centro criptológico nacional

Specific Compliance Profile
CCN-STIC 885

Office 365 Specific Compliance Profile
Corporate Cloud Service

December 2019

MINISTERIO DE DEFENSA

Edit:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.06.02 16:01:05 +02'00'

NIPO: 083-19-266-3

Date of Edition: December 2019

LIMITATION OF RESPONSIBILITY

This document is provided in accordance with the terms compiled in it, expressly rejecting any type of implicit guarantee that might be related to it. In no case can the National Cryptologic Centre be considered liable for direct, indirect, accidental or extraordinary damage derived from using information and software that are indicated even when warning is provided concerning this damage.

LEGAL NOTICE

FOREWORD

The current national and international scenario is dominated by developments in Information and Communication Technologies (ICT) and by risks emerging from their use. The Administration is fully aware of this scenario and it is necessary for this body to develop, acquire, conserve and secure use of ICTs to guarantee that its services run effectively for the citizen's and the country's best interests.

Working from the Centre's knowledge and experience on threats and vulnerabilities in terms of emerging risks, Law 11/2002, dated 6th May, regulating the National Intelligence Centre, entrusts the National Intelligence Centre the functions related to information technology security, according to the Article 4.e), and to the protection of classified information, according to the Article 4.f). It also gives, through the Article 9.2.f), its Secretary of State-Director the responsibility of managing the National Cryptologic Centre.

One of the most outstanding functions that it assigns to it, in Royal Decree 421/2004, dated 12th March, regulating the National Cryptologic Centre is to draw up and disseminate standards, instructions, guides and recommendations to guarantee security for the Administration's information and communication technologies.

Royal Decree 3/2010, dated 8th January, develops the National Security Framework (hereinafter called ENS) in the field of Electronic Administration which is also referred in the second section of Article 156 of Law 40/2015, dated 1st October, of the Public Sector Legal System. The National Security Framework establishes the security policy, in matters of use of electronic means, which ensures the protection of information.

Indeed, Royal Decree 3/2010, dated 8th January, updated by Royal Decree 951/2015, dated 23rd October, sets the basic principles and minimum requirements as well as any protection measures to be introduced in Administration systems. In article 29, it authorises the CCN to develop CIS guidelines to ease the fulfilment of these minimum requirements.

The CCN-STIC documents series was drawn up to comply with this function and the ENS, aware of the importance of establishing a frame of reference on this matter that can be used as support so that Administration staff can carry out their difficult and occasionally thankless task of providing security for ICT systems within their responsibility.

July 2019

Felix Sanz Roldan
Secretary of State
Director of the National Cryptologic Centre

INDEX

1. INTRODUCTION

1. Under the principle of proportionality and in order to facilitate compliance with the National Security Framework (ENS) for certain entities or sectors of activity, specific compliance profiles may be implemented, comprising a set of security measures which, as a result of the required risk analysis, are applicable to a specific security category.

2. A specific compliance profile is a set of security measures, whether or not included in Royal Decree 3/2010 of 8 January, which, as a result of the required risk analysis, are applicable to a specific entity or sector of activity and for a specific security category.

3. The CCN-STIC Guidelines of the National Cryptologic Centre can establish specific compliance profiles for specific entities or sectors, which will include the list of measures and reinforcements that are applicable in each case, or the criteria for their determination.

4. The National Cryptologic Centre, in the exercise of its competences, will validate and publish the corresponding specific compliance profiles that are defined, allowing those entities included in its scope to achieve a better and more efficient adaptation to the ENS, rationalising the required resources without undermining the protection pursued and demanded.

5. The audits will be carried out according to the category of the system and, if applicable, the specific compliance profile that corresponds, as provided in Annex I and Annex III of Royal Decree 3/2010, of 8 January, and in accordance with the provisions of the Technical Instruction on Information Systems Security Audit.

6. To this end, after performing a risk analysis considering the vulnerabilities and threats faced by the use of this technology in Public Sector entities, and in order to ensure the highest security of information systems, the mandate imposed to the CCN is fulfilled by validating the **following Specific Compliance Profile to ensure security in the services contracted in the Microsoft Azure Cloud in the PaaS, IaaS and SaaS modalities**.

2. INVOLVED TECHNOLOGIES

7. This compliance profile can be applied to all those entities whose information system, after a correct categorisation process, obtains HIGH level security needs or lower, and the services of which this information system is composed only correspond to those offered by the Microsoft Office 365 Cloud solution, in its deployment mode as a public cloud and offering Software as a Service (SaaS) services.

8. In accordance with the provisions of *CCN-STIC 823* ICT Security Guide *Using Cloud Services,* clouds with public deployment models are defined as those whose infrastructure is offered to the general public or a large group of industries, and this infrastructure is controlled by a cloud service provider.

9. For the application of this Specific Compliance Profile, the Microsoft Office 365 Cloud solution offers services whose systems are ENS certified in the HIGH category.

3. STATEMENT OF APPLICABILITY

10. The declaration of applicability is the set of measures that apply to compliance with the ENS. The set of measures will depend on the levels associated with the security dimensions.

11. It has been determined that, for services contracted in the Microsoft Office 365 Cloud, the measures that are applicable or not and, if applicable, the requirement in terms of maturity level of the measure is as follows:

Dimensions					
Affected	CAT B	CAT M	CAT A		
				org	Application
category	apply	=	=	[org.1]	HIGH
category	apply	=	=	[org.2]	HIGH
category	apply	=	=	[org.3]	HIGH
category	apply	=	=	[org.4]	HIGH
category	apply	+	++	[op.pl.1]	HIGH
category	apply	+	++	[op.pl.2]	HIGH
category	apply	=	=	[op.pl.3]	HIGH
D	n.a.	apply	=	[op.pl.4]	HIGH
category	n.a.	n.a.	apply	[op.pl.5]	HIGH
A T	apply	=	=	[op.acc.1]	HIGH
I C A T	apply	=	=	[op.acc.2]	HIGH
I C A T	n.a.	apply	=	[op.acc.3]	HIGH
I C A T	apply	=	=	[op.acc.4]	HIGH
I C A T	apply	+	++	[op.acc.5]	HIGH
I C A T	apply	+	++	[op.acc.6]	HIGH
I C A T	apply	+	=	[op.acc.7]	HIGH
category	apply	=	=	[op.exp.1]	HIGH
category	apply	=	=	[op.exp.2]	HIGH
category	n.a.	apply	=	[op.exp.3]	HIGH
category	apply	=	=	[op.exp.4]	HIGH
category	n.a.	apply	=	[op.exp.5]	HIGH
category	apply	=	=	[op.exp.6]	HIGH
category	n.a.	apply	=	[op.exp.7]	HIGH
T	apply	+	++	[op.exp.8]	HIGH
category	n.a.	apply	=	[op.exp.9]	HIGH
T	n.a.	n.a.	apply	[op.exp.10]	HIGH

category	apply	+	=	[op.exp.11]	HIGH
category	n.a.	apply	=	[op.ext.1]	HIGH
category	n.a.	apply	=	[op.ext.2]	HIGH
D	n.a.	n.a.	apply	[op.ext.9]	n/a*
D	n.a.	apply	=	[op.cont.1]	n/a
D	n.a.	n.a.	apply	[op.cont.2]	n/a
D	n.a.	n.a.	apply	[op.cont.3]	n/a
category	n.a.	apply	=	[op.mon.1]	HIGH
category	apply	+	++	[op.mon.2]	HIGH

category	apply	=	=	[mp.if.1]	n/a*
category	apply	=	=	[mp.if.2]	n/a*
category	apply	=	=	[mp.if.3]	n/a*
D	apply	+	=	[mp.if.4]	n/a*
D	apply	=	=	[mp.if.5]	n/a*
D	n.a.	apply	=	[mp.if.6]	n/a*
category	apply	=	=	[mp.if.7]	n/a*
D	n.a.	n.a.	apply	[mp.if.9]	n/a*
category	n.a.	apply	=	[mp.per.1]	HIGH
category	apply	=	=	[mp.per.2]	HIGH
category	apply	=	=	[mp.per.3]	HIGH
category	apply	=	=	[mp.per.4]	HIGH
D	n.a.	n.a.	apply	[mp.per.9]	n/a
category	apply	+	=	[mp.eq.1]	HIGH
A	n.a.	apply	+	[mp.eq.2]	HIGH
category	apply	=	+	[mp.eq.3]	HIGH
D	n.a.	apply	=	[mp.eq.9]	HIGH
category	apply	=	+	[mp.com.1]	HIGH
C	n.a.	apply	+	[mp.com.2]	HIGH
I A	apply	+	++	[mp.com.3]	HIGH
category	n.a.	n.a.	apply	[mp.com.4]	HIGH
D	n.a.	n.a.	apply	[mp.com.9]	n/a
C	apply	=	=	[mp.si.1]	HIGH
I C	n.a.	apply	+	[mp.si.2]	HIGH
category	apply	=	=	[mp.si.3]	HIGH
category	apply	=	=	[mp.si.4]	HIGH
C	apply	+	=	[mp.si.5]	HIGH
category	n.a.	apply	=	[mp.sw.1]	HIGH
category	apply	+	++	[mp.sw.2]	HIGH
category	apply	=	=	[mp.info.1]	HIGH
C	apply	+	=	[mp.info.2]	HIGH

C	n.a.	n.a.	apply	[mp.info.3]	HIGH
I A	apply	+	++	[mp.info.4]	n/a*
T	n.a.	n.a.	apply	[mp.info.5]	n/a
C	apply	=	=	[mp.info.6]	n/a*
D	apply	=	=	[mp.info.9]	HIGH
category	apply	=	=	[mp.s.1]	HIGH
category	apply	=	+	[mp.s.2]	HIGH
D	n.a.	apply	+	[mp.s.8]	HIGH
D	n.a.	n.a.	apply	[mp.s.9]	n/a

3.1 IMPLEMENTATION MEASURES

12. Of the 75 security measures defined in Annex II of RD 3/2010, **a total of 56* measures apply**. They are as follows:

Organisational Framework (4):

[org.1] Security policy

[org.2] Security regulations

[org.3] Security procedures

[org.4] Authorisation process

Operational Framework (26):

[op.pl.1] Risk analysis

[op.pl.2] Security architecture

[op.pl.3] Acquisition of new components

[op.pl.4] Dimensioning / Capacity Management

[op.pl.5] Certified components

[op.acc] Access control

[op.acc.1] Identification

[op.acc.2] Access requirements

[op.acc.3] Segregation of functions and tasks

[op.acc.4] Access rights management process

[op.acc.5] Authentication mechanism

[op.acc.6] Local access (local logon)

[op.acc.7] Remote access (remote login)

[op.exp] Exploitation

[op.exp.1] Inventory of assets

[op.exp.2] Security configurations

[op.exp.3] Configuration Management

[op.exp.4] Maintenance

[op.exp.5] Change management

[op.exp.6] Protection against malware

[op.exp.7] Incident Management

[op.exp.8] User activity log

[op.exp.9] Incident Management Log

[op.exp.10] Protection of activity logs

[op.exp.11] Protection of cryptographic keys

[op.ext] External services

[op.ext.1] Contracting and service level agreements

[op.ext.2] Daily management

[op.mon] System monitoring

[op.mon.1] Intrusion detection

[op.mon.2] Metric system

Protective Measures (26):

[mp.if] Protection of installations and infrastructure

[mp.per] Personnel management

[mp.per.1] Workplace characterisation

[mp.per.2] Duties and obligations

[mp.per.3] Awareness

[mp.per.4] Training

[mp.eq] Equipment protection

[mp.eq.1] Workstation clear

[mp.eq.2] Workplace lock

[mp.eq.3] Protection of portable equipment

[mp.eq.9] Alternative means

[mp.com] Communications protection

[mp.com.1] Secure perimeter

[mp.com.2]Protection of confidentiality

[mp.com.3]Protection of authenticity and integrity

[mp.com.4]Network Segregation

[mp.si] Protection of information media

[mp.si.1] Labeling

[mp.si.2] Cryptography

[mp.si.3] Custody

[mp.si.4] Transportation

[mp.si.5] Deletion and destruction

[mp.sw] Protection of computer applications

[mp.sw.1] Development

[mp.sw.2] Acceptance and commissioning

[mp.info] Protection of information

[mp.info.1] Personal data

[mp.info.2] Qualification of information

[mp.info.3] Encryption

[mp.info.9] Backup

[mp.s] Protection of services

[mp.s.1] Email protection

[mp.s.2] Protection of web services and applications

[mp.s.8] Protection against denial of service

4. ENFORCEMENT CRITERIA

4.1 [OP.ACC] Authentication Mechanisms

13. The set of measures "op.acc Authentication Mechanisms" will be applied in category and HIGH level, with the following particularities:

- The authentication mechanisms provided by Office 365 comply with the requirements of the National Security Framework as long as they are configured for this purpose by the entity using the service.
- This configuration, which must be applied, is described in the Secure Configuration Guides for Office 365 and its related services, referenced in section 5 of this Guide regarding Security Configuration.
- For access to those elements of the system where the authentication mechanisms provided by Office 365 cannot be applied, as in the case of the system administration equipment, these measures will be applied in the HIGH category and level.

4.2 [OP.EXP. 2] Security Configuration

14. This measure of category and HIGH level will be applied, with the following particularities:

    - The security configuration that applies to the services provided by Office 365 will be as reflected in the Secure Configuration Guides for Office 365 and its related services, referenced in section 5 of this guide regarding Security Configuration.

15. The other components of the system must have an associated security configuration following the requirements of Annex II of the ENS.

4.3 [OP.EXP.8] User Activity Log

16. This measure of category and HIGH level will be applied, with the following particularities:

    - The mechanisms for logging user activity provided by Office 365 comply with the requirements of the National Security Framework as long as they are configured for this purpose by the entity using the service.
    - This configuration, which must be applied, is described in the Secure Configuration Guides for Office 365 and its related services, referenced in section 5 of this Guide regarding Security Configuration.
    - In those elements of the system where the activity logging mechanisms provided by Office 365 cannot be applied, as in the case of the equipment for system administration, this measure will be applied in the HIGH category and level.

4.4 [OP.EXP.10] Protection of User Activity Log

17. This measure of category and HIGH level will be applied, with the following particularities:

    - The mechanisms for the protection of activity logs provided by Office 365 will be used. However, the correct configuration of these activity log protection mechanisms will be the responsibility of the entity using the service.
    - The configuration that must be applied is described in the Secure Configuration Guides for Office 365 and its related services, referenced in section 5 of this Guide regarding Security Configuration.
    - In those elements of the system where the activity log protection mechanisms provided by Office 365 cannot be applied, as in the case of the equipment for system administration, this measure will be applied in the HIGH category and level.

4.5 [OP.EXT.9] Alternative means

18. The measure "op.ext.9 Alternative Means" is applicable only when, after the correct categorisation of the system, a HIGH level of security is established in the Traceability dimension of the system.

19. In this case, the measure will be applied with the following particularities:

    - The means replication mechanisms provided by Office 365 will be used.
    - The correct configuration of these mechanisms is described in the Secure Configuration Guides for Office 365 and its related services, referenced in section 5 of this Guide regarding Security Configuration.

4.6 [MP.IF] Installation and infrastructure protection measures

20. Measures of category and HIGH level must be applied, with the following particularities:

    - As the physical system is located in the cloud service provider's installations, only the service provider's company will be required to comply with the ENS for this Cloud service.

21. The application of the measure "mp.if.9 Alternative Installations", will only be applicable when the availability dimension has been evaluated as HIGH, and always taking into consideration the redundancy solutions in the installations offered by the Cloud service provider.

4.7 [MP.SW.1] Application Development

22. This measure will not be applicable as long as the development tasks in the system that supports the Cloud platform are prohibited, and this is expressly forbidden in the system's regulations, as long as the Security Manager considers it necessary.

23. Otherwise, this measure will be applied with the indicated requirements and level of security.

4.8 [MP.INFO.2] Rating Information

24. This measure will be applied to all those documents that form part of the information security management system related to the platform (procedures, policies, etc.) and to those relating to the operation and rules of use of the Cloud services, which will become available to users.

25. This measure will not be required for documents shared by users using Cloud services.

26. However, it is recommended to apply the security configurations for qualification of information described in the Secure Configuration Guides for Office 365 and its related services, referenced in Section 5 of this Guide regarding Security Configuration.

4.9 [MP.INFO.4] Electronic signature

27. This measure will not be applicable as long as the use of the electronic signature is not contemplated for functionalities related to the use and/or administration, configuration or maintenance of the platform, and is considered as such by the Security Manager.

4.10 [MP.INFO.6] Cleaning up documents

28. This measure will be applicable to all those documents that form part of the information security management system related to the platform (procedures, policies, etc.) and to those relating to the operation and rules of use of the Cloud services, which are made available to users, and it will be the responsibility of the user entity to have the procedures in place for this purpose.

4.11 [MP.INFO.9] Backup

29. This measure of category and HIGH level must be applied, with the following particularities:

    - The backup mechanisms provided by Office 365 will be used. However, the entity using the service will be responsible for the correct configuration of these backup mechanisms.
    - The configuration that must be applied is described in the Secure Configuration Guides for Office 365 and its related services, referenced in section 5 of this Guide regarding Security Configuration.

30. In those elements of the system where the backup mechanisms provided by Office 365 cannot be applied, as in the case of the system administration equipment, this measure will be applied in the HIGH category and level.

4.12 [MP.S.1] E-mail Protection

31. This measure will be especially applicable to Office 365 services because of its own implementation of e-mail services. The mechanisms for e-mail protection provided by Office 365 will be used.

32. However, it will be the responsibility of the entity using the service to correctly configure these e-mail protection mechanisms. The configuration that must be applied is described in the Secure Configuration Guides for Office 365 and its related services, referenced in section 5 of this Guide regarding Security Configuration.

5. SECURITY CONFIGURATION

33. In order to respond to the requirements established in this Specific Compliance Profile using Office 365 technology, you must consult the following guides: "CCN-STIC 885A Secure Configuration Guide for Office 365", "CCN-STIC 885B

Secure Configuration Guide for SharePoint Online", "CCN-STIC 885C Secure Configuration Guide for Exchange Online" and "CCN-STIC 884D Secure Configuration Guide for Teams", and apply the configurations indicated in them.

34. If you choose to use other technologies for the application of this Corporate Cloud Systems Specific Compliance Profile, the security configuration must have been previously validated by the CCN.