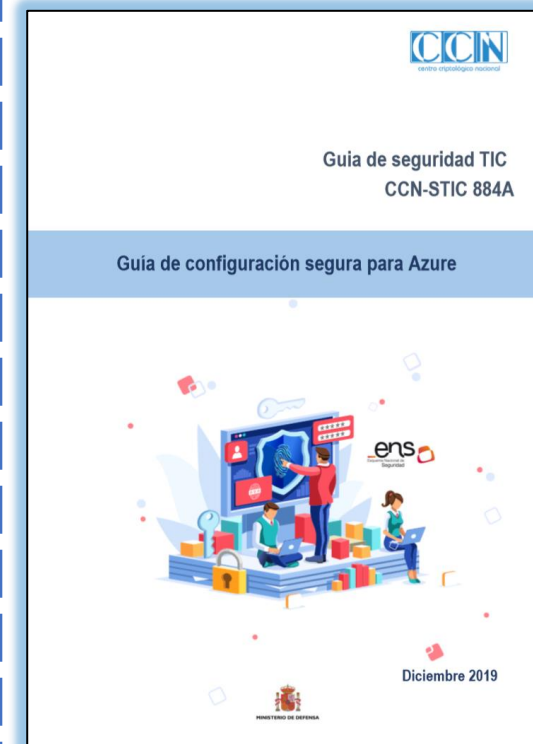
CONTROL

TRUST
but
VERIFY

Microsoft

Customer

2019/2020



Herramientas a nuestra disposición en 2019....

ESTRUCTURA DE LAS GUIAS AZURE

MICROSOFT AZURE- SERIE CCN-STIC-884



CCN-STIC-884A- Guía de configuración segura para Azure



CCN-STIC-884B- Guía de configuración segura para Kubernetes



CCN-STIC-884C- Guía de configuración segura para SQL Database



CCN-STIC-884D- Guía de configuración segura para Cognitive Services

ESTRUCTURA DE LAS GUÍAS OFFICE 365

OFFICE 365 - SERIE CCN-STIC-885



CCN-STIC-885A - Guía de configuración segura para Office 365



CCN-STIC-885B - Guía de configuración segura para Sharepoint Online



CCN-STIC-885C - Guía de configuración segura para Exchange Online



CCN-STIC-885D - Guía de configuración segura para Microsoft Teams

Herramientas a nuestra disposición en 2020....



Le damos la bienvenida a Clara Cloud®
Por favor, introduzca sus datos de
acceso.

Enter username



Enter password



Login



IVAN, bienvenido a Clara Cloud,

Plataforma de Evaluación
de Cumplimiento CLOUD - CCN-STIC 884/885

Comenzar evaluación

© Centro Criptológico Nacional 2020

[Aviso legal](#) • [Política de protección de datos](#) • [Política de cookies](#)



Datos generales



Servicios



Controles



Lanzamiento



Informes

Datos del organismo

Organismo

Plain Concepts

DIR3

ABCD

Datos del responsable de seguridad

Nombre

Iván González

Email

igonzalez@plainconcepts.com

Teléfono de contacto

555 555 555

Siguiente

cn-cert | 

Evaluación | Informes | Guías | **IV**



Datos generales



Servicios



Controles



Lanzamiento



Informes



Buscador de servicios



- ☐ Servicios esenciales
- ☐ Kubernetes
- ☐ Cognitive Services
- ☐ SQL Database



Buscador de servicios



- ☒ Servicios esenciales
- ☐ SharePoint Online
- ☐ Exchange Online
- ☐ Microsoft Teams

Anterior

Siguiente

Datos generales

Servicios

Controles

Lanzamiento

Informes

Office 365 > Servicios Esenciales

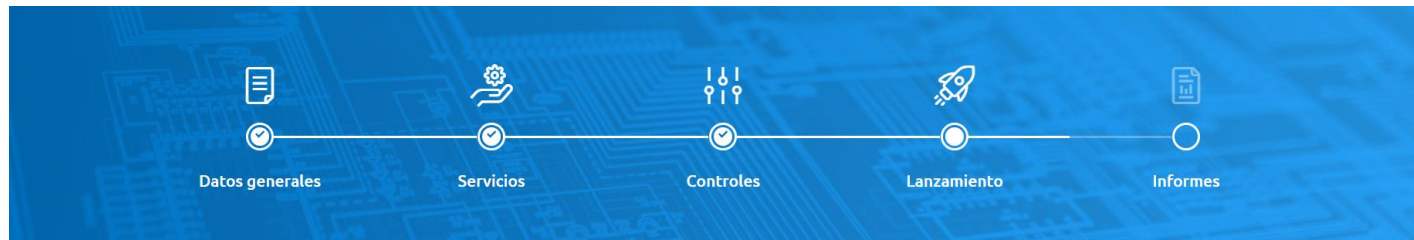
Buscador de controles

Q

Categoría	Control	Aplica
Control de Acceso	Identificación	☒
	Segregación de funciones y tareas	☒
	Mecanismo de autenticación	☒
	Acceso local	☒
	Acceso remoto	☒
Explotación	Protección frente a código dañino	☒
	Protección frente a código dañino - ATP	☒
	Registro de la actividad de los usuarios	☒
	Protección de los registros de actividad	☒
Monitorización	Monitorización del sistema	☒
Protección de la información	Calificación de la información - Políticas de Retención	☒
	Calificación de la información - DLPs	☒
	Calificación de la información - Sensitivity Labels	☒
	Cifrado	☒
	Limpieza de documentos	☒

Anterior

Siguiente



Office365 > Servicios Esenciales



Se va a realizar el lanzamiento del servicio

A continuación deberá introducir un **usuario del tenant con derechos de administración** sobre los servicios que se van a evaluar.

Las credenciales introducidas se usarán para **lanzar el proceso de assesment** y no se almacenarán internamente.

☐ He leído y estoy de acuerdo

Usuario



El campo usuario no es correcto

Password



El campo password no es correcto

Cancelar lanzamiento

Anterior

Lanzamiento

Informes

Filtro



1 - 10 de 30



Auditoría ▾	Organismo ▾	Tenant ▾	Fecha	Tipos		
5290	PLAIN CONCEPTS	plain823.onmicrosoft.com	Nov 30 2020 12:38PM	Ejecutivo 	Técnico 	
5289	PLAIN CONCEPTS	plaincloudlab.onmicrosoft.com	Nov 30 2020 11:26AM	Ejecutivo 	Técnico 	
5288	PLAIN CONCEPTS	plain823.onmicrosoft.com	Nov 30 2020 11:08AM	Ejecutivo 	Técnico 	

Informe ejecutivo de evaluación de cumplimiento

Office 365 > Servicios Esenciales

Imprimir informe PDF

Datos del organismo

Organismo	DIR3	Tenant	GUID Tenant	Fecha	ID
PLAIN CONCEPTS	ABCD	plain823.onmicrosoft.com	182ce8a4-2cb6-4737-848e-5f551f46095c	30 Nov 2020 12:38:29:267	5290

Datos del responsable de seguridad

Nombre	Email	Teléfono de contacto
IVÁN GONZÁLEZ	IGONZALEZ@PLAINCONCEPTS.COM	555 555 555

Panel de control

Puntuación de Cumplimiento

Office 365

60

Cumplimiento de medidas: 9 de 15.
* Máximo 100.

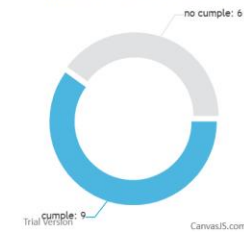
Grado de cumplimiento

Office 365

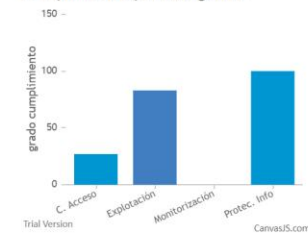
64 %

Media grado de cumplimiento de controles.

Cumplimiento de medidas



Cumplimiento por categorías



Análisis de cumplimiento

Categoría	Control	Cumple
Control de Acceso	Identificación	✗
	Segregación de funciones y tareas	✓
	Mecanismo de autenticación	✗
	Acceso local	✗
	Acceso remoto	✗
Explotación	Protección frente a código dañino	✗
	Protección frente a código dañino - ATP	✓
	Registro de la actividad de los usuarios	✓
	Protección de los registros de actividad	✓
Monitorización	Monitorización del sistema	✗
Protección de la información	Calificación de la información - Políticas de Retención	✓
	Calificación de la información - DLPs	✓
	Calificación de la información - Sensitivity Labels	✓
	Cifrado	✓
	Limpieza de documentos	✓

Control de Acceso
op.acc.5 - Mecanismo de autenticación

Objetivo: Detectar si se ha aplicado Multi-Factor Authentication (MFA) para los usuarios de la organización.

Cumple: **N** Grado de cumplimiento: **0%**

Evidencias:

Número de usuarios globales sin MFA: 7

Número de usuarios globales con MFA: 0

El porcentaje de usuarios globales sin MFA es: 100%

Se recomienda habilitar Multi-Factor Authentication (MFA) para los usuarios de la organización.

Rol: Company Administrator

Ord	Rol	EmailAddress	Displayname	MFA
1	Company Administrator	admin@plain823.onmicrosoft.com	Admin Office 365	Disabled
2	Company Administrator	jose@plain823.onmicrosoft.com	jose	Disabled
3	Company Administrator	ivan@plain823.onmicrosoft.com	ivan	Disabled

Total usuarios sin MFA del rol *Company Administrator*: 3.

Todos los administradores globales deben tener habilitado el MFA.

Recomendaciones:

Es buena práctica requerir MFA en el inicio de sesión para todos los usuarios, pero es necesario al menos para los administradores. El MFA hace que los usuarios escriban un segundo método de identificación para comprobar que son quienes dicen que son.

Explotación

op.exp.6 - Protección frente a código dañino - ATP

Objetivo: Determinar si se comprueba periódicamente la detección de amenazas en tiempo real, accesible desde el Centro de Seguridad y cumplimiento de Office 365, y se genera el informe pertinente. * Si la organización dispone de Office 365 Advanced Threat Protection (Office 365 ATP).

Cumple: **S** Grado de cumplimiento: **100%**

Evidencias:

La organización **dispone** de un licenciamiento para el Service Plan **ATP_ENTERPRISE**.

A continuación se comprueban **políticas ATP de O365**. La Directiva ATP habilita las siguientes protecciones:

- Vínculos seguros para los clientes de escritorio de Office 365 ProPlus y las aplicaciones móviles de Office.
- Documentos seguros: antes de que un usuario pueda confiar en un archivo abierto en Office 365 ProPlus, Microsoft defender ATP comprobará el archivo.
- ATP para proteger los archivos en SharePoint Online, OneDrive para la empresa y Microsoft Teams.

Nombre	IsValid	EnableSafeLinksForO365Clients	EnableSafeLinksForO365Clients	EnableATPForSPOTeamsODB
Default	True	True	True	False

Recomendaciones:

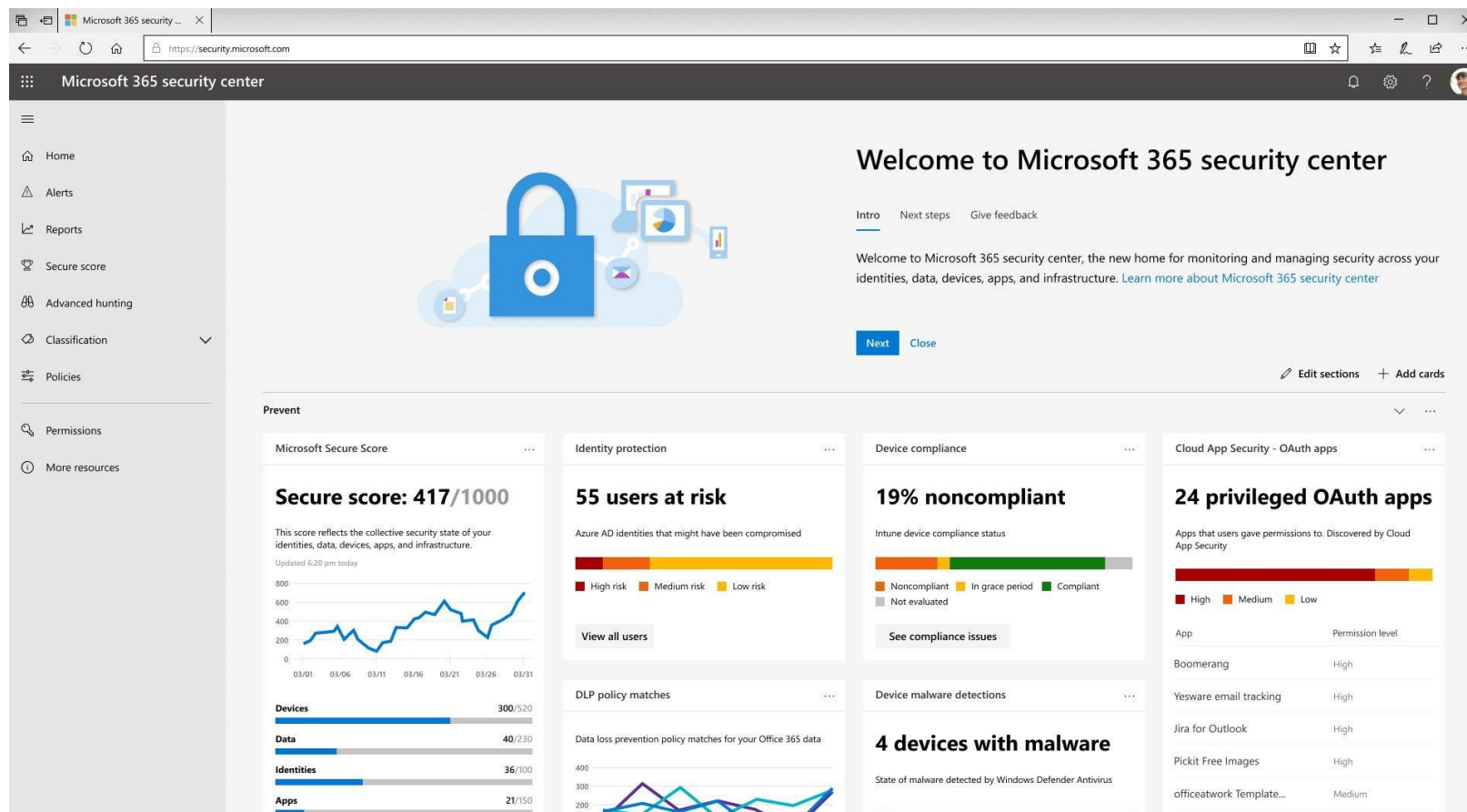
La organización dispone de Office 365 Advanced Threat Protection (Office 365 ATP) y cuenta con un explorador de detecciones en tiempo real, accesible desde el Centro de Seguridad y cumplimiento de Office 365.

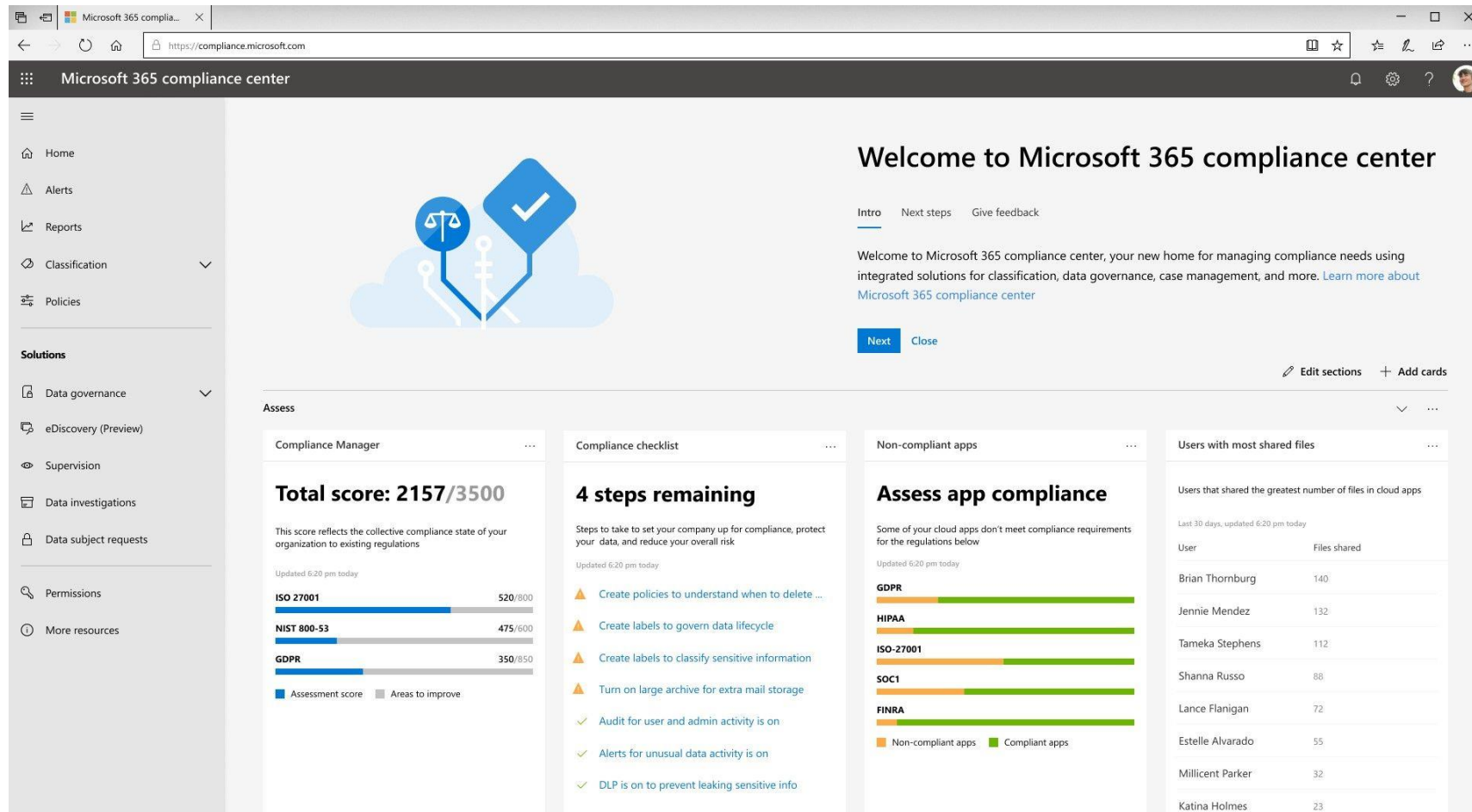
En el explorador [Administración de amenazas\Explorador] se dispone de un informe detallado donde pueden realizarse las siguientes acciones:

- Ver malware detectado por las características de seguridad de Office 365.
- Ver datos sobre direcciones url de suplantación de identidad y hacer clic en veredicto.
- Iniciar un proceso de investigación y respuesta automatizado desde una vista en el explorador.
- Investigar el correo electrónico malintencionado, etc.

Microsoft Compliance Center
Azure Security Center

Otras herramientas a nuestra disposición





The screenshot shows the Microsoft 365 compliance center interface. The left sidebar contains navigation links: Home, Alerts, Reports, Classification, Policies, Solutions (Data governance, eDiscovery (Preview), Supervision, Data investigations, Data subject requests), Permissions, and More resources. The main content area is titled "Welcome to Microsoft 365 compliance center" and includes a "Next" button. Below the welcome message, there are four sections: "Assess" (Total score: 2157/3500), "Compliance checklist" (4 steps remaining), "Non-compliant apps" (Assess app compliance), and "Users with most shared files".

Assess

Compliance Manager

Total score: 2157/3500

This score reflects the collective compliance state of your organization to existing regulations

Updated 6:20 pm today

Standard	Score	Max Score
ISO 27001	520	800
NIST 800-53	475	600
GDPR	350	850

■ Assessment score ■ Areas to improve

Compliance checklist

4 steps remaining

Steps to take to set your company up for compliance, protect your data, and reduce your overall risk

Updated 6:20 pm today

- ▲ Create policies to understand when to delete ...
- ▲ Create labels to govern data lifecycle
- ▲ Create labels to classify sensitive information
- ▲ Turn on large archive for extra mail storage
- ✓ Audit for user and admin activity is on
- ✓ Alerts for unusual data activity is on
- ✓ DLP is on to prevent leaking sensitive info

Non-compliant apps

Assess app compliance

Some of your cloud apps don't meet compliance requirements for the regulations below

Updated 6:20 pm today

Regulation	Non-compliant apps	Compliant apps
GDPR	100%	0%
HIPAA	100%	0%
ISO-27001	100%	0%
SOC1	100%	0%
FINRA	100%	0%

■ Non-compliant apps ■ Compliant apps

Users with most shared files

Users that shared the greatest number of files in cloud apps

Last 30 days, updated 6:20 pm today

User	Files shared
Brian Thornburg	140
Jennie Mendez	132
Tameka Stephens	112
Shanna Russo	88
Lance Flanigan	72
Estelle Alvarado	55
Millicent Parker	32
Katina Holmes	23

Security Center | Overview

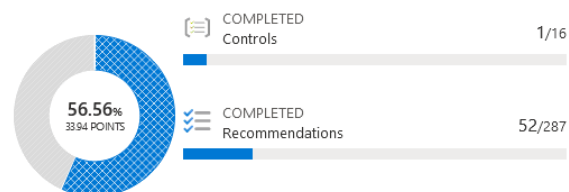
Showing 41 subscriptions

[Subscriptions](#) [What's new](#)

41 Azure subscriptions
1 AWS accounts
3 GCP projects
235 Active recommendations
112 Security alerts

Secure score

Current secure score



[Improve your secure score >](#)

Compliance

Current compliance by passed controls



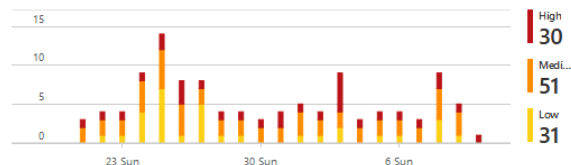
[Improve your compliance >](#)

Azure Defender

Resource Coverage

93% For full coverage turn on 8 resource bundles

Alerts by severity



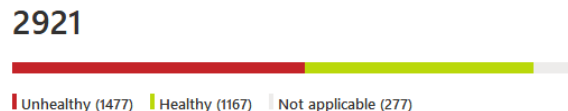
[Enhance your threat protection capabilities >](#)

Inventory

Unmonitored vms

43 For a better protection of your org we recommend to install agents

Total Resources



[Explore your resources >](#)

Insights

Most prevalent recommendations (by resources)

Audit diagnostic setting	686
Disk encryption should be applied on virt...	118
A vulnerability assessment solution shou...	117
Secure transfer to storage accounts shou...	102

Controls with the highest potential increase

Remediate vulnerabilities	+11% (6pt)
Remediate security configurations	+6% (4pt)
Enable encryption at rest	+6% (4pt)

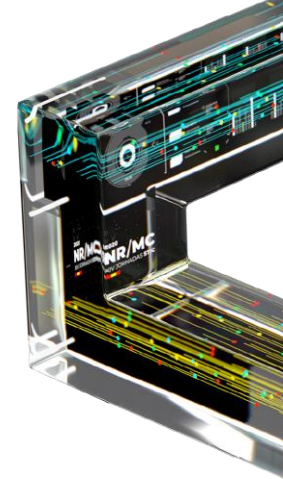
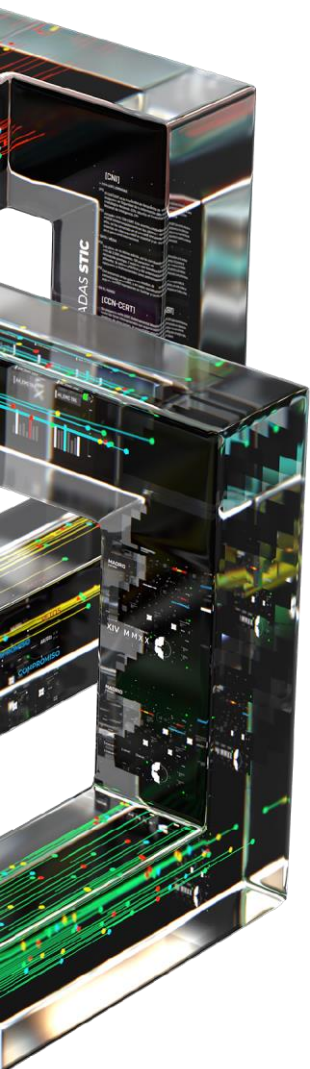
[View controls >](#)

Azure Security Center community

Join the Azure Security Center community on GitHub to interact with other customers and experts and learn, provide feedback, and share knowledge about Security Center.

[View Azure Community >](#)

Herramientas a nuestra disposición en 2021....



MUCHAS GRACIAS

#XIVJORNADASCCNCERT