GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

Esquema Nacional de Seguridad Industrial

ENSI_C4V_02- Diccionario de Controles del Modelo de Construcción de Capacidades de Ciberseguridad de la Cadena de Valor (C4V)

certsi_

CERT DE SEGURIDAD E INDUSTRIA

ÍNDICE

NOVIEMBRE 2016

1. OBJETO DEL DOCUMENTO

Este documento proporciona un diccionario de controles para evaluar el nivel de Capacidades en Ciberseguridad de la Cadena de Valor (C4V) en un SCI, evaluación que se realizará según la metodología de evaluación descrita en el documento ENSI_C4V_01 - Modelo de Construcción de Capacidades de Ciberseguridad de la Cadena de Valor (C4V).

Los controles contenidos en este documento son parte esencial del proceso de medición de las capacidades de ciberseguridad en la cadena de valor de los SCI, conformando las medidas que serán evaluadas para conocer el grado de madurez y robustez en ciberseguridad de cada ente evaluado.

Se han considerado las siguientes cuatro categorías de controles:

- Controles de carácter general
- Controles relativos la confidencialidad
- Controles relativos a la integridad
- Controles relativos a la disponibilidad

Correspondientes a las medidas de seguridad generales o comunes que deberán evaluarse para determinar los tres tipos restantes de medidas correspondientes a las tres dimensiones de evaluación de ciberseguridad que se han considerado (confidencialidad, integridad y disponibilidad).

A cada control proporcionado se le ha asignado una prioridad (de 1 a 3) en cada uno de los niveles (de A+ a D) en los que debe evaluarse si dicho control se cumple o no.

Se incluyen también varias tablas que muestran la correspondencia de los controles del modelo C4V con los controles de otros modelos de controles (NIST SP 800-82, Indicadores de ciberresiliencia del modelo de INCIBE y Marco de Ciberseguridad)

2. ACERCA DEL ENSI

La promulgación de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas (Ley PIC), puso de manifiesto la importancia de la seguridad de las Infraestructuras Críticas dentro de la Seguridad del Estado. Por su parte, la Estrategia de Seguridad Nacional [1] de 2013 reconoce, por primera vez, las ciberamenazas como uno de los riesgos y amenazas a la seguridad nacional. Complementando la anterior, la Estrategia de Ciberseguridad Nacional [2] de 2013 completa la apuesta por la protección de los sistemas de control industrial como elemento clave en un enfoque integral de la ciberseguridad

En este contexto, el Instituto Nacional de Ciberseguridad (INCIBE), del Ministerio de Energía, Turismo y Agenda Digital, y el Centro Nacional de Infraestructuras Críticas del Ministerio del Interior, de la mano del acuerdo suscrito en 2012 y renovado en 2015 entre la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD) y la Secretaría de Estado de la Seguridad (SES), promueven el Esquema Nacional de Seguridad Industrial (ENSI), como instrumento para mejorar la seguridad de las infraestructuras críticas industriales y con una vocación global en tanto que es aplicable en sistemas de control industrial de cualquier organización.

Para ello, favorecer el tratamiento homogéneo de la seguridad y extender su aplicación a toda la cadena de valor de las organizaciones industriales, reconociendo el papel de proveedores y clientes, son las claves para dibujar el panorama completo al que responde el ENSI, que podría conformar la base para nuevas iniciativas que permitieran al ENSI ampliarse e incluir la seguridad desde un punto de vista más integral.

El ENSI se concreta en cuatro elementos esenciales que se configuran para atender a las necesidades específicas de su ámbito de aplicación:

- ARLI-SI: Metodología de Análisis de Riesgos Ligero de Seguridad Integral como punto de partida y piedra angular del proceso de mejora de la seguridad. Con entidad propia, dentro de esta metodología, ARLI-CIB permite un acercamiento específico, y también ligero, al Análisis de Riesgos de Ciberseguridad en sistemas de control industrial.
- IMC: Indicadores para la Mejora de Ciberresiliencia, como instrumento de diagnóstico y medición de la capacidad para soportar y sobreponerse a desastres y perturbaciones procedentes del ámbito digital.
- C4V: Modelo de Construcción de Capacidades en Ciberseguridad de la Cadena de Valor como elemento imperante en la operativa y actividad de la prestación de servicio del operador: proveedores y clientes.
- SA: Sistema de Acreditación en Ciberseguridad, garantía de la aplicación de unas medidas de seguridad mínimas equivalentes en todas las arquitecturas que prestan servicios equiparables o semejantes.

La aproximación práctica y ligera predomina en todos los elementos del ENSI y dibuja un marco completo para la mejora de la ciberseguridad en sistemas de control industrial.

Aquí, las diferentes guías y documentos de articulación, siempre alineados con todo lo establecido para los Planes de Seguridad del Operador, Planes de Protección Específicos y Planes Estratégicos Sectoriales, aportarán las instrucciones, criterios y herramientas para facilitar su aplicación por parte de los diferentes agentes.

3. DESCRIPCIÓN DE LOS NIVELES

Los apartados siguientes incluye las medidas de seguridad en cada uno de los niveles de capacidad para cada una de las dimensiones del modelo (confidencialidad, integridad y disponibilidad), además de una cuarta tabla que incluye las medidas de seguridad generales que afectan a las tres dimensiones. Las tablas contienen la siguiente información:

- **Referencia –** Es un código de identificación único para el control
- **Sección –** Agrupación en la que se clasifican las medidas de seguirdad del modelo correspondientes a los 14 capítulos en los que se han clasificado
- **Medida de seguridad –** Descripción detallada de las medidas
- **Prioridad por niveles (A+; A; B; C; D) –** Para cada uno de los cinco niveles de capacidad del modelo en los que la medida de seguridad es aplicable, se identifica un nivel de prioridad (que puede ser 1, 2 ó 3).
  Las celdas no vacías indican que el control es de aplicación en el correspondiente nivel de capacidad

Los códigos de prioridad pueden ser utilizados para secuenciar las decisiones para la implementación de las medidas de seguridad y para la asignación inicial de medidas y mejoras a las líneas base. Esta secuenciación recomendada ayuda a asegurar que las medidas de seguridad fundamentales para cada uno de los niveles de capacidad, de las que dependen el resto, han sido implementado primero, posibilitando a las organizaciones desplegar medidas de una manera más estructura de acuerdo con los recursos disponibles. La implementación de las medidas de seguridad según los códigos de prioridad no implican la consecución de un nivel de capacidad hasta que las medidas de seguridad de un nivel se hayan implementado en la medida establecida en la metodología. El objetivo de estos códigos de prioridad no es el de servir como mecanismo de selección de medidas, puesto que todas las medidas de seguridad de un nivel de capacidad son, en cierta forma, necesarias para alcanzar dicho nivel, sino para su secuencia de implementación.

4. MAPEOS

Esta sección recoge mapeos de las medidas de seguridad identificadas en el modelo con los siguientes documentos

- NIST SP 800-82
- Indicadores de ciberresiliencia del modelo de INCIBE
- Cybersecurity Framework – Indica la función clave del marco de ciberseguridad a la que corresponde el control del modelo

4.1.1. NIST SP 800-82

C4V	NIST82	
01. Programa de Gestión de Seguridad de la información [ISMP - Infosec management program]	AC-5	PM-4
	CA-1	PM-6
	CA-2; CA-2(1); CA-2(2)	PM-9
	CA-5	PM-11
	CA-7; CA-7(1)	PM-14
	CA-8	PM-15
	IA-1	RA-1
	MP-1	RA-2
	PE-1	RA-3
	PE-18	SA-2
	PL-1	SA-9
	PL-7	SA-10
	PM-1	SA-11
	PM-2	SI-2; SI-2(1); SI-2(2)
	PM-3	
02. Operación de Sistemas [SO - Systems Operation]	AC-19	PL-4(1)
	AC-22	PL-8
	CA-6	PM-5
	CA-9	PM-10
	CM-2	RA-5(4)
	CM-2(1); CM-2(2); CM-2(3); CM-2(7)	SA-4; SA-4(1); SA-4(2); SA-4(9)
	CM-3; CM-3(1); CM-3(2)	SA-5
	CM-4	SA-9(2)

	CM-5(3) CM-6; CM-6(1); CM-7; CM-7(1); CM-7(2) CM-8; CM-8(1); CM-8(2); CM-8(4); CM-8(5) CM-11 MP-3 MP-7; MP-7(1) PL-2; PL-2(3)	SA-10 SA-11 SC-18 SC-28 SI-7(14) SI-10 SI-11 SI-12
03. Seguridad del Personal [PS - Personnel Security]	AT-1 AT-2; AT-2(2) AT-3 AT-4 PL-4 PM-3 PM-12	PS-2 PS-3 PS-4; PS-4(2) PS-6 PS-7 PS-8
04. Seguridad de la Instalación [FS - Facility Security]	AC-19(5) AC-20(2) MA-2 MA-6 MP-2 MP-4 MP-5; MP-5(4) MP-6; MP-6(1); MP-6(2) PE-2 PE-3; PE-3(1) PE-4 PE-5 PE-6(1); PE-6(4)	PE-8 PE-9; PE-9(1) PE-10 PE-11; PE-11(1) PE-12 PE-13; PE-13(1); PE-13(2); PE-13(3) PE-14 PE-15 PE-16 PE-18 SC-8(1)
05. Procesamiento para Terceros [TPP - Third Party Processing]	AC-20; AC-20(1) SA-4 SA-9	SA-12 SC-4
06. Resiliencia [RE - Resilience]	CP-1	CP-10, CP-10(2); CP-10(4)

	CP-2; CP-2(1); CP-2(2); CP-2(3); CP-2(4); CP-2(5); CP-2(8) CP-3(1) CP-4; CP-4(1); CP-4(2) CP-6; CP-6(1); CP-6(2) CP-7; CP-7(1); CP-7(3); CP-7(4) CP-8(1) CP-9; CP-9(1); CP-9(2); CP-9(3); CP-9(5)	MA-1 MA-2; MA-2(2) MA-3; MA-3(1); MA-3(2); MA-3(3) MA-4; MA-4(2); MA-4(3) MA-5(1) MA-6 PE-17 PM-11 SC-24 SI-12
07. Cumplimiento [CO - Compliance]	CM-10	
08. Protección contra Códigos Maliciosos [MCP - Malicious Code Protection]	SI-3; SI-3(1); SI-3(2) SI-5	SI-16
09. Controles de Red [NC - Network Controls]	AC-4 AC-6(3) AC-17; AC-17(1); AC17-(2); AC-17(3); AC-17(4) AC-18(1); AC-18(5) CA-3; CA-3(5) CP-8; CP-8(2); CP-8(3); CP-8(4) IA-2(1); IA-2(2) IA-3 SC-2	SC-3 SC-5 SC-7; SC-7(3); SC-7(4); SC-7(5); SC-7(7); SC-7(8); SC-7(21) SC-8 SC-17 SC-19 SC-20 SC-21 SC-22 SC-23
10. Monitorización [MO – Monitoring]	AC-2(12) AU-1 AU-2; AU-2(3); AC-2(4) AU-3; AU-3(1); AU-3(2) AU-4 AU-5(1); AU-5(2)	AU-11 AU-12; AU-12(1) CM-5(1); CM-5(2) CM-6(2) IR-4(4) PE-6

	AU-6; AU-6(1); AU-6(3); AU-6(5); AU-6(6) AU-7; AU-7(1) AU-8; AU-8(1) AU-9; AU-9(2); AU-9(3); AU-9(4) AU-10	PE-8(1) PM-14 SC-7 SI-4; SI-4(2); SI-4(4); SI-4(5) SI-7; SI-7(1); SI-7(2)
11. Controles de Acceso [AC - Access Control]	AC-1 AC-2; AC-2(2); AC-2(3); AC-2(5); AC-2(11); AC-2(13) AC-3 AC-6; AC-6(1), AC-6(5), AC-6(9) AC-7 AC-10 AC-11 AC-12	AC-14 CM-5 IA-2(3); IA-2(4); IA-2(8); IA-2(9); IA-2(11) IA-4 IA-5; IA-5(1); IA-5(2); IA-5(3); IA-5(11) IA-6 IA-8 PS-5
12. Desarrollo Seguro [SD - Secure Development]	RA-5; RA-5(1); RA-5(2) SA-3 SA-11	SA-15 SA-16
13. Gestión de Incidentes [IH - Incident Handling]	IR-2(1) IR-4; IR-4(1); IR-2(2); IR-4(4) IR-5 IR-6; IR-6(1)	IR-7 IR-8 SI-5(1) SI-7(7) SI-17
14. Criptografía [CR - Cryptography]	SC-12; SC-12(1)	SC-13
15. Sistemas de Control Industrial [ICS - Industrial Control Systems]	AC-2(1) AC-8 AC-11 AC-18(4) AC-21 AU-4	MA-2 MA-4 MP-6(3) PE-11 PE-15 PM-8

	AU-5	PM-16
	AU-5(3)	RE-5(5)
	CM-1	SC-7(18)
	CM-4(1)	SA-10
	CM-7(5)	SC-15
	CM-8(3)	SC-24
	CM-9	SC-39
	CP-12	SC-41
	IA-3(1); IA-3(4)	SI-6
	IR-1	SI-7(5)
	IR-2	SI-8; SI-8(1); SI-8(2)
	IR-3; IR-3(2)	SI-13

4.1.2. Indicadores de ciberresiliencia

C4V	Indicadores de Ciberresiliencia
01. Programa de Gestión de Seguridad de la información [ISMP - Infosec management program]	Anticipar – 7 Resistir – 4, 5, 6, 7, 8 y 9
02. Operación de Sistemas [SO - Systems Operation]	Evolucionar - 1
03. Seguridad del Personal [PS - Personnel Security]	Anticipar – 8 y 9
04. Seguridad de la Instalación [FS - Facility Security]	-
05. Procesamiento para Terceros [TPP - Third Party Processing]	Anticipar – 3 Recuperar – 15, 16, 17 y 18 Evolucionar – 2 y 3
06. Resiliencia [RE - Resilience]	Anticipar – 1, 2, 3, 4, 5 y 6 Recuperar – 10, 11, 12, 13, 14, 19 y 20 Evolucionar – 4
07. Cumplimiento [CO - Compliance]	-
08. Protección contra Códigos Maliciosos [MCP - Malicious Code Protection]	-

C4V	Indicadores de Ciberresiliencia
09. Controles de Red [NC - Network Controls]	-
10. Monitorización [MO - Monitoring]	Resistir – 10, 11, 12 y 13
11. Controles de Acceso [AC - Access Control]	-
12. Desarrollo Seguro [SD - Secure Development]	Resistir – 1, 2, 3 y 5
13. Gestión de Incidentes [IH - Incident Handling]	Resistir – 13 Recuperar – 1, 2, 3, 4, 5, 6, 7, 8 y 9
14. Criptografía [CR - Cryptography]	

4.1.3. Etapas de ciberseguridad

C4V	Marco de ciberseguridad
01. Programa de Gestión de Seguridad de la información [ISMP - Infosec management program]	Identify - AM-5; AM-6; BE-1; BE-3; GV-2; GV-4; RA-1; RA-2; RA-3; RA-4; RA-5; RA-6; RM-1; RM-2; RM-3 Protect – AC-4; DS-5; IP-1; IP-2; IP-3; IP-7; IP-8; IP-10; IP-12 Detect – AE-2; AE-3; AE-4; CM-3; CM-6; CM-7; DP-1; DP-2; DP-3; DP-4; DP-5 Respond – CO-3; CO-5; AN-1; MI-3
02. Operación de Sistemas [SO - Systems Operation]	Identify - AM-1; AM-2; AM-3; RA-1 Protect – DS-1; DS-3; DS-7; IP-1; IP-2; IP-3; IP-7; IP-12; PT-3 Detect – AE-1; CM-2; CM-3; CM-5; CM-6; CM-7; DP-4; DP-5; MI-3
03. Seguridad del Personal [PS - Personnel Security]	Identify - AM-6; RA-3 Protect – AT-1; AT-2; AT-3; AT-4; AT-5; DS-5; IP-11 Detect – CM-6

C4V	Marco de ciberseguridad
04. Seguridad de la Instalación [FS - Facility Security]	Identify – BE-4 Protect – AC-2; AC-3; DS-3; IP-5; IP-6; MA-1; PT-2 Detect – CM-2; CM-7; DP-3 Respond – CO-3; AN-1
05. Procesamiento para Terceros [TPP - Third Party Processing]	Identify - AM-4; BE-1 Protect – AC-3; AT-3; IP-2 Detect – CM-6
06. Resiliencia [RE - Resilience]	Identify - AM-5; AM-6; BE-1; BE-5 Protect – DS-4; IP-4; IP-7; IP-9; IP-10, MA-1; MA-2 Detect – AE-4 Respond – RP-1; CO-1; CO-3; CO-4; AN-2; AN-4; IM-1; IM-2 Recover – RP-1; IM-1; IM-2; CO-3
07. Cumplimiento [CO - Compliance]	Detect – CM-3
08. Protección contra Códigos Maliciosos [MCP - Malicious Code Protection]	Identify – RA-1; RA-2; RA-3 Detect – CM-4; DP-3 Respond – CO-5; MI-3
09. Controles de Red [NC- Network Controls]	Identify - AM-3; BE-4 Protect - AC-3; AC-5; DS-2; DS-4; DS-5; PT-4 Detect – AE-1
10. Monitorización [MO - Monitoring]	Identify – RA-1 Protect – DS-4; DS-5; DS-6; IP-8; PT-1 Detect – AE-1; AE-2; AE-3; AE-4; AE-5; CM-2; CM-3; CM-5; CM-7; DP-2; DP-3; DP-4; DP-5 Respond – RP-1; CO-2; CO-3; CO-4; AN-1; AN-2; AN-3; AN-4; MI-1; MI-2; IM-1; IM-2 Recover – RP-1; IM-1; IM-2; CO-3
11. Controles de Acceso [AC - Access Control]	Protect – AC-1; AC-4; DS-5; PT-3 Detect – CM-1; CM-3

C4V	Marco de ciberseguridad
12. Desarrollo Seguro [SD - Secure Development]	Identify – RA-1 Protect – IP-2 Detect – CM-8; DP-4; DP-5 Respond – CO-3
13. Gestión de Incidentes [IH - Incident Handling]	Protect – IP-7; IP-9 Detect – AE-3; AE-4; AE-5 Respond – RP-1; CO-1; CO-2; CO-3; CO-4; CO-5; AN-1; AN-2; AN-3; AN-4; MI-1; MI-2; IM-1; IM-2 Recover – RP-1; IM-1; IM-2; CO-3
14. Criptografía [CR – Cryptography]	Protect – DS-5

5. CONTROLES

5.1. Controles de carácter general

Referencia	Sección	Medidas de seguridad	Prioridad por niveles				
			A	B	C	D	E
01. Programa de Gestión de Seguridad de la información [ISMP]							
G[ISMP.01]2-01	[ISMP.01] Estrategia y planificación de seguridad	Objetivos de seguridad de la información claramente establecidos y aprobados oficialmente por la dirección ejecutiva.				1	
G[ISMP.01]2-04	[ISMP.01] Estrategia y planificación de seguridad	Conjunto de indicadores de seguridad empleados para saber el grado de implementación de las medidas de seguridad.				2	
G[ISMP.01]3-01	[ISMP.01] Estrategia y planificación de seguridad	Proceso de seguridad de la información integrado con los procesos empresariales pertinentes.	2	2	1		
G[ISMP.01]3-02	[ISMP.01] Estrategia y planificación de seguridad	Sistema de gestión de Seguridad de la información implementado (plan, organización y control de recursos).			1		
G[ISMP.01]3-03	[ISMP.01] Estrategia y planificación de seguridad	Conjunto de indicadores de seguridad empleados para saber el número, tipo e impacto de los incidentes de seguridad.			2		
G[ISMP.01]4-02	[ISMP.01] Estrategia y planificación de seguridad	Mantenimiento del conocimiento y la evaluación comparativa de la industria de seguridad a través de redes, foros especializados en seguridad o asociaciones profesionales.	2	2			
G[ISMP.01]4-03	[ISMP.01] Estrategia y planificación de seguridad	El proceso de gestión de seguridad de la información implementado se actualiza y mejora continuamente.	2	2			
G[ISMP.01]4-04	[ISMP.01] Estrategia y planificación de seguridad	Conjunto de indicadores de seguridad empleados para medir la eficiencia del sistema de seguridad.	2	2			
G[ISMP.01]5-03	[ISMP.01] Estrategia y planificación de seguridad	La organización protege el plan de seguridad de la información contra su divulgación y modificación no autorizadas.	1				
G[ISMP.02]3-02	[ISMP.02] Asignación de responsabilidades	Medidas demostrables y oficiales para respaldar la seguridad de la información mediante una orientación registrada clara, compromiso, asignación explícita y verificación del cumplimiento de la asignación por la dirección ejecutiva.	2	2	2		
G[ISMP.02]3-03	[ISMP.02] Asignación de responsabilidades	Funciones y responsabilidades claramente asignadas en el campo de la seguridad de la información, aplicando la separación de las funciones.	1	1	1		

G[ISMP.02]3-04	[ISMP.02] Asignación de responsabilidades	Al menos, las siguientes responsabilidades de gestión se han asignado a un individuo o a un equipo: • Establecer, registrar y distribuir los procedimientos de respuesta y escalada de los incidentes de seguridad. • Monitorizar y analizar las alertas e información de seguridad, y distribuirlas entre el personal apropiado. • Establecer, registrar y distribuir los procedimientos de respuesta y escalada de los incidentes de seguridad. • Administrar las cuentas de usuario, incluyendo las incorporaciones, eliminaciones y modificaciones. • Monitorizar y controlar todos los accesos a los datos.	1	1	1		
G[ISMP.02]3-05	[ISMP.02] Asignación de responsabilidades	Al menos, las siguientes funciones no se asignan a las mismas personas: a) Operación de sistemas b) Desarrollo c) Auditoría de los sistemas de información d) Directivo en Seguridad de la Información	1	1	1		
G[ISMP.02]4-03	[ISMP.02] Asignación de responsabilidades	Establecer claramente en los acuerdos de servicios, las responsabilidades de los proveedores y usuarios de dichos servicios (especialmente en los servicios en la nube).	2	2			
G[ISMP.02]5-01	[ISMP.02] Asignación de responsabilidades	Enfoque integral de la función de seguridad (física y cibernética).	1				
G[ISMP.03]1-01	[ISMP.03]. Gestión de riesgos	Inicio del proceso de identificación del apetito de riesgo.					1
G[ISMP.03]2-01	[ISMP.03] Gestión de riesgos	Desarrollo y mantenimiento del marco de gestión de riesgos de la organización para gestionar riesgos.				2	
G[ISMP.03]2-02	[ISMP.03] Gestión de riesgos	La organización desarrolla, disemina y revisa/actualiza una política de evaluación de riesgos oficial y registrada (de conformidad con una metodología sólida) que abarca el propósito, el alcance, las funciones, las responsabilidades, el compromiso con la gestión, la coordinación entre las entidades de la organización y el cumplimiento.				3	
G[ISMP.03]2-03	[ISMP.03] Gestión de riesgos	El funcionario que autoriza o el representante designado por el mismo, revisa y aprueba la decisión de la categorización de la seguridad, de conformidad con un apetito de riesgo (aún no definido oficialmente).	1	1	1	1	
G[ISMP.03]2-04	[ISMP.03] Gestión de riesgos	El análisis de riesgos se realiza en lenguaje natural, con el objetivo de: . Identificar los activos más valiosos . Identificar las amenazas más probables . Identificar los dispositivos de seguridad que protegen de esas amenazas . Identificar los principales riesgos residuales				1	

G[ISMP.03]3-06	[ISMP.03] Gestión de riesgos	Evaluaciones de riesgos anuales semioficiales, de conformidad con un marco institucional que determine la probabilidad e impacto de todos los riesgos identificados, empleando métodos cualitativos o cuantitativos, con el objetivo de: . Identificar y valorar cualitativamente los activos más valiosos . Identificar y cuantificar las amenazas más probables . Identificar y valorar los dispositivos de seguridad que protegen de esas amenazas . Identificar y valorar los principales riesgos residuales			1		
G[ISMP.03]3-07	[ISMP.03] Gestión de riesgos	Umbrales de tolerancia al riesgo registrados y actualizados, junto con las medidas de tratamiento de riesgos.			1		
G[ISMP.03]4-01	[ISMP.03] Gestión de riesgos	Los riesgos se mitigan a un nivel aceptable. Los niveles de aceptación basados en los criterios de riesgos se establecen y registran conforme a plazos de resolución razonables y aprobación ejecutiva.	2	2			
G[ISMP.03]4-02	[ISMP.03] Gestión de riesgos	Los resultados de la evaluación de riesgos incluyen actualizaciones de las políticas de seguridad, procedimientos, normas y controles para garantizar que continúan siendo pertinentes y efectivos.	2	2			
G[ISMP.03]4-03	[ISMP.03] Gestión de riesgos	Evaluaciones de riesgo oficiales anuales (o tras cambios significativos), de conformidad con un marco institucional que determine la probabilidad y el impacto de todos los riesgos identificados, con el objetivo de: . Identificar y valorar cualitativamente los activos más valiosos . Identificar y cuantificar las amenazas más probables . Identificar las vulnerabilidades que permiten esas amenazas . Identificar y valorar los dispositivos de seguridad que protegen de esas amenazas . Identificar y valorar los principales riesgos residuales	1	1			
G[ISMP.03]5-02	[ISMP.03] Gestión de riesgos	Las evaluaciones de riesgo, incluyendo la definición de tolerancia al riesgo, se actualizan cuando así lo aconsejan las iniciativas inteligentes.	1				
G[ISMP.04]2-01	[ISMP.04] Asignación de recursos	Presupuesto específico para las iniciativas de seguridad de la información.				1	
G[ISMP.04]3-01	[ISMP.04] Asignación de recursos	Presupuesto independiente para las iniciativas de seguridad de la información, garantizando que todas las solicitudes de planificación de capital y de inversión poseen los recursos necesarios para implementar el programa de seguridad de la información, y garantizando que se registran todas las excepciones a este requisito.	1	1	1		
G[ISMP.04]4-01	[ISMP.04] Asignación de recursos	Monitorización y evaluación eficiente de las inversiones en seguridad de la información, y medida que garantiza que los recursos de seguridad de la información están disponibles para el gasto según lo previsto.	2	2			
G[ISMP.05]2-02	[ISMP.05] Políticas y normas de seguridad de la información	Procedimientos operativos diarios de acuerdo con los requisitos normativos.	2	2	2	2	
G[ISMP.05]2-03	[ISMP.05] Políticas y normas de seguridad de la información	Desarrollo de las políticas de uso de las tecnologías críticas y definición del uso adecuado de dichas tecnologías.	3	3	3	3	

G[ISMP.05]2-04	[ISMP.05] Políticas y normas de seguridad de la información	Política de seguridad de la información, aprobada oficialmente por el Directivo Superior, que se ha comunicado a los usuarios (empleados o no) de conformidad con los siguientes requisitos: . Organización e implementación de los procesos de seguridad . Análisis y gestión de riesgos . Gestión/seguridad del personal . Profesionalidad . Controles y autorización de accesos . Protección de las instalaciones . Adquisición de productos (sistemas y servicios) . Seguridad por defecto · Integridad y actualización de los sistemas · Protección de datos (inactivos y en tránsito/medios) · Prevención contra la conexión a través de sistemas interconectados · Mejora constante de los procesos de seguridad · Registro de actividad · Incidentes de seguridad · Protección de los sistemas y de la comunicación · Continuidad empresarial	3	3	3	3	
G[ISMP.05]3-01	[ISMP.05] Políticas y normas de seguridad de la información	Revisión de las políticas y los procedimientos operativos, al menos anualmente y tras cambios significativos.	2	2	2		
G[ISMP.06]1-01	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	Inicio del inventario de vulnerabilidades y reparaciones y monitorización de las vulnerabilidades pendientes, midiendo los plazos de resolución.					1
G[ISMP.06]2-01	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	La organización desarrolla un plan de evaluación de seguridad que describe el alcance de la evaluación, incluyendo los controles de seguridad objeto de evaluación, los procedimientos que se han de utilizar para determinar la efectividad, el entorno, el equipo y las funciones y responsabilidades (en los entornos SCI, la política aborda concretamente las propiedades únicas y los requisitos del SCI, así como la relación con los sistemas que no son SCI).	3	3	3	3	
G[ISMP.06]2-02	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	La organización desarrolla, disemina y revisa/actualiza una política de auditoría oficial y registrada que abarca el propósito, el alcance, las funciones, las responsabilidades, el compromiso con la gestión, la coordinación entre las entidades de la organización y el cumplimiento.	3	3	3	3	
G[ISMP.06]2-03	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	La organización desarrolla un plan de acción y objetivos de las TIC para registrar las medidas correctoras previstas de la organización que tienen el objetivo de subsanar las debilidades/deficiencias, y actualiza dicho plan atendiendo a los resultados de las evaluaciones de seguridad.	3	3	3	3	
G[ISMP.06]2-04	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	La organización incorpora la resolución de fallos en el proceso de gestión de la configuración de la organización.	2	2	2	2	
G[ISMP.06]3-01	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	La organización desarrolla y revisa/actualiza los procedimientos oficiales y registrados para facilitar la implementación de la política de auditoría y los controles de auditoría asociados.	3	3	3		

G[ISMP.06]3-02	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	Planificación de auditorías y evaluaciones realizados por un organismo independiente.	1	1	1		
G[ISMP.06]3-07	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	El proceso de resolución de fallos se gestiona de forma centralizada, midiendo los plazos desde el conocimiento, hasta la reparación y resolución.	1	1	1		
G[ISMP.06]4-01	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	Planificación de auditorías en base a las evaluaciones de riesgo.		2			
G[ISMP.06]4-05	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	El proceso de resolución de fallos emplea mecanismos automáticos para determinar el estado de los elementos del sistema de información en relación con la resolución de fallos.		2			
G[ISMP.06]4-08	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	Las vulnerabilidades explotables encontradas durante las pruebas de penetración son corregidas, y se repiten las pruebas para verificar las correcciones.	1	1			
G[ISMP.06]5-03	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	La organización emplea mecanismos automáticos para ayudar a garantizar que el plan de acción y objetivos es riguroso, está actualizado y es de fácil acceso.	2				
G[ISMP.06]5-04	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	La organización mide el tiempo que transcurre entre la identificación de los fallos y su resolución, y adopta medidas correctoras cuando dicho tiempo supera la ejecución prevista.	2				
G[ISMP.06]5-05	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	Mejorar constantemente la efectividad del proceso de seguridad.	2				
G[ISMP.06]5-06	[ISMP.06] Pruebas de seguridad, procesos y rendimiento	Realizar pruebas de penetración internas y externas al menos cada 6 meses y tras cualquier actualización o modificación de infraestructuras o aplicaciones, tanto a nivel de red como a nivel de aplicación (o empleo de un sistema de réplica, de virtualización o simulador para realizar pruebas de penetración de sistemas SCI).	1				
G[ICS.26]2-01	[ICS.26] Plan de Infraestructuras Críticas	La organización se encarga de las cuestiones de seguridad de la información en el desarrollo, registro y actualización de una infraestructura crítica y un plan de protección de los recursos principales.	2	2	2	2	
02. Operación de Sistemas [SO]							
G[SO.01]2-04	[SO.01] Gestión de cambios	Proceso de autorización establecido para nuevos (elementos de) sistemas de información.	1	1	1	1	
G[SO.01]3-02	[SO.01] Gestión de cambios	Procedimiento de control de cambios implantado que incluye el registro, la identificación, planificación y pruebas, análisis de impactos, aprobación oficial, comunicación de cambios y procedimientos de reversión.	3	3	3		
G[SO.01]4-01	[SO.01] Gestión de cambios	Se mantiene un registro de auditoría de todas las actualizaciones de las bibliotecas de programas operativos.	2	2			
G[SO.01]5-04	[SO.01] Gestión de cambios	La organización emplea mecanismos automáticos para registrar/notificar/prohibir cambios.	2				
G[SO.02]2-02	[SO.02] Identificación y gestión de activos	Identificación de los componentes de los sistemas de información (equipos, redes internas y conexiones con redes externas, así como puntos de acceso al sistema).				2	

G[SO.02]3-02	[SO.02] Identificación y gestión de activos	Actualización del inventario como parte integral de las instalaciones de componentes, eliminaciones y actualizaciones del sistema de información, verificando que todos los componentes incluidos en el límite de autorización de dicho sistema no están duplicados en otros inventarios de componentes del sistema de información.	2	2	2		
G[SO.02]4-04	[SO.02] Identificación y gestión de activos	Existen mecanismos automatizados para detectar nuevos activos en la infraestructura.	2	2			
G[SO.02]5-02	[SO.02] Identificación y gestión de activos	La organización incluye en el inventario información acerca de los componentes del sistema de información, lo que supone una forma para que los responsables de la administración de dichos componentes puedan identificarlos.	2				
G[SO.03]2-01	[SO.03] Procedimientos de gestión y tratamiento de información/conocimientos	Política aprobada que establece el tratamiento, procesamiento, almacenamiento y principios de comunicación de la información, de conformidad con [SO.2] y la normativa legal.	3	3	3	3	
C[SO.03]3-09	[SO.03] Procedimientos de gestión y tratamiento de información/conocimientos	La organización restringe el uso de medios extraíbles en sistemas de información específicos, sobre todo si los medios no tienen propietarios identificables.	1	1	1		
G[SO.03]4-01	[SO.03] Procedimientos de gestión y tratamiento de información/conocimientos	La organización designa y forma a individuos autorizados para publicar información en un sistema de información de acceso público.	1	1			
G[SO.03]4-02	[SO.03] Procedimientos de gestión y tratamiento de información/conocimientos	La organización revisa el contenido de información propuesto antes de su publicación en los sistemas de acceso público para garantizar que no se incluya información privada.	1	1			
G[SO.04]3-01	[SO.04] Seguridad de la documentación de sistemas	La documentación de los sistemas de información (manuales de administrador y de usuario, diagramas de arquitectura, etc.) solo se ponen a disposición del personal autorizado para garantizar la configuración, instalación y funcionamiento de los sistemas operativos, así como el uso efectivo de los elementos de seguridad de los sistemas.			2		
G[SO.04]3-02	[SO.04] Seguridad de la documentación de sistemas	Una vez enviada, debe permanecer bajo control de la persona autorizada, sin ser desatendida y, si está en formato electrónico, se ha de cifrar.	2	2	3		
G[SO.04]3-04	[SO.04] Seguridad de la documentación de sistemas	No se comparte en foros públicos cualquier información relacionada con los sistemas utilizados, los detalles de la configuración o las cuestiones de seguridad y, si se menciona, se hace de forma anónima.			1		
G[SO.04]4-02	[SO.04] Seguridad de la documentación de sistemas	No se comparte en foros públicos cualquier información relacionada con los sistemas utilizados, los detalles de configuración o las cuestiones de seguridad.	1	1			
G[SO.05]2-01	[SO.05] Requisitos de seguridad de los sistemas de información	Los requisitos empresariales de los nuevos sistemas de información, o las mejoras de los sistemas de información ya existentes, incluyen requisitos para los controles de seguridad atendiendo a los resultados de los análisis de riesgo, de conformidad con la arquitectura de seguridad y teniendo en cuenta las necesidades de los requisitos técnicos, la formación y las limitaciones financieras.				2	
G[SO.05]2-02	[SO.05] Requisitos de seguridad de los sistemas de información	La arquitectura de seguridad de la información desarrollada para el sistema de información describe la filosofía y el enfoque general que se ha de adoptar para proteger la confidencialidad, integridad y disponibilidad de la información de la organización, y también describe cómo la arquitectura de seguridad es parte integrante y sostiene la arquitectura empresarial.	1	1	1	1	

G[SO.05]2-03	[SO.05] Requisitos de seguridad de los sistemas de información	Habilitación exclusiva de aquellos servicios, protocolos, demonios (daemons), etc. necesarios y seguros, imprescindibles para el funcionamiento del sistema.	1	1	1	1	
G[SO.05]2-05	[SO.05] Requisitos de seguridad de los sistemas de información	Eliminación de todas las funcionalidades innecesarias, como las secuencias de comandos, controladores, elementos, subsistemas, sistemas de archivos y servidores web innecesarios.	1	1	1	1	
G[SO.05]2-07	[SO.05] Requisitos de seguridad de los sistemas de información	La organización determina el software no autorizado y emplea una política de lista negra para prohibir la ejecución de software no autorizado.	1	1	1	1	
G[SO.05]2-08	[SO.05] Requisitos de seguridad de los sistemas de información	La organización desarrolla, disemina y revisa/actualiza una política de adquisición de sistemas y servicios oficial y registrada que incluye consideraciones sobre la seguridad de la información y abarca el propósito, el alcance, las funciones, las responsabilidades, el compromiso con la gestión, la coordinación entre las entidades de la organización y el cumplimiento.				3	
G[SO.05]2-10	[SO.05] Requisitos de seguridad de los sistemas de información	La organización establece las restricciones de uso, los requisitos de configuración, los de conexión y las directrices para la implementación de dispositivos móviles controlados, y autoriza la conexión de los dispositivos móviles a los sistemas de información de la organización.	3	3	3	3	
G[SO.05]3-05	[SO.05] Requisitos de seguridad de los sistemas de información	Las bases de seguridad se revisan y actualizan (si procede) al menos cada año o tras cambios significativos, incluyendo la lista de software no autorizado, las vulnerabilidades detectadas y los incidentes de seguridad.	2	2	2		
G[SO.05]3-06	[SO.05] Requisitos de seguridad de los sistemas de información	La organización incluye los requisitos funcionales, de resistencia y de garantía de la seguridad, así como los de documentación en materia de seguridad y los criterios de aceptación de los contratos de adquisición de sistemas de información.	2	2	2		
G[SO.05]4-01	[SO.05] Requisitos de seguridad de los sistemas de información	El cumplimiento con los requisitos básicos de seguridad se reevalúa al menos de forma anual, o tras cambios significativos.		2			
G[SO.05]5-01	[SO.05] Requisitos de seguridad de los sistemas de información	La organización emplea mecanismos automatizados para gestionar de forma centralizada, y lleva a cabo la aplicación y verificación de los ajustes de configuración de los componentes críticos de manera continuada.	2				
G[SO.06]2-01	[SO.06] Control de software operativo	Los sistemas operativos solo emplean códigos ejecutables aprobados y no códigos de desarrollo ni compiladores.				2	
G[SO.06]2-02	[SO.06] Control de software operativo	Políticas, procedimientos y mecanismos aprobados oficialmente para restringir la instalación de software no autorizado.				3	
G[SO.06]3-02	[SO.06] Control de software operativo	Las aplicaciones y el software de sistemas operativos solo se implementan tras pruebas exhaustivas y exitosas (utilidad, seguridad, efectos en otros sistemas y facilidad de uso) en sistemas independientes.	1	1	1		
G[SO.06]3-03	[SO.06] Control de software operativo	Utilización de configuraciones seguras a fin de permitir exclusivamente la ejecución de códigos móviles autorizados y funcionalidades autorizadas.	1	1	1		
G[SO.06]4-01	[SO.06] Control de software operativo	Empleo de un sistema de control de configuración para mantener el control de todo el software implementado, así como de la documentación de los sistemas.		1			

G[SO.06]5-01	[SO.06] Control de software operativo	El sistema de información impide la instalación de componentes de software y firmware establecidos por la organización sin la verificación de que el componente se ha firmado digitalmente mediante un certificado reconocido y aprobado por la organización.	1				
G[ICS.09]1-01	[ICS.09] Gestión de la configuración	Inicio del proceso de gestión de la configuración.					2
G[ICS.09]2-01	[ICS.09] Gestión de la configuración	La organización desarrolla, disemina y revisa/actualiza una política de gestión de la configuración oficial y registrada que abarca el propósito, el alcance, las funciones, las responsabilidades, el compromiso con la gestión, la coordinación entre las entidades de la organización y el cumplimiento.	3	3	3	3	
G[ICS.09]3-01	[ICS.09] Gestión de la configuración	La organización desarrolla, registra e implementa un plan de gestión de la configuración para el sistema de información que: a. Abarca las funciones, responsabilidades y los procesos y procedimientos de gestión de la configuración; b. Establece un proceso para identificar los elementos de configuración a lo largo del ciclo de vida de desarrollo del sistema y para gestionar la configuración de los elementos de configuración; c. Define los elementos de configuración de los sistemas de información y sitúa los elementos de configuración bajo la gestión de la configuración, y d. Protege el plan de gestión de la configuración de su divulgación y modificación no autorizadas.	2	2	2		
G[ICS.09]3-02	[ICS.09] Gestión de la configuración	La organización exige que el desarrollador del sistema de información, de los componentes del sistema o del servicio del sistema de información lleve a cabo la gestión de la configuración.	2	2	2		
G[ICS.09]4-01	[ICS.09] Gestión de la configuración	El proceso de gestión de la configuración se actualiza y revisa anualmente.		2			
G[ICS.09]5-01	[ICS.09] Gestión de la configuración	El proceso de gestión de la configuración está sujeto a un continuo plan de mejora.	2				
G[ICS.11]3-01	[ICS.11] Software autorizado/listas blancas	La organización identifica el software no autorizado y emplea una política de lista blanca para permitir la ejecución de software autorizado, y revisa y actualiza la lista anualmente.	1	1	1		
G[ICS.12]3-01	[ICS.12] Detección automática de componentes no autorizados	La organización emplea mecanismos automatizados para detectar la adición de componentes no autorizados en el ámbito de aplicación.	1	1	1		
G[ICS.14]3-01	[ICS.14] Identificación y autenticación de dispositivos	El sistema de información verifica los dispositivos críticos antes de establecer conexiones locales/remotas/de red mediante autenticación bidireccional basada en la criptografía.	1	1	1		
G[ICS.14]3-02	[ICS.14] Identificación y autenticación de dispositivos	La organización garantiza que la identificación y autenticación de dispositivos mediante la certificación se realiza mediante un proceso de gestión de la configuración establecido por la organización.	2	2	2		
G[ICS.21]2-01	[ICS.21] Dispositivos informáticos de colaboración	El sistema de información: a. Prohíbe la activación remota de dispositivos informáticos de colaboración, con las excepciones establecidas por la organización para los casos en los que se permita dicha activación remota; y b. Ofrece indicaciones de uso explícitas para los usuarios físicamente presentes en los dispositivos.	2	2	2	2	
G[ICS.22]2-01	[ICS.22] Aislamiento del proceso	Los sistemas de información pueden mantener dominios de ejecución independientes para cada proceso de ejecución asignando a cada proceso un espacio de dirección independiente.	2	2	2	2	

G[ICS.23]2-01	[ICS.23]. Dispositivos de puerto y de entrada/salida	La organización desactiva o elimina físicamente puertos de conexión o dispositivos de entrada/salida en componentes de sistemas de información SCI.	1	1	1	1	
03. Seguridad del Personal [PS]							
G[PS.01]2-01	[PS.01] Responsabilidades del usuario	Se informa a los usuarios de su responsabilidad de: · Mantener la concienciación y el cumplimiento de las políticas de seguridad publicadas, los procedimientos, normas y requisitos reglamentarios aplicables. · Seguir prácticas de seguridad adecuadas en cuanto a la selección y uso de contraseñas (si procede). · Mantener un ambiente de trabajo seguro y protegido. · Mantener la confidencialidad de las contraseñas personales y mantener las contraseñas del grupo en el ámbito de los miembros del grupo. · Dejar los equipos sin vigilancia de forma segura.	2	2	2	2	
G[PS.02]1-01	[PS.02] Formación y concienciación	Inicio de la definición del plan de formación.					1
G[PS.02]1-02	[PS.02] Formación y concienciación	Inicio de la definición del plan de concienciación.					1
G[PS.02]2-01	[PS.02] Formación y concienciación	Implementar un programa oficial de concienciación de la seguridad que abarca el propósito, el alcance, las funciones, las responsabilidades, el compromiso con la gestión, la coordinación entre las entidades de la organización y el cumplimiento.	2	2	2	2	
G[PS.02]2-03	[PS.02]Formación y concienciación	La organización ofrece formación basada en roles en materia de seguridad para los usuarios de sistemas de información y registra y monitoriza las actividades formativas individuales.	2	2	2	2	
G[PS.02]2-05	[PS.02]. Formación y concienciación	Formar al personal tras la contratación y, al menos, una vez al año.	2	2	2	2	
G[PS.02]3-02	[PS.02] Formación y concienciación	Anualmente se exige al personal que confirme haber leído y entendido las políticas y procedimientos en materia de seguridad (actualización de medidas de concienciación).	1	1	1		
G[PS.02]3-03	[PS.02] Formación y concienciación	La organización incluye formación en materia de concienciación sobre seguridad para el reconocimiento y notificación de indicadores potenciales de amenaza interna.	1	1	1		
G[PS.02]3-05	[PS.02] Formación y concienciación	Se mantiene actualizado el plan formativo en materia de seguridad y ciberresiliencia.	1	1	1		
G[PS.02]4-01	[PS.02] Formación y concienciación	Los gestores son los responsables de mantener la concienciación y el cumplimiento de las políticas de seguridad, así como de los procedimientos y las normas correspondientes a su área de responsabilidad.	2	2			
G[PS.02]4-02	[PS.02] Formación y concienciación	Gestión, actualización y verificación de las actividades formativas en materia de seguridad y ciberresiliencia incluidas en el plan.	2	2			
G[PS.02]5-01	[PS.02] Formación y concienciación	La organización incluye ejercicios prácticos en la formación de la concienciación en materia de seguridad que simulan ataques informáticos reales.	1				
G[PS.02]5-02	[PS.02] Formación y concienciación	El equipo de respuesta a los incidentes de la organización participa en los ejercicios prácticos que simulan ataques informáticos.	1				

G[PS.03]2-01	[PS.03] Seguridad de las personas	Clara definición y distribución de las responsabilidades del cese o cambio de empleo.	2	2	2	2	
G[PS.03]2-03	[PS.03] Seguridad de las personas	Los usuarios (empleados, contratistas, terceros, arrendatarios y/o clientes) firman acuerdos contractuales sobre sus responsabilidades en materia de seguridad antes de obtener el acceso al entorno (instalaciones, sistemas, etc.).	1	1	1	1	
G[PS.03]2-05	[PS.03] Seguridad de las personas	El derecho de acceso a la información y a las instalaciones de procesamiento de información de todos los empleados, contratistas y usuarios terceros se deroga cuando termina su empleo, contrato o acuerdo, o se modifican tras haber sufrido cambios.	1	1	1	1	
G[PS.03]3-01	[PS.03] Seguridad de las personas	Establecimiento y seguimiento de los procesos disciplinarios.	2	2	2		
G[PS.03]3-03	[PS.03] Seguridad de las personas	Los empleados, contratistas y usuarios terceros deben devolver todos los activos de la organización en un plazo definido y registrado una vez que su empleo, contrato o acuerdo haya finalizado.	2	2	2		
G[PS.03]3-04	[PS.03] Seguridad de las personas	Todos los usuarios con acceso a información (candidatos a empleo, contratistas y terceros) están sujetos a una verificación de sus antecedentes de conformidad con la normativa local. Los procedimientos de verificación se definen de acuerdo con la clasificación de la información a la que se va a tener acceso.		1	1		
G[PS.03]5-01	[PS.03] Seguridad de las personas	Procesos anuales de evaluación continua (revisión adicional de encuestas, políticas y procedimientos).	1				
G[PS.03]5-02	[PS.03] Seguridad de las personas	La organización utiliza mecanismos automatizados para notificar el cese de un individuo al personal o a los cargos establecidos por la organización.	2				
04. Seguridad de la Instalación [FS]							
G[FS.01]3-06	[FS.01] Perímetro de seguridad física	Usar cámaras de video y/o mecanismos de control de acceso para monitorizar los accesos físicos individuales a zonas sensibles.	1	1	1		
G[FS.01]3-07	[FS.01] Perímetro de seguridad física	Almacenar la información sobre los accesos durante al menos tres (3) meses, a menos que la ley disponga otra cosa.	2	2	2		
G[FS.01]3-08	[FS.01] Perímetro de seguridad física	Restricción del acceso físico a puntos de acceso inalámbricos, portales, dispositivos portátiles, hardware de redes/comunicaciones y líneas de telecomunicación.	1	1	2		
G[FS.01]3-09	[FS.01] Perímetro de seguridad física	Evaluación de los riesgos del perímetro físico y evaluación de los perímetros al menos una vez al año.			2		
G[FS.01]3-10	[FS.01] Perímetro de seguridad física	Revisión de la información sobre los accesos.	2	2	1		
G[FS.01]4-03	[FS.01] Perímetro de seguridad física	Perímetro IDS conectado a un puesto de mando.		2			
G[FS.01]4-07	[FS.01] Perímetro de seguridad física	Instalación de un sistema de detección de intrusos.		2			
G[FS.01]4-08	[FS.01] Perímetro de seguridad física	Restricción del acceso físico a los conectores de red de acceso público.	2	2			

G[FS.01]4-09	[FS.01] Perímetro de seguridad física	Evaluación de los riesgos del perímetro físico y evaluación de los perímetros al menos dos veces al año.	1	1			
G[FS.01]4-10	[FS.01] Perímetro de seguridad física	Las evaluaciones de riesgo incluyen los edificios adyacentes y su cumplimiento con los requisitos reglamentarios y legales pertinentes.	2	2			
G[FS.01]5-03	[FS.01] Perímetro de seguridad física	Perímetro protegido con CCTV con infrarrojos y espectro visible.	2				
G[FS.01]5-05	[FS.01] Perímetro de seguridad física	Capacidades IDS con tecnología duplicada y conectada a un puesto de mando con dispositivos anti-sabotaje.	2				
G[FS.02]2-02	[FS.02] Controles de acceso físico	Restricción del acceso a las instalaciones al personal autorizado con controles de acceso.	2	2	2	2	
G[FS.02]2-03	[FS.02] Controles de acceso físico	La organización desarrolla y mantiene una lista de las personas con acceso autorizado a la instalación donde se encuentra el sistema de información, atendiendo al puesto de trabajo de la persona, y elimina de la lista a las personas cuando ya no es necesario su acceso.	2	2	2	2	
G[FS.02]2-04	[FS.02] Controles de acceso físico	Registro de las entradas y salidas de todos los visitantes.				2	
G[FS.02]2-05	[FS.02] Controles de acceso físico	Se informa a todos los visitantes de las guías que se han de observar (seguridad, emergencias, etc.).	2	2	2	2	
G[FS.02]2-06	[FS.02] Controles de acceso físico	Todas las salas tienen controles de acceso con registro mediante código PIN.				2	
G[FS.02]2-07	[FS.02] Controles de acceso físico	Todos los visitantes llevan alguna señal que permite identificarlos como tal.	2	2	2	2	
G[FS.02]2-09	[FS.02] Controles de acceso físico	Vigilancia del acceso de los visitantes a zonas sensibles.			1	1	
G[FS.02]2-10	[FS.02] Controles de acceso físico	Se autoriza a todos los visitantes antes de entrar a zonas en las que se procesa o guarda información.	2	2	2	2	
G[FS.02]3-01	[FS.02] Controles de acceso físico	Todas las salas tienen controles de acceso con registro mediante código PIN y/o tarjeta inteligente.			2		
G[FS.02]3-03	[FS.02] Controles de acceso físico	Todos los derechos de acceso se revisan y actualizan al menos una vez al año.			2		
G[FS.02]3-05	[FS.02] Controles de acceso físico	Doble autenticación para acceder al centro de datos.	2	2	2		
G[FS.02]3-06	[FS.02] Controles de acceso físico	El acceso físico se revoca inmediatamente al término, y todos los mecanismos de acceso físico, como llaves, tarjetas de acceso, etc., se devuelven o deshabilitan.	1	1	1		
G[FS.02]4-01	[FS.02] Controles de acceso físico	Todas las salas tienen controles de acceso con registro mediante biometría.		1			
G[FS.02]4-02	[FS.02] Controles de acceso físico	Los derechos de acceso se revisan y actualizan al menos dos veces al año.		1			

G[FS.02]4-04	[FS.02] Controles de acceso físico	Las puertas externas se cierran automáticamente cuando las internas están abiertas.		2			
G[FS.02]4-06	[FS.02] Controles de acceso físico	Las combinaciones y las llaves se cambian cuando se pierden llaves, se ponen en peligro las combinaciones o las personas cambian o cesan su empleo.		2			
G[FS.02]5-02	[FS.02] Controles de acceso físico	Todas las salas poseen controles de acceso dobles con registro.	2				
G[FS.02]5-03	[FS.02] Controles de acceso físico	Los derechos de acceso se revisan y actualizan trimestralmente.	1				
G[FS.02]5-04	[FS.02] Controles de acceso físico	Los controles de acceso implementan sistemas anti pass-back.	2				
G[FS.02]5-05	[FS.02] Controles de acceso físico	Las combinaciones y llaves se cambian, al menos, una vez al año.	2				
G[FS.02]5-06	[FS.02] Controles de acceso físico	Se emplea un proceso de pruebas de penetración que incluye intentos, anuales y sin previo aviso, de evitar o eludir los controles de seguridad de los puntos de acceso físico a la instalación.	1				
G[FS.03]2-01	[FS.03] Localización y protección de equipos	Están prohibidas las tareas no supervisadas en las zonas seguras.	2	2	2	2	
G[FS.03]2-06	[FS.03] Localización y protección de equipos	Instalación de un SAI para permitir el apagado programado de los equipos.	2	2	2	1	
G[FS.03]2-07	[FS.03] Localización y protección de equipos	Instalación de generadores eléctricos con combustible in situ para cubrir los fallos de sistemas SAI durante, al menos, 8 horas.				1	
G[FS.03]2-09	[FS.03] Localización y protección de equipos	Restricción del acceso a zonas de almacenamiento de medios.	2	2	2	2	
G[FS.03]2-10	[FS.03] Localización y protección de equipos	La organización emplea y mantiene un sistema de luces de emergencia automático para el sistema de información que se activa en caso de corte o interrupción de energía y que abarca las salidas de emergencia y las vías de evacuación de la instalación.	2	2	2	2	
G[FS.03]2-11	[FS.03] Localización y protección de equipos	La organización emplea y mantiene dispositivos/sistemas de extinción y detección de incendios para el sistema de información abastecidos por una fuente de energía independiente.	1	1	1	1	
G[FS.03]2-12	[FS.03] Localización y protección de equipos	La organización mantiene los niveles de temperatura y humedad en la instalación donde se encuentra el sistema de información y monitoriza dichos niveles.				2	
G[FS.03]3-04	[FS.03] Localización y protección de equipos	La capacidad de combustible del generador es de 24 horas.			1		
G[FS.03]3-09	[FS.03] Localización y protección de equipos	La organización emplea dispositivos/servicios de extinción de incendios para el sistema de información que proporciona una notificación automática de cualquier activación de los respondedores de emergencia y de la organización cuando no hay personal en la instalación.	2	2	2		
G[FS.03]3-10	[FS.03] Localización y protección de equipos	La organización emplea un sistema de monitorización de la temperatura y la humedad que proporciona una alarma o notificación de los cambios potencialmente perjudiciales para el personal o los equipos.	2	2	2		

G[FS.03]3-13	[FS.03] Localización y protección de equipos	La organización protege al sistema de información de daños provocados por fugas de agua mediante compuertas de cierre o aislamiento que son accesibles, funcionan correctamente y son conocidas por el personal principal.	2	2	2		
G[FS.03]4-03	[FS.03] Localización y protección de equipos	Garantía de suministro continúo para asegurar el funcionamiento constante de los generadores.		1			
G[FS.03]4-04	[FS.03] Localización y protección de equipos	Los cables de alimentación se separan de la comunicación para evitar interferencias.		2			
G[FS.03]4-05	[FS.03] Localización y protección de equipos	Las líneas de entrada de electricidad y comunicación se encuentran bajo tierra.		2			
G[FS.03]4-07	[FS.03] Localización y protección de equipos	Las salas de comunicaciones están cerradas con llave.	2	2			
G[FS.03]5-04	[FS.03] Localización y protección de equipos	Tanto el suministro de electricidad como el de comunicaciones tienen dos vías independientes activas.	1				
G[FS.04]2-01	[FS.04] Seguridad de los equipos fuera de las instalaciones	Aprobación de la política de uso de los equipos fuera de las instalaciones que incluye la autorización de salida.	3	3	3	3	
G[FS.04]2-03	[FS.04] Seguridad de los equipos fuera de las instalaciones	Registro detallado de las entradas y salidas de los equipos del sistema de información, incluyendo los ordenadores portátiles, registrando a las personas que las autorizan.	2	2	2	2	
G[ICS.16]2-01	[ICS.16] Mantenimiento no local	Todas las actividades de mantenimiento se aprueban y monitorizan (especialmente el mantenimiento no local).	1	1	1	1	
G[ICS.17]5-01	[ICS.17] Desinfección de los medios	La organización aplica técnicas de desinfección no destructivas a los dispositivos de almacenamiento portátiles antes de conectarlos al sistema de información.	1				
05. Procesamiento para Terceros [TPP]							
G[TPP.01]3-02	[TPP.01] Procesamiento compartido	Los accesos y privilegios de cada entidad se restringen exclusivamente a su propio entorno de datos: espacio en disco, CPU, ancho de banda, memoria, etc.	1	1	1		
G[TPP.01]4-02	[TPP.01] Procesamiento compartido	Cada entidad se aísla de las actividades maliciosas de los coarrendatarios (bloqueo de la IP, confiscación de recursos, etc.).	1	1			
G[TPP.02]1-01	[TPP.02] Seguridad de la cadena de suministro	Inicio de la Identificación de las dependencias de terceros, del análisis de sus factores de riesgos y de la definición de los requisitos de seguridad.					1
G[TPP.02]1-02	[TPP.02] Seguridad de la cadena de suministro	Los proveedores contratados poseen al menos una calificación “E” o se le requieren medidas de seguridad equivalentes establecidas por acuerdos según el nivel de servicio, cuyo cumplimiento se monitoriza, al menos, trimestralmente.					1
G[TPP.02]2-01	[TPP.02] Seguridad de la cadena de suministro	Mantener una lista de proveedores de servicios.	2	2	1	1	
G[TPP.02]2-03	[TPP.02] Seguridad de la cadena de suministro	Los acuerdos de nivel de servicios de redes o infraestructuras registran claramente los controles de seguridad, los niveles de capacidad y servicio, así como los requisitos de los negocios o clientes.				1	

G[TPP.02]2-04	[TPP.02] Seguridad de la cadena de suministro	Los proveedores contratados poseen al menos una calificación “D” o se le requieren medidas de seguridad equivalentes establecidas por acuerdos de nivel de servicio, cuyo cumplimiento se monitoriza, al menos, trimestralmente.				1	
G[TPP.02]2-05	[TPP.02] Seguridad de la cadena de suministro	Identificación de los factores de riesgo de la subcontratación de terceros e implementación de controles cuando sea necesario. Los servicios deberían tener los niveles adecuados de madurez y gestión.			1	1	
G[TPP.02]3-02	[TPP.02] Seguridad de la cadena de suministro	Los acuerdos de terceros que, de forma directa o indirecta, tienen un impacto sobre los activos de información de la organización o los datos que, de manera explícita, cubren todos los requisitos de seguridad pertinentes	1	1	1		
G[TPP.02]3-03	[TPP.02] Seguridad de la cadena de suministro	Proceso establecido para contratar a los proveedores de servicios, incluyendo la debida solicitud antes de su contratación.	1	1	1		
G[TPP.02]3-04	[TPP.02] Seguridad de la cadena de suministro	Provisiones de los acuerdos de nivel de servicio (incluyendo las cuestiones de seguridad) garantizadas por subcontratistas.	1	1	1		
G[TPP.02]3-07	[TPP.02] Seguridad de la cadena de suministro	Los proveedores contratados poseen al menos una calificación “C” o se le requieren medidas de seguridad equivalentes establecidas por acuerdos de nivel de servicio, cuyo cumplimiento se monitoriza, al menos, cada dos meses.			1		
G[TPP.02]4-01	[TPP.02] Seguridad de la cadena de suministro	Programa para monitorizar el cumplimiento del proveedor de servicios con las directrices del vendedor.	1	1			
G[TPP.02]4-02	[TPP.02] Seguridad de la cadena de suministro	Acuerdos y procedimientos interinstitucionales con las entidades involucradas en la cadena de suministro para notificar los compromisos de dicha cadena de suministro.	2	2			
G[TPP.02]4-03	[TPP.02] Seguridad de la cadena de suministro	Divulgación de los subcontratistas del proveedor de servicios imprescindibles para la prestación de los servicios.	2	2			
G[TPP.02]4-04	[TPP.02] Seguridad de la cadena de suministro	Los proveedores contratados poseen al menos una calificación “B” o se le requieren medidas de seguridad equivalentes establecidas por acuerdos de nivel de servicio, cuyo cumplimiento se monitoriza mensualmente.		1			
G[TPP.02]5-01	[TPP.02] Seguridad de la cadena de suministro	Empleo de todas las fuentes de inteligencia para analizar a los potenciales proveedores.	2				
G[TPP.02]5-03	[TPP.02] Seguridad de la cadena de suministro	Transparencia en el tipo de intervención que se le permite al proveedor de servicios o a terceros en relación con los datos de los clientes y los procesos.	2				
G[TPP.02]5-04	[TPP.02] Seguridad de la cadena de suministro	Los proveedores contratados poseen una calificación “A” o se le requieren medidas de seguridad equivalentes establecidas por acuerdos de nivel de servicio, cuyo cumplimiento se monitoriza mensualmente.	1				
G[TPP.02]5-05	[TPP.02] Seguridad de la cadena de suministro	Debido a restricciones reglamentarias, siempre que sea posible, no serán necesarios los proveedores de servicios críticos.	2				
07. Cumplimiento [CO]							
G[CO.01]2-03	[CO.01] Cumplimiento de los requisitos legales	Política de cumplimiento de los derechos de propiedad intelectual publicada que define el uso legal de software y de productos de información en cada jurisdicción legislativa y las obligaciones contractuales de la organización (no duplicar, convertir a otro formato o extraer de grabaciones comerciales que no sean las permitidas).	2	2	2	2	

G[CO.01]3-01	[CO.01] Cumplimiento de los requisitos legales	Mantener la concienciación de las políticas para proteger los derechos de propiedad intelectual y notificar acerca de la intención de emprender medidas en contra de quienes los violen.	2	2	2		
08. Protección contra Códigos Maliciosos [MCP]							
G[MCP.01]2-02	[MCP.01]. Protección contra programas maliciosos	Instalación de un software para detectar y corregir software malicioso que escanea equipos (páginas web, correos electrónicos, dispositivos) y protege a su memoria de ejecuciones de códigos no autorizados.				1	
G[MCP.01]2-03	[MCP.01] Protección contra programas maliciosos	Mecanismos de protección contra códigos maliciosos que realizan escaneos semanales del sistema de información y escaneos a tiempo real de los archivos de fuentes externas cuando se descargan, abren o ejecutan dichos archivos.				2	
G[MCP.01]3-01	[MCP.01] Protección contra programas maliciosos	Utilización de un Software antivirus capaz de detectar, eliminar y proteger contra todo tipo de software malicioso conocido en todos los sistemas comúnmente afectados por software malicioso (puertos de entrada y salida, servidores o equipos informáticos móviles).	1	1	1		
G[MCP.01]3-02	[MCP.01] Protección contra programas maliciosos	Todos los mecanismos antivirus son actuales, funcionan activamente y generan registros de auditoría.	2	2	2		
G[MCP.01]3-04	[MCP.01] Protección contra programas maliciosos	La firma del antivirus se actualiza automáticamente cada 12 horas.	2	2	2		
G[MCP.01]3-05	[MCP.01] Protección contra programas maliciosos	Los mecanismos de protección contra código malicioso realizan escaneos diarios.	2	2	2		
G[MCP.01]4-02	[MCP.01] Protección contra programas maliciosos	Suscripción a un sistema de información acerca de nuevos códigos maliciosos lanzados.	1	1			
G[ICS.24]3-01	[ICS.24] Protección anti-spam	La organización: a. Emplea mecanismos anti-spam en los puntos de entrada y salida del sistema de información para detectar y adoptar medidas contra mensajes no solicitados; y b. Actualiza los mecanismos anti-spam cuando se lanzan al mercado nuevos mecanismos de acuerdo con las políticas y procedimientos de la gestión de la configuración de la organización.	2	2	2		
G[ICS.24]3-02	[ICS.24] Protección anti-spam	La organización gestiona de forma centralizada los mecanismos anti-spam.	2	2	2		
G[ICS.24]3-03	[ICS.24] Protección anti-spam	El sistema de información actualiza automáticamente los mecanismos anti-spam.	2	2	2		
G[ICS.27]5-01	[ICS.27] Programa de concienciación de amenazas	La organización implementa un programa de concienciación de amenazas que incluye la capacidad de intercambio de información entre organizaciones.	1				
09. Controles de Red [NC]							
G[NC.01]2-05	[NC.01] Gestión de redes	La organización autoriza las conexiones del sistema de información, registra los requisitos de seguridad y la naturaleza de la información, y los monitoriza de forma continua.	2	2	2	2	
G[NC.01]3-02	[NC.01] Gestión de redes	Para entornos inalámbricos, cambiar los valores inalámbricos que vienen por defecto incluyendo, entre otros, claves de cifrado, contraseñas y cadenas comunitarias SNMP.	2	2	2		

G[NC.01]3-04	[NC.01] Gestión de redes	Cables de conexión y puentes etiquetados en ambos extremos de los cables con el nombre de la conexión.	2	2	2		
G[NC.01]3-05	[NC.01] Gestión de redes	El sistema de información, en combinación con un dispositivo remoto, evita que el dispositivo establezca simultáneamente conexiones no remotas con el sistema y se comunique a través de otra conexión con fuentes en redes externas.	1	1	1		
G[NC.01]3-07	[NC.01] Gestión de redes	La organización: a. Establece restricciones de uso y directrices para la implementación de tecnologías de Voz sobre Protocolo de Internet (VoIP) atendiendo al daño potencial que se podría causar al sistema de información si se utilizan de forma maliciosa, y b. Autoriza, monitoriza y controla el uso de VoIP en el sistema de información.	2	2	2		
G[NC.01]4-02	[NC.01] Gestión de redes	La organización restringe las comunicaciones inalámbricas a límites controlados reduciendo la potencia de las transmisiones inalámbricas o configurándolas de forma que los accesos sean de punto a punto.	1	1			
G[NC.02]2-01	[NC.02] Controles de encaminamiento en la red	Las puertas de enlace de seguridad se utilizan para validar las direcciones de origen y de destino en puntos de control de redes internas y externas para garantizar que las conexiones informáticas y los flujos de información sean adecuados.	1	1	1	1	
G[NC.02]2-04	[NC.02] Controles de encaminamiento en redes	Registro de la justificación comercial para el uso de todos los servicios, protocolos y puertos permitidos, incluyendo el registro de los elementos de seguridad implementados en los protocolos considerados inseguros (FTP, Telnet, SSL2.0, POP3, IMAP, SNMPv1 y v2, etc.).	3	3	3	3	
G[NC.02]2-05	[NC.02] Controles de encaminamiento en la red	El conjunto de reglas de los cortafuegos y routers se revisa, al menos, cada año.				1	
G[NC.02]2-06	[NC.02] Controles de encaminamiento en la red	El tráfico entrante y saliente se restringe al que resulte necesario para el entorno (por defecto prohíbe el tráfico, excepto el permitido).	1	1	1	1	
G[NC.02]2-08	[NC.02] Controles de encaminamiento en la red	No se permiten las conexiones directas entrantes o salientes para el tráfico entre Internet y el entorno.	2	2	2	2	
G[NC.02]3-01	[NC.02] Controles de encaminamiento en la red	Los conjuntos de reglas de los cortafuegos y routers se revisan, al menos, cada seis meses.			1		
G[NC.02]4-03	[NC.02] Controles de encaminamiento en la red	Los conjuntos de reglas de los cortafuegos y routers se revisan, al menos, cada cuatro meses .		2			
G[NC.02]5-02	[NC.02] Controles de encaminamiento en la red	Cortafuegos y capacidades SDI/SPI integradas.	1				
G[NC.02]5-04	[NC.02] Controles de encaminamiento en la red	Los conjuntos de reglas de los cortafuegos y routers se revisan, al menos, cada dos meses.	2				
G[NC.03]2-01	[NC.03] Segregación en las redes	Existen dominios de red internos y externos.			2	2	
G[NC.03]2-02	[NC.03] Segregación en las redes	Hay un cortafuegos en cada conexión de Internet y entre cualquier zona desmilitarizada (DMZ) y la zona de red interna.	1	1	1	1	
G[NC.03]2-04	[NC.03] Segregación en las redes	Los componentes del sistema que almacenan datos se sitúan en una zona de red interna, separada de la DMZ y otras redes no seguras.	1	1	1	1	

G[NC.03]3-01	[NC.03] Segregación en las redes	La red de servicios se aísla del resto de las redes. La funcionalidad de la gestión del sistema de información incluye, por ejemplo, las funciones necesarias para administrar bases de datos, componentes de redes, terminales o servidores, y normalmente requiere un acceso de usuario privilegiado.	2	2	2		
G[NC.03]3-03	[NC.03] Segregación en las redes	Restringir la gestión de acceso a la VLAN de forma que las partes de redes no seguras no puedan explotar la gestión de interfaces y protocolos, como las SNMP.	1	1	1		
G[NC.03]3-04	[NC.03] Segregación en las redes	Usar listas de control de acceso en dispositivos de transmisión IP para proteger contra servidores Proxy de capa 2 en redes VLAN privadas.	2	2	2		
G[NC.03]4-01	[NC.03] Segregación en las redes	Existen diferentes dominios para reducir el impacto de amenazas.	1	1			
G[NC.03]4-03	[NC.03] Segregación en las redes	Usar mecanismos de seguridad de puertos para limitar el número de direcciones MAC permitidas (o similares, IEEE 802.1x y EAP, etc.).	1	1			
G[NC.03]4-04	[NC.03] Segregación en las redes	Las redes del vendedor se segmentan adecuadamente, incluyendo las zonas para: gestionar la nube, la migración en caliente (si se está utilizando la virtualización del servidor), las redes de almacenamiento y, para las IaaS, los clientes tienen sus propias zonas de seguridad de la máquina virtual. Por lo general, el sistema de información aísla las funciones de seguridad de las funciones que no lo son.	1	1			
G[NC.03]5-01	[NC.03] Segregación en las redes	La infraestructura de red virtual utilizada (en redes PVLAN y VLAN 802.1q) se ajusta a normas específicas del vendedor y/o normas de buenas prácticas (por ejemplo, la suplantación de direcciones MAC, los ataques al ARP, etc. se evitan mediante una configuración de seguridad específica).	1				
G[NC.04]2-01	[NC.04] Autenticación de usuarios para conexiones externas	La organización registra los métodos permitidos de acceso remoto al sistema de información.	1	1	1	1	
G[NC.04]2-06	[NC.04] Autenticación de usuarios para conexiones externas	Implementación de una doble autenticación para el acceso remoto de cuentas privilegiadas a la red.				1	
G[NC.04]3-02	[NC.04] Autenticación de usuarios para conexiones externas	Implementación de una doble autenticación para el acceso remoto de empleados, administradores y terceros a la red.			1		
G[NC.04]3-05	[NC.04] Autenticación de usuarios para conexiones externas	El sistema de información protege la autenticidad de las sesiones de comunicación (contra el nivel de paquetes) e invalida los identificadores de sesión cuando el usuario cierra sesión o tras otras sesiones.	1	1	1		
G[NC.04]4-05	[NC.04] Autenticación de usuarios para conexiones externas	La organización autoriza el acceso a la red a comandos privilegiados establecidos por la organización solo para necesidades operacionales esenciales establecidas por la misma.	2	2			
G[ICS.04]4-01	[ICS.04] Restricción de la configuración inalámbrica por parte de usuarios.	La organización identifica y autoriza expresamente a los usuarios permitidos a configurar de forma independiente capacidades de redes inalámbricas.	2	2			
10. Monitorización [MO]							

G[MO.01]1-01	[MO.01] Registros de auditoría	Existen procedimientos iniciales del uso del sistema de monitorización (incluyendo la detección de software no autorizado y de conexiones no autorizadas).					1
G[MO.01]2-01	[MO.01] Registros de auditoría	Aprobación de la política de registros de auditoría.	3	3	3	3	
G[MO.01]2-02	[MO.01] Registros de auditoría	Los registros de auditoría se permiten y activan para que los componentes del sistema enlacen todos los accesos a dichos componentes con cada usuario individual y detecten conexiones no autorizadas.	2	2	2	2	
G[MO.01]2-03	[MO.01] Registros de auditoría	La organización distribuye la capacidad de almacenamiento de los registros de auditorías según la política de registros de auditoría.	2	2	2	2	
G[MO.01]2-04	[MO.01] Registros de auditoría	El sistema de información utiliza relojes internos del sistema para generar marcas de tiempo para los registros de auditoría.				1	
G[MO.01]3-01	[MO.01] Registros de auditoría	La activación de los registros estará bajo control directo del responsable central de la seguridad de la información/responsable de la protección de datos.	2	2	2		
G[MO.01]3-02	[MO.01] Registros de auditoría	Los relojes de todos los sistemas de información pertinentes se sincronizan con una fuente de tiempo exacta acordada previamente.			1		
G[MO.01]3-03	[MO.01] Registros de auditoría	Los registros almacenan, al menos, las siguientes entradas de registros de auditoría de todos los componentes del sistema para cada incidente: · Identificación del usuario. · Tipo de incidente. · Tipo de acceso. · Fecha y hora. · Éxito de la indicación de fallos. · Origen del incidente. · Identidad o nombre de los datos, componentes del sistema o recursos afectados.	1	1	1		
G[MO.01]3-04	[MO.01] Registros de auditoría	Actualización de los procedimientos de los registros de auditoría.	2	2	2		
G[MO.01]4-01	[MO.01] Registros de auditoría	Los administradores del sistema no tienen permiso para eliminar o desactivar los registros de sus propias actividades.	1	1			
G[MO.01]4-02	[MO.01] Registros de auditoría	Los relojes de todos los sistemas de información pertinentes se sincronizan con dos fuentes de tiempo exactas acordadas previamente.	1	1			
G[MO.01]4-05	[MO.01] Registros de auditoría	Las herramientas de monitorización de intrusiones se examinan, al menos, de forma anual.	1	1			
G[MO.01]4-06	[MO.01] Registros de auditoría	Los registros de auditoría también incluyen: · Uso de las utilidades y aplicaciones del sistema. · Archivos a los que se accede y tipo de acceso. · Registro de cada acceso.	1	1			
G[MO.01]5-01	[MO.01] Registros de auditoría	Se aplican continuas acciones de mejoras a los procedimientos de monitorización.	2				

G[MO.02]2-01	[MO.02] Uso del sistema de monitorización	Los registros almacenan los accesos lógicos a los sistemas.				1	
G[MO.02]2-02	[MO.02] Uso del sistema de monitorización	Los registros se revisan mensualmente y se informa de los resultados.				1	
G[MO.02]3-01	[MO.02] Uso del sistema de monitorización	Los registros de auditoría de todos los componentes del sistema permiten reconstruir los siguientes incidentes: · Registros de fallos. · Intentos no válidos de accesos lógicos. · Todos los accesos individuales a los datos. · Todas las medidas adoptadas por las personas con privilegios administrativos o de root. · Acceso a los registros de auditoría. · Usos y modificaciones a los mecanismos de identificación y autenticación. · Inicio, cese o pausa de los registros de auditoría. · Creación, modificación y eliminación de los objetos del sistema (incluyendo las identificaciones de los usuarios). · Puesta en funcionamiento y cese del sistema. · Intento de acceso no autorizado.	1	1	1		
G[MO.02]3-02	[MO.02] Uso del sistema de monitorización	Revisión diaria de, al menos, los siguientes registros de seguridad: · Todos los incidentes de seguridad. · Registros de todos los componentes del sistema en el ámbito de aplicación del servicio. · Registros de todos los componentes críticos del sistema. · Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, cortafuegos, sistemas de detección de intrusiones/sistemas de prevención de intrusiones (SDI/SPI), servidores de autenticación, servidores de redirección de comercio electrónico, etc.).		1	1		
G[MO.02]3-03	[MO.02] Uso del sistema de monitorización	La organización utiliza una capacidad para reducir auditorías y generar informes que permite una rápida revisión, tras la solicitud de auditorías, de los análisis y de los requisitos de información. Tras las investigaciones de los incidentes de seguridad, ofrece la posibilidad de procesar los registros de auditoría de incidentes de interés, sin modificar los registros de auditoría originales.	2	2	2		
G[MO.02]3-04	[MO.02] Uso del sistema de monitorización	Los registros (de todos los demás componentes del sistema) se revisan semanalmente.		1	1		
G[MO.02]3-05	[MO.02] Uso del sistema de monitorización	Existe la posibilidad de detectar anomalías, como la capacidad para detectar tráfico IP inusual potencialmente malicioso y el comportamiento de los usuarios o del equipo de asistencia.			1		
G[MO.02]4-01	[MO.02] Uso del sistema de monitorización	Los registros de auditoría de todos los componentes del sistema también permiten reconstruir los siguientes incidentes: · Intentos de acceso no autorizado. · Inserción/extracción de dispositivos de entrada/salida. · Alertas o mensajes de la consola. · Excepciones de registros de los sistemas. · Alarmas de gestión de redes. · Cambios o intentos de cambio de las configuraciones de seguridad del sistema.	1	1			
G[MO.02]4-02	[MO.02] Uso del sistema de monitorización	El sistema de auditoría analiza y correlaciona los registros de auditoría entre diferentes repositorios para conocer la situación de toda la organización.		1			

G[MO.02]4-03	[MO.02] Uso del sistema de monitorización	Las técnicas SDI/SPI se emplean para monitorizar el tráfico en el perímetro del entorno, así como en los puntos críticos existentes en su interior, y alertan al personal sobre posibles incidentes. Se mantienen actualizados todos los sistemas de detección y prevención de intrusiones, las bases de seguridad y las firmas.		1			
G[MO.02]4-07	[MO.02] Uso del sistema de monitorización	Se emplean mecanismos de detección de cambios (por ejemplo, herramientas de monitorización de la integridad de archivos) para alertar al personal de la modificación no autorizada de los archivos críticos del sistema, los archivos de configuración o los archivos de contenido; y se configura el software para que realice comparaciones de archivos críticos al menos semanalmente.		1			
G[MO.02]4-08	[MO.02] Uso del sistema de monitorización	En caso de que sea necesario, los registros se monitorizan en línea mediante un sistema automático que genera alertas clasificadas que son enviadas a una unidad de gestión de crisis.		1			
G[MO.02]5-01	[MO.02] Uso del sistema de monitorización	Configurar los mecanismos de detección de cambios (por ejemplo, las herramientas de monitorización de la integridad de archivos) para realizar diariamente comparaciones de archivos críticos.	1				
G[MO.02]5-03	[MO.02] Uso del sistema de monitorización	Los registros se monitorizan en línea, junto con los sistemas SDI/SPI de las instalaciones del Centro de Operaciones de Redes/Centro de Operaciones de Seguridad, permitiendo de esta forma la revisión y el análisis centralizado de los registros de auditoría de los múltiples componentes del sistema.	1				
G[MO.02]5-04	[MO.02] Uso del sistema de monitorización	La organización correlaciona la información de los registros de auditoría con la información que se obtiene de la monitorización de los accesos físicos, a fin de mejorar la capacidad de identificar actividades sospechosas, inapropiadas, inusuales o maliciosas.	1				
G[MO.02]5-05	[MO.02] Uso del sistema de monitorización	Para mejorar el conocimiento de la situación de toda la organización, ésta relaciona la información que se obtiene de fuentes no técnicas (por ejemplo, los registros de recursos humanos) con la información de las auditorías.	1				
G[MO.02]5-06	[MO.02] Uso del sistema de monitorización	Los registros de todos los demás componentes del sistema se revisan diariamente.	1				
G[MO.03]2-01	[MO.03] Protección de la información de los registros	Los registros se protegen mediante un sistema de autorización para limitar su acceso a las personas que desean visualizarlos por motivos laborales y se protegen de modificaciones no autorizadas.				2	
G[MO.03]2-02	[MO.03] Protección de la información de los registros	Los registros se almacenan durante, al menos, 1 año, con un mínimo de 3 meses en los que estarán inmediatamente disponibles para su análisis.				1	
G[MO.03]3-01	[MO.03] Protección de la información de los registros	Los registros se archivan en sistemas especializados con controles de monitorización de la integridad de los archivos.			1		
G[MO.03]3-03	[MO.03] Protección de la información de los registros	Los registros se almacenan durante, al menos, 2 años.			1		
G[MO.03]4-01	[MO.03] Protección de la información de los registros	El sistema de información emplea mecanismos criptográficos para proteger la integridad de la información de auditoría y de las herramientas de auditoría. Los registros poseen una marca de tiempo.		1			
G[MO.03]4-02	[MO.03] Protección de la información de los registros	Los registros se almacenan durante, al menos, 5 años.		1			
G[MO.03]4-03	[MO.03] Protección de la información de los registros	El sistema de información realiza una copia de seguridad de los registros de auditoría en un sistema físico o un componente del sistema diferente al sistema o componente objeto de auditoría.		1			

G[MO.03]4-04	[MO.03] Protección de la información de los registros	El sistema de registros se monitoriza y genera alertas a tiempo real cuando detecta problemas relacionados con la capacidad de almacenamiento, la recepción de registros o la superación de umbrales.	2	2			
G[MO.03]5-01	[MO.03] Protección de la información de los registros	Los registros se almacenan en medios de una sola escritura.	1				
G[MO.03]5-02	[MO.03] Protección de la información de los registros	Los registros se almacenan durante, al menos, 10 años.	1				
G[MO.03]5-03	[MO.03] Protección de la información de los registros	La organización exige e impone una doble autorización para la eliminación de registros.	1				
G[ICS.06]2-01	[ICS.06] Auditoría y rendición de cuentas	El sistema de información descarga los registros de auditoría periódicamente en un sistema o medio diferente al sistema objeto de auditoría.				1	
G[ICS.06]3-01	[ICS.06] Auditoría y rendición de cuentas	El sistema de información descarga los registros de auditoría semanalmente en un sistema o medio diferente al sistema objeto de auditoría.			1		
G[ICS.06]4-01	[ICS.06] Auditoría y rendición de cuentas	El sistema de información descarga los registros de auditoría diariamente en un sistema o medio diferente al sistema objeto de auditoría.		1			
G[ICS.06]5-01	[ICS.06] Auditoría y rendición de cuentas	El sistema de información descarga los registros de auditoría directamente en un sistema o medio diferente al sistema objeto de auditoría.	1				
G[ICS.07]2-01	[ICS.07] Respuesta a los fallos en el procesamiento de auditoría	El sistema alerta en caso de fallo en el procesamiento de auditoría.	2	2	2	2	
G[ICS.08]5-01	[ICS.08] Generación de auditoría	El sistema de información proporciona la posibilidad de que las personas o funciones establecidas por la organización para cambiar la auditoría puedan llevar a cabo su actividad en un umbral de tiempo determinado.	2				
11. Control de Acceso [AC]							
G[AC.01]1-01	[AC.01] Requisitos empresariales para el control del acceso	El acceso a los recursos del sistema está protegido para que solo los usuarios autorizados puedan utilizarlos de acuerdo con las instrucciones del propietario del sistema.	2	2	2	2	2
G[AC.01]1-02	[AC.01] Requisitos empresariales para el control del acceso	La organización establece las acciones de los usuarios que se pueden llevar a cabo en el sistema de información sin identificación o autenticación.					2
G[AC.01]2-01	[AC.01] Requisitos empresariales para el control del acceso	Establecimiento, aprobación y registro de la política de control del acceso (en entornos SCI, la política aborda específicamente las propiedades y requisitos únicos de los SCI y las relaciones con los sistemas que no son SCI).	3	3	3	3	
G[AC.01]2-02	[AC.01] Requisitos empresariales para el control del acceso	Se registran y aprueban las políticas y procedimientos de acceso de usuarios, para conceder y revocar tanto el acceso normal como el acceso privilegiado a las aplicaciones, bases de datos e infraestructuras del servidor y de la red, de acuerdo con los requisitos empresariales, de seguridad, de cumplimiento y con los requisitos de los acuerdos de nivel de servicio.	3	3	3	3	
G[AC.01]2-03	[AC.01] Requisitos empresariales para el control del acceso	La organización emplea el concepto del mínimo privilegio.	2	2	2	2	

G[AC.01]3-01	[AC.01] Requisitos empresariales para el control del acceso	Las cuentas con privilegios del sistema y de administración no se asignan a usuarios no privilegiados, sino que se reservan para un mínimo (personal o funciones autorizados), se monitorizan de forma exhaustiva y han de ser sometidas a una inspección adicional.	1	1	1		
G[AC.02]2-01	[AC.02] Procedimientos de inicio de sesión seguros	No se muestran los identificadores del sistema o de la aplicación hasta que el proceso de inicio de sesión no se haya completado con éxito.	2	2	2	2	
G[AC.02]2-02	[AC.02] Procedimientos de inicio de sesión seguros	Limitar a más de 6 el número permitido de intentos fallidos de inicio de sesión.				1	
G[AC.02]2-05	[AC.02] Procedimientos de inicio de sesión seguros	No ofrecer mensajes de ayuda durante el proceso de inicio de sesión que pudieran resultar de ayuda a usuarios no autorizados.	2	2	2	2	
G[AC.02]2-06	[AC.02] Procedimientos de inicio de sesión seguros	Imponer un tiempo de espera de 30 minutos para continuar con más intentos de inicio de sesión cuando se alcanza el número máximo de intentos de inicio de sesión.				1	
G[AC.02]3-02	[AC.02] Procedimientos de inicio de sesión seguros	Limitar a 6 el número permitido de intentos fallidos de inicio de sesión.			1		
G[AC.02]3-03	[AC.02] Procedimientos de inicio de sesión seguros	Rechazar cualquier intento adicional sin autorización específica cuando se alcanza el número máximo de intentos de inicio de sesión.	2	2	1		
G[AC.02]4-03	[AC.02] Procedimientos de inicio de sesión seguros	Limitar a 3 el número permitido de intentos fallidos de inicio de sesión.	1	1			
G[AC.02]4-06	[AC.02] Procedimientos de inicio de sesión seguros	Se emplea una doble autenticación para gestionar los componentes críticos de la infraestructura, como los cortafuegos.	1	1			
G[AC.02]4-07	[AC.02] Procedimientos de inicio de sesión seguros	Los sistemas pueden limitar el número máximo de sesiones simultáneas por cuenta, por tipo de cuenta o a través de una combinación.	2	2			
G[AC.03]2-02	[AC.03] Identificación y autenticación de usuarios	La adición, eliminación y modificación de cuentas, credenciales y otros objetos de identificación requiere de la aprobación por parte de usuarios autorizados (especialmente la identificación compartida, los invitados, la identificación temporal y las urgentes).	3	3	3	3	
G[AC.03]2-03	[AC.03] Identificación y autenticación de usuarios	Usar identificaciones de usuario únicas. El uso de identificaciones grupales solo se permite en los casos en los que resulta necesario por motivos empresariales u operacionales, siendo siempre aprobadas y registradas.	1	1	1	1	
G[AC.03]2-04	[AC.03] Identificación y autenticación de usuarios	Eliminar/desactivar cuentas de usuario inactivas al menos de forma anual.				1	
G[AC.03]3-04	[AC.03] Identificación y autenticación de usuarios	Eliminar/desactivar cuentas de usuario inactivas al menos cada 90 días.		1	1		
G[AC.03]3-05	[AC.03] Identificación y autenticación de usuarios	El sistema de información elimina automáticamente cuentas temporales y urgentes tras su periodo de validez.	2	2	2		
G[AC.03]4-01	[AC.03] Identificación y autenticación de usuarios	Implementación de mecanismos de autenticación con contraseña de un solo uso.	2	2			

G[AC.03]4-04	[AC.03] Identificación y autenticación de usuarios	Cuando se usan otros mecanismos de autenticación (por ejemplo, identificadores físicos o lógicos, tarjetas inteligentes, certificados, etc.), el uso de dichos mecanismos debe asignarse de la siguiente forma: Los mecanismos de autenticación deben ser asignados a una cuenta individual y no deben ser compartidos por múltiples cuentas. Los controles físicos y/o lógicos se deben aplicar para garantizar que solo la cuenta prevista pueda usar esos mecanismos para acceder.	2	2			
G[AC.03]5-03	[AC.03] Identificación y autenticación de usuarios	Eliminar/desactivar cuentas de usuario inactivas al menos cada 30 días.	1				
G[AC.03]5-04	[AC.03] Identificación y autenticación de usuarios	La organización desactiva las cuentas de usuarios que suponen un riesgo considerable en un plazo de 15 días a partir de la detección del riesgo.	2				
G[AC.04]2-01	[AC.04] Sistema de gestión de contraseñas (si procede)	Imponer cambios de contraseñas cada año.				1	
G[AC.04]2-02	[AC.04] Sistema de gestión de contraseñas (si procede)	Mantener un registro de las últimas contraseñas de los usuarios y evitar su reutilización.				1	
G[AC.04]2-03	[AC.04] Sistema de gestión de contraseñas (si procede)	Imponer una restricción de vida útil mínima.	2	2	2	2	
G[AC.04]2-04	[AC.04] Sistema de gestión de contraseñas (si procede)	Transmitir las contraseñas de forma protegida.				2	
G[AC.04]2-05	[AC.04] Sistema de gestión de contraseñas (si procede)	La contraseña inicial es temporal y los usuarios están obligados a cambiarla inmediatamente.	2	2	2	2	
G[AC.04]2-06	[AC.04] Sistema de gestión de contraseñas (si procede)	Las contraseñas temporales se otorgan a los usuarios de forma segura.	2	2	2	2	
G[AC.04]2-07	[AC.04] Sistema de gestión de contraseñas (si procede)	Las contraseñas no se almacenan sin protección en ningún sistema informático.				1	
G[AC.04]2-08	[AC.04] Sistema de gestión de contraseñas (si procede)	Modificación de las contraseñas preestablecidas del vendedor.	1	1	1	1	
G[AC.04]2-09	[AC.04] Sistema de gestión de contraseñas (si procede)	Exigir una contraseña de, al menos, 4 caracteres.				1	
G[AC.04]3-01	[AC.04] Sistema de gestión de contraseñas (si procede)	Imponer cambios de contraseñas cada 90 días.			1		
G[AC.04]3-02	[AC.04] Sistema de gestión de contraseñas (si procede)	Mantener un registro de las 4 últimas contraseñas de los usuarios y evitar su reutilización.			1		
G[AC.04]3-04	[AC.04] Sistema de gestión de contraseñas (si procede)	Usar contraseñas que contengan tanto caracteres numéricos como alfabéticos.			1		
G[AC.04]3-05	[AC.04] Sistema de gestión de contraseñas (si procede)	Las contraseñas no se almacenan como texto sin cifrar en ningún sistema informático.			1		
G[AC.04]3-06	[AC.04] Sistema de gestión de contraseñas (si procede)	Exigir una contraseña de, al menos, 7 caracteres.		1	1		

G[AC.04]4-01	[AC.04] Sistema de gestión de contraseñas (si procede)	Imponer cambios de contraseñas cada 60 días.		1			
G[AC.04]4-02	[AC.04] Sistema de gestión de contraseñas (si procede)	Mantener un registro de las 6 últimas contraseñas de los usuarios y evitar su reutilización.		1			
G[AC.04]4-03	[AC.04] Sistema de gestión de contraseñas (si procede)	Imponer al menos dos (2) cambios de caracteres cuando se crean nuevas contraseñas.		2			
G[AC.04]4-04	[AC.04] Sistema de gestión de contraseñas (si procede)	Las contraseñas deben contener tanto caracteres numéricos como alfabéticos, minúsculas y mayúsculas.	1	1			
G[AC.04]4-05	[AC.04] Sistema de gestión de contraseñas (si procede)	La organización emplea herramientas automatizadas para determinar si los autenticadores son lo suficientemente fuertes para resistir los ataques que tienen por objetivo descubrirlos o ponerlos en riesgo.	2	2			
G[AC.04]4-06	[AC.04] Sistema de gestión de contraseñas (si procede)	Hacer ilegibles todas las credenciales (como contraseñas o frases) durante la transmisión y almacenamiento de todos los componentes del sistema usando una criptografía compleja.	1	1			
G[AC.04]5-01	[AC.04] Sistema de gestión de contraseñas (si procede)	Imponer cambios de contraseñas cada 30 días.	1				
G[AC.04]5-02	[AC.04] Sistema de gestión de contraseñas (si procede)	Mantener un registro de las 12 últimas contraseñas de los usuarios y evitar su reutilización.	1				
G[AC.04]5-03	[AC.04] Sistema de gestión de contraseñas (si procede)	Imponer al menos cuatro (4) cambios de caracteres cuando se crean nuevas contraseñas.	2				
G[AC.04]5-04	[AC.04] Sistema de gestión de contraseñas (si procede)	Exigir una contraseña de, al menos, 10 caracteres.	1				
G[AC.06]3-03	[AC.06] Periodo de inactividad de sesión	En entornos con personal y cuando no se requieran respuestas inmediatas del operador (SCI), la pantalla de sesión desaparece tras 60 minutos de inactividad.			2		
G[AC.06]4-02	[AC.06] Periodo de inactividad de sesión	Las sesiones de las aplicaciones y redes se cierran tras 60 minutos de inactividad.		2			
G[AC.06]4-03	[AC.06] Periodo de inactividad de sesión	En entornos con personal y cuando no se requieran respuestas inmediatas del operador (SCI), la pantalla de sesión desaparece tras 15 minutos de inactividad.	2	2			
G[AC.06]5-05	[AC.06] Periodo de inactividad de sesión	Las sesiones de las aplicaciones y redes se cierran tras 15 minutos de inactividad.	2				
G[AC.07]4-01	[AC.07] Límite del tiempo de conexión	Se utilizan intervalos de tiempo para sesiones interactivas regulares.	2	2			
G[AC.07]5-01	[AC.07] Límite del tiempo de conexión	Los periodos de conexión pueden restringirse al horario normal de oficina (si no se requiere su funcionamiento durante horas extra).	2				
G[ICS.01]3-01	[ICS.01] Gestión de cuentas	Gestión automática de las cuentas del sistema: la organización emplea mecanismos automáticos para reforzar la gestión de las cuentas del sistema de información.	2	2	2		
G[ICS.02]2-01	[ICS.02] Notificación de uso del sistema	Mostrar una nota de advertencia general avisando de que solo los usuarios autorizados deberían acceder al ordenador.	3	3	3	3	

G[ICS.03]3-01	[ICS.03] Bloqueo de sesión	Cuando no es aconsejable el bloqueo de sesión (se necesita una respuesta inmediata del operador), las pantallas se sitúan en una zona con controles de acceso físico que limitan el acceso a las personas con permiso y con necesidad de conocer la información mostrada.	2	2	2		
12. Desarrollo Seguro [SD]							
G[SD.03]2-01	[SD.03] Seguridad por Defecto (desarrollar sistemas y aplicaciones seguras)	Aprobación y distribución de la política redactada en materia de desarrollo seguro.	3	3	3	3	
G[SD.03]2-02	[SD.03] Seguridad por Defecto (desarrollar sistemas y aplicaciones seguras)	Incorporar la seguridad de la información mediante SDLC.	1	1	1	1	
G[SD.03]2-03	[SD.03] Seguridad por Defecto (desarrollar sistemas y aplicaciones seguras)	Implementación de una política de codificación que abarca: · Orientación arquitectónica (por ejemplo “que el nivel de disponibilidad de la página Web no se dirija directamente a la base de datos”). · Niveles mínimos de documentación requeridos. · Requisitos de pruebas obligatorias. · Niveles mínimos de comentarios en código y estilo de comentario preferido. · Uso de la gestión de excepciones. · Uso del flujo de bloques de control (por ejemplo, “Todos los usos del flujo condicional emplean bloques con declaración explícita"). · Nomenclatura preferida de variables, funciones, clases y métodos de tablas. · Preferencia de un código sostenible y legible a un código inteligente y complejo. · Modelado de amenazas/Análisis de riesgos. · Usar un juego actual de herramientas de compiladores. · Usar herramientas de análisis estático.	2	2	2	2	
G[SD.03]3-01	[SD.03] Seguridad por Defecto (desarrollar sistemas y aplicaciones seguras)	Servicios Web seguros desarrollados mediante: · Comunicaciones seguras. · Protección de las credenciales. · Garantía del buen estado de los mensajes. · Protección de la integridad y confidencialidad de los mensajes (por ejemplo, mediante el uso de SAML). · Control del acceso. · Registro de información que permite reconstruir la operación.	2	2	2		

G[SD.03]3-02	[SD.03] Seguridad por Defecto (desarrollar sistemas y aplicaciones seguras)	Desarrollar aplicaciones de software atendiendo a las mejores prácticas de la industria (Guía OWASP, SANS CWE Top 25, SAFEcode, CERT Secure Coding. etc.), al menos: · Usar el mínimo privilegio. · Implementar el sistema de sandboxing. · Minimizar el uso de las funciones de cadena inseguras y las funciones de almacenamiento. · Validar las entradas y salidas. · Usar operaciones de enteros exactos para las asignaciones de memoria dinámicas y matrices de offset. · Usar bibliotecas para proteger de las secuencias de comandos de sitios cruzados. · Usar formatos de datos canónicos. · Evitar la concatenación de cadenas para declaraciones SQL dinámicas. · Eliminar la criptografía simple. · Usar registros y rastreos. · Eliminar las cuentas de aplicaciones personalizadas, identificaciones de usuarios y contraseñas antes de convertirse en usuarios activos.	2	2	2		
G[SD.03]3-04	[SD.03] Seguridad por Defecto (desarrollar sistemas y aplicaciones seguras)	Los procesos de desarrollo requieren que los desarrolladores se formen en técnicas de codificación seguras.	1	1	1		
G[SD.03]3-05	[SD.03] Seguridad por Defecto (desarrollar sistemas y aplicaciones seguras)	Las pruebas incluyen: · Pruebas de robustez. · Pruebas de penetración.	2	2	2		
G[SD.04]2-02	[SD.04] Desarrollo externo de software	Requisitos contractuales para la calidad y la funcionalidad de la seguridad de códigos.	2	2	1	1	
G[SD.04]2-05	[SD.04] Desarrollo externo de software	Pruebas a realizar antes de la instalación para detectar códigos maliciosos y troyanos.			2	2	
G[SD.04]4-01	[SD.04] Desarrollo externo de software	Certificación de la calidad y precisión del trabajo realizado – revisión de códigos.	1	1			
G[SD.04]4-02	[SD.04] Desarrollo externo de software	Formación certificada en seguridad para desarrolladores de software externos.	2	2			
G[SD.05]1-01	[SD.05] Control de vulnerabilidades técnicas	Las vulnerabilidades se identifican ocasionalmente y se han identificado los orígenes de las vulnerabilidades.					1
G[SD.05]1-02	[SD.05] Control de vulnerabilidades técnicas	Inicio de la categorización y priorización de las vulnerabilidades.					1
G[SD.05]1-03	[SD.05] Control de vulnerabilidades técnicas	Inicio del proceso de gestión de las vulnerabilidades.					1
G[SD.05]2-01	[SD.05] Control de vulnerabilidades técnicas	Definición y establecimiento de las funciones y responsabilidades asociadas a la gestión de las vulnerabilidades técnicas, incluyendo la monitorización de vulnerabilidades, la evaluación de riesgos de las vulnerabilidades, reparaciones, seguimiento de activos y responsabilidades de coordinación.	2	2	2	2	

G[SD.05]2-04	[SD.05] Control de vulnerabilidades técnicas	Las evaluaciones internas y externas de vulnerabilidades se llevan a cabo anualmente y tras cambios significativos.				1	
G[SD.05]3-03	[SD.05] Control de vulnerabilidades técnicas	Primero se abordan los sistemas en alto riesgo: en el plazo de 1 mes tras su comercialización, se instalan los últimos parches de seguridad suministrados por el vendedor en los componentes de sistemas y el software crítico.			1		
G[SD.05]3-04	[SD.05] Control de vulnerabilidades técnicas	Uso de recursos de información para identificar las vulnerabilidades técnicas pertinentes y para mantener el nivel de concienciación en software y otras tecnologías.	2	2	2		
G[SD.05]3-05	[SD.05] Control de vulnerabilidades técnicas	La evaluación de las vulnerabilidades internas y externas se lleva a cabo trimestralmente y tras cambios significativos por personal cualificado.			1		
G[SD.05]3-06	[SD.05] Control de vulnerabilidades técnicas	Existe un proceso formal para identificar y asignar una escala de riesgo a las nuevas vulnerabilidades de seguridad.	1	1	1		
G[SD.05]3-08	[SD.05] Control de vulnerabilidades técnicas	La organización emplea herramientas de análisis de vulnerabilidades que incluyen la capacidad de actualizar fácilmente las vulnerabilidades del sistema de información que han de ser analizadas (antes de un nuevo análisis o cuando se identifican y notifican nuevas vulnerabilidades).	1	1	1		
G[SD.05]4-01	[SD.05] Control de vulnerabilidades técnicas	La evaluación de vulnerabilidades internas y externas se lleva a cabo mensualmente y tras cambios significativos, usando fuentes de información de vulnerabilidades y con categorización y prioridades actualizadas.	2	1			
G[SD.05]4-04	[SD.05] Control de vulnerabilidades técnicas	Ninguna vulnerabilidad “de alto riesgo” detectada en los análisis de vulnerabilidad.	1	1			
G[SD.05]5-01	[SD.05] Control de vulnerabilidades técnicas	Aplicación de acciones de mejora en los análisis de vulnerabilidades, los orígenes de las vulnerabilidades y en la revisión de su información, así como en la priorización y categorización de las vulnerabilidades.	2				
G[SD.05]5-02	[SD.05] Control de vulnerabilidades técnicas	Se aplican continuas acciones de mejora en el proceso de gestión de vulnerabilidades.	2				
G[ICS.20]3-01	[ICS.20] Acceso privilegiado al análisis de vulnerabilidades	El sistema de información implementa una autorización de acceso privilegiado a componentes críticos de los sistemas de información para actividades de análisis de vulnerabilidades seleccionadas.	2	2	2		
13. Gestión de Incidentes [IH]							
G[IH.01]1-01	[IH.01] Notificación de los incidentes y deficiencias de seguridad de la información	Procedimiento inicial para medir el tiempo entre la identificación de incidentes/ataques informáticos y su notificación al equipo de respuesta.					1
G[IH.01]1-02	[IH.01] Notificación de los incidentes y deficiencias de seguridad de la información	Detección y notificación de los incidentes de seguridad recientemente iniciados.					1
G[IH.01]1-03	[IH.01] Notificación de los incidentes y deficiencias de seguridad de la información	Explicación de los incidentes según la tipificación predefinida recientemente iniciada.					2

G[IH.01]1-04	[IH.01] Notificación de los incidentes y deficiencias de seguridad de la información	Criterios de identificación de incidentes recientemente iniciados, pero no concluidos.					1
G[IH.01]2-02	[IH.01] Notificación de los incidentes y deficiencias de seguridad de la información	Establecimiento de un punto de contacto para la notificación de los incidentes de seguridad de la información.				1	
G[IH.01]2-03	[IH.01] Notificación de los incidentes y deficiencias de seguridad de la información	Los empleados, clientes, contratistas, terceros de sistemas de información y los usuarios de servicios han de anotar y notificar cualquier deficiencia de seguridad observada o de la que se tenga sospecha.	2	2	2	2	
G[IH.01]2-04	[IH.01] Notificación de los incidentes y deficiencias de seguridad de la información	Los incidentes en la seguridad de la información deben ser notificados mediante canales de comunicación predefinidos, de forma rápida y oportuna, de acuerdo con los requisitos legales, reglamentarios y contractuales.	1	1	1	1	
G[IH.01]3-02	[IH.01] Notificación de los incidentes y deficiencias de seguridad de la información	El punto de contacto para los incidentes en la seguridad de la información está disponible 8 horas al día durante 5 días.			1		
G[IH.01]3-03	[IH.01] Notificación de los incidentes y deficiencias de seguridad de la información	Existe un procedimiento de notificación de incidentes en la seguridad de la información, además de los procedimientos de respuesta y escalamiento de incidentes, que incluye la explicación de los incidentes de acuerdo con una tipificación predefinida (plan de respuesta a incidentes).	1	1	1		
G[IH.01]4-01	[IH.01] Notificación de los incidentes y deficiencias de seguridad de la información	El punto de contacto para los incidentes de seguridad de la información está disponible todos los días sin interrupción (en línea).		1			
G[IH.01]5-01	[IH.01] Notificación de los incidentes y deficiencias de seguridad de la información	El punto de contacto para los incidentes de seguridad de la información está disponible todos los días sin interrupción (en línea y por teléfono).	1				
G[IH.01]5-02	[IH.01] Notificación de los incidentes y deficiencias de seguridad de la información	Se aplican continuos métodos de mejora para la identificación del periodo entre la identificación y la notificación de los incidentes informáticos, los criterios de identificación, la explicación de incidentes, etc.	1				
G[IH.02]1-01	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	Los incidentes comienzan a ser analizados.					1
G[IH.02]1-02	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	Existe una estructura inicial definida para la gestión de incidentes.					1
G[IH.02]2-02	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	Existen procedimientos establecidos para gestionar los diferentes tipos de incidentes en la seguridad de la información (por ejemplo, si se detecta un punto de acceso inalámbrico no autorizado o se generan alertas por la detección de cambios).				2	
G[IH.02]2-03	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	Las acciones para recuperarse de las violaciones de seguridad y los fallos del sistema se controlan cuidadosa y formalmente (permitidos, registrados, notificados a la gestión, etc.).				2	

G[IH.02]2-04	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	La organización monitoriza y registra los incidentes en la seguridad del sistema de información.	1	1	1	1	
G[IH.02]2-05	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	Identificación clara de las funciones y responsabilidades de los equipos.	1	1	1	1	
G[IH.02]3-01	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	Los procedimientos abarcan: el análisis y la identificación de la causa, contención, planificación e implementación de medidas correctivas, la comunicación con las personas afectadas o involucradas en la recuperación, y la notificación de las medidas a las autoridades pertinentes.	1	1	1		
G[IH.02]3-04	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	Proporcionar una adecuada formación al personal con responsabilidades en materia de respuesta a las violaciones de seguridad.	2	2	2		
G[IH.02]3-06	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	Proceso para modificar y desarrollar el plan de respuesta a incidentes de acuerdo con la experiencia acumulada y para incorporar los desarrollos de la industria.	2	2	2		
G[IH.02]3-07	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	La organización desarrolla un plan de respuesta a incidentes que incluye lo siguiente: · Funciones, responsabilidades, estrategias de comunicación y contacto en caso de problemas, incluyendo la notificación de las marcas de pago, como mínimo. · Procedimientos de respuesta a incidentes específicos. · Procedimientos de recuperación y continuidad empresarial. · Procesos de copia de seguridad de datos. · Análisis de requisitos legales para la notificación de problemas. · Cobertura y respuestas de todos los componentes críticos del sistema.	1	1	1		
G[IH.02]4-01	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	La organización emplea mecanismos automáticos para reforzar el proceso de gestión de incidentes.		2			
G[IH.02]4-02	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	Existen mecanismos establecidos para permitir la cuantificación y monitorización de los tipos, volúmenes y costes de los incidentes en la seguridad de la información, así como los criterios de identificación de incidentes (con el objetivo de identificar incidentes recurrentes o de alto impacto).	2	2			
G[IH.02]4-04	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	La capacidad de respuesta a los incidentes del sistema de información se analiza, al menos, anualmente y se actualiza de acuerdo con los resultados de las pruebas.	2	2			
G[IH.02]5-01	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	La organización emplea mecanismos automáticos para aumentar la disponibilidad de la información y apoyo relacionados con la respuesta a incidentes.	1				
G[IH.02]5-05	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	Incorporación de Incidentes simulados en la formación en materia de respuesta a incidentes para facilitar la respuesta efectiva del personal en situaciones de crisis.	1				

G[IH.02]5-06	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	Alertas de seguridad, advertencias y directrices de seguridad de la información realizadas por una organización externa de forma continua.	2				
G[IH.02]5-07	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	Establecimiento de un CSIRT oficial.	1				
G[IH.02]5-08	[IH.02] Gestión de incidentes y mejoras de seguridad de la información	Se aplican continuas mejoras a la respuesta a incidentes, por ejemplo, como resultado de la medida de los tiempos para la resolución de incidentes.	2				
G[ICS.05]2-01	[ICS.05] Intercambio de información	La organización colabora e intercambia información sobre los incidentes potenciales de forma puntual con el correspondiente CSIRT/CERT.	1	1	1	1	
G [ICS.15]2-01	[ICS.15] Política y procedimientos para la respuesta a incidentes	La organización desarrolla un plan de respuesta a incidentes que incluye lo siguiente: Funciones, responsabilidades y estrategias de comunicación y contacto en el caso de problemas, incluyendo la notificación de las marcas de pago, como mínimo. Procedimientos de respuesta a incidentes específicos. Procedimientos de recuperación y continuidad empresarial. Procesos de copia de seguridad de datos. Análisis de requisitos legales para la notificación de problemas. Cobertura y respuestas de todos los componentes críticos del sistema.	3	3	3	3	
G [ICS.15]2-02	[ICS.15] Política y procedimientos para la respuesta a incidentes	Proporcionar una adecuada formación al personal con responsabilidades en materia de respuesta a las violaciones de seguridad.	1	1	1	1	
G[ICS.29]1-01	[ICS.29] Notificación de incidentes	Se han remitido varias notificaciones de incidentes graves en la seguridad a las Fuerzas de Seguridad del Estado.					1
G[ICS.29]2-01	[ICS.29] Notificación de incidentes	Existe un procedimiento informal para notificar incidentes graves a las Fuerzas de Seguridad del Estado.				1	
G[ICS.29]3-01	[ICS.29] Notificación de incidentes	Existe un procedimiento registrado y aprobado para notificar incidentes graves a las Fuerzas de Seguridad del Estado.			1		
G[ICS.29]4-01	[ICS.29] Notificación de incidentes	Gestión, actualización y verificación del procedimiento de notificación de incidentes graves en la seguridad.		1			

5.2. Controles relacionados con la confidencialidad

Referencia	Sección	Control	A	B	C	D	E
02. Operación de Sistemas [SO]							

C[SO.03]2-01	[SO.03] Procedimientos de gestión de la información	Todos los medios se etiquetan para indicar su nivel de clasificación.	2	2	2	2	
C[SO.03]4-03	[SO.03] Procedimientos de gestión de la información	La información altamente confidencial se cifra tanto en su fase de inactividad como en la de tránsito.	1	1			
03. Seguridad del Personal [PS]							
C[PS.01]3-02	[PS.01] Responsabilidades del usuario	Se exige a los usuarios que firmen una declaración en la que indiquen que han entendido las condiciones de acceso.	2	2	2		
04. Seguridad de la Instalación [FS]							
C[FS.04]3-01	[FS.04] Seguridad de los equipos fuera de las instalaciones	Codificación de la información en dispositivos móviles (ordenadores portátiles, tabletas, smartphones, etc.).			2		
C[FS.05]2-01	[FS.05]. Protección de los medios físicos en tránsito	Los medios se envían en paquetes para proteger el contenido de daños físicos.				2	
C[FS.05]2-02	[FS.05] Protección de los medios físicos en tránsito	Uso de envases cerrados.				2	
C[FS.05]3-01	[FS.05] Protección de los medios físicos en tránsito	Los medios se cifran o protegen con protección equivalente.	2	2	2		
C[FS.05]3-02	[FS.05] Protección de los medios físicos en tránsito	Inventarios y registros de entrada y salida de todos los dispositivos con capacidad de almacenamiento.	2	2	2		
C[FS.05]4-01	[FS.05] Protección de los medios físicos en tránsito	Solo se utilizan empresas de mensajería de confianza (lista cerrada).	2	2			
C[FS.05]4-02	[FS.05] Protección de los medios físicos en tránsito	Medios enviados mediante mensajería segura u otro método de entrega que pueda ser rastreado con precisión.		2			
C[FS.05]4-03	[FS.05] Protección de los medios físicos en tránsito	Existe un procedimiento para detectar cualquier diferencia entre los medios enviados y los medios recibidos.	2	2			

C[FS.05]5-02	[FS.05] Protección de los medios físicos en tránsito	Los medios se entregan en mano.	2				
C[FS.06]2-01	[FS.06] Eliminación segura de equipos	Existe una política aprobada para la reutilización y eliminación de los equipos.				3	
C[FS.06]3-01	[FS.06] Eliminación segura de equipos	La política para la reutilización y eliminación de quipos se aplica *ad hoc*.	3	3	3		
C[FS.07]2-01	[FS.07] Gestión de medios extraíbles	Todos los medios se almacenan en un entorno seguro y vigilado.	2	2	2	2	
C[FS.07]2-02	[FS.07] Gestión de medios extraíbles	Los medios están disponibles para el personal autorizado.	1	1	1	1	
C[FS.07]2-03	[FS.07] Gestión de medios extraíbles	Se requiere autorización para los medios extraídos de la organización.	2	2	2	2	
C[FS.07]3-01	[FS.07] Gestión de medios extraíbles	Se imposibilita la recuperación del contenido de los medios reutilizables que han de ser eliminados de la organización cuando ya no resulta necesario.	2	2	2		
C[FS.07]4-01	[FS.07] Gestión de medios extraíbles	El etiquetado de los medios resulta comprensible para los usuarios autorizados, pero no para los usuarios externos.	2	2			
C[FS.08]2-01	[FS.08] Eliminación de los medios	Los medios se eliminan de forma segura y vigilada (incineración, trituración, etc.).	2	2	2	2	
C[FS.08]3-01	[FS.08] Eliminación de los medios	Existen procedimientos establecidos para identificar los elementos que han de ser eliminados de forma segura, al menos, anualmente.			2		
C[FS.08]3-02	[FS.08] Eliminación de los medios	Los medios almacenados para su eliminación se guardan en un sitio seguro.	2	2	2		
C[FS.08]3-03	[FS.08] Eliminación de los medios	Rastreo, registro y verificación de las acciones de desinfección y eliminación de medios.	2	2	2		
C[FS.08]3-04	[FS.08] Eliminación de los medios	Los equipos y procedimientos de desinfección se examinan, al menos, anualmente.	2	2	2		
C[FS.08]4-01	[FS.08] Eliminación de los medios	Existen procedimientos establecidos para identificar los elementos que han de ser eliminados de forma segura al menos bianualmente	2	2			
C[FS.08]5-01	[FS.08] Eliminación de los medios	La desinfección de medios críticos se aplica mediante la regla de las dos personas.	2				
C[FS.08]5-02	[FS.08] Eliminación de los medios	La organización examina los equipos y procedimientos de desinfección para verificar que se está consiguiendo la desinfección prevista.	2				

C[FS.09]3-02	[FS.09] Política de escritorio limpio y de pantalla limpia	Los sistemas de información ocultan, mediante el cierre de sesión o mediante protección física, la información visible previamente en la pantalla con una imagen visible públicamente.	2	2	2		
05. Procesamiento para Terceros [TPP]							
C[TPP.01]3-01	[TPP.01] Procesamiento compartido	Cada entidad solo ejecuta procesos que tienen acceso a los datos de su entidad.	1	1	1		
09. Controles de Redes [NC]							
C[NC.05]3-01	[NC.05] Salvaguardar la confidencialidad en redes públicas	Usar una criptografía compleja y protocolos de seguridad para proteger los datos confidenciales durante las transmisiones en redes abiertas y públicas: Internet, redes inalámbricas, GSM, GPRS, etc.	1	1	1		
C[NC.05]3-03	[NC.05] Salvaguardar la confidencialidad en redes públicas	Solo se aceptan certificados de autoridades de certificación de confianza.	1	1	1		
C[NC.05]5-01	[NC.05] Salvaguardar la confidencialidad en redes públicas	Proveedor para implementar DNSSEC.	2				
C[NC.05]5-03	[NC.05] Salvaguardar la confidencialidad en redes públicas	Los sistemas de información que proporcionan colectivamente servicios de resolución de nombres/direcciones están a prueba de fallos e implementan la separación de funciones internas/externas.	2				
11. Controles de Acceso [AC]							
C[AC.02]5-01	[AC.02] Procedimientos de inicio de sesión seguros	Los sistemas de información implementan la autenticación multifactor para accesos locales a cuentas no privilegiadas.	1				
C[AC.02]5-02	[AC.02] Procedimientos de inicio de sesión seguros	Los sistemas de información implementan la autenticación multifactor para los accesos remotos a cuentas privilegiadas y no privilegiadas, de forma que se facilite uno de los factores a través de un dispositivo separado del sistema que accede.	1				

C[AC.08]2-01	[AC.08] Gestión de acceso de usuarios	Existe un procedimiento de registro de usuarios oficial establecido para otorgar y revocar el acceso a todos los sistemas de información y servicios que: · Comprueban que el usuario posee la autorización del propietario del sistema para el uso del sistema de información o servicio. · Comprueban que el nivel de acceso otorgado es apropiado al objetivo empresarial y cumple con la política de seguridad de la organización. · Restringen los derechos de acceso a la identificación de usuarios privilegiados a los privilegios mínimos necesarios para realizar las responsabilidades del trabajo. · Asignan privilegios atendiendo a la clasificación y función individual del personal de trabajo. · Los controles de acceso se implementan mediante un sistema de control de acceso automático. · Verifican la identidad del usuario antes de restablecer contraseñas. · Mantienen un registro oficial de todas las personas registradas para usar el servicio. · Revocan inmediatamente el acceso de usuarios que finalizan su labor.	3	3	3	3	
C[AC.08]3-01	[AC.08] Gestión de acceso de usuarios	El procedimiento de control de acceso incluye: · Buscar, eliminar o bloquear anualmente identificaciones de usuarios y cuentas redundantes. · Acceso "denegado para todos", a menos que se especifique lo contrario. · Autenticar todos los accesos a cualquier base de datos. Esto incluye todos los accesos de las aplicaciones, administradores y demás usuarios.	2	2	1		
C[AC.08]4-01	[AC.08] Gestión de acceso de usuarios	El procedimiento de control de acceso incluye: · No hay identificaciones de grupos, ni siquiera para la administración de usuarios (root). · No usar cuentas y contraseñas grupales, compartidas o genéricas, u otros métodos de autenticación. · Revocar o eliminar inmediatamente los derechos de acceso de los usuarios que han cambiado de funciones o trabajos o han abandonado la organización. · Buscar, eliminar o bloquear mensualmente identificaciones de usuarios y cuentas redundantes. · Garantizar que las identificaciones de usuarios redundantes no se otorgan a otros usuarios.	2	2			
14. Criptografía [CR]							
C[CR.01]2-01	[CR.01] Gestión principal	Definición y aprobación de la política sobre el uso de controles criptográficos.	3	3	3	3	

5.3. Controles relacionadas con la integridad

Referencia	Sección	Control	A	B	C	D	E
02. Operación de Sistemas							

I[SO.09]2-01	[SO.09] Procesamiento correcto en aplicaciones	Validación de los datos de entrada: · Definición de las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.	2	2	2	2	
I[SO.09]2-02	[SO.09] Procesamiento correcto en aplicaciones	Control del procesamiento interno: · Revisar todos los registros y archivos.	1	1	1	1	
I[SO.09]2-03	[SO.09] Procesamiento correcto en aplicaciones	Validación de los datos de salida: · Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos. · Los errores de validación de los datos de entrada se revisan y resuelven de manera puntual. · El sistema de información actúa de forma predecible y registrada cuando se reciben datos de entrada no válidos. · El sistema de información identifica las potenciales condiciones de error en materia de seguridad, genera mensajes de errores que proporcionan la información necesaria para aplicar medidas correctivas sin revelar información confidencial y solo revela dichos mensajes al personal autorizado.	2	2	2	2	
I[SO.09]3-01	[SO.09] Procesamiento correcto en aplicaciones	Validación de los datos de entrada: · Revisión de los límites de los datos de entrada. · Limitar las entradas de datos a rangos específicos. · Procedimientos para responder a los errores de validación. · Registro de las actividades involucradas en el proceso de entrada de datos.	1	1	1		
I[SO.09]4-01	[SO.09] Procesamiento correcto en aplicaciones	Validación de los datos de entrada: · Revisión periódica del contenido de los campos principales. · Inspección de los documentos impresos de entrada para detectar cambios no autorizados.	2	2			
04. Seguridad de la Instalación [FS]							
I[FS.04]3-01	[FS.04] Seguridad de los equipos fuera de las instalaciones	Codificación de la información en dispositivos móviles (ordenadores portátiles, tabletas, smartphones, etc.).			2		
I[FS.04]4-01	[FS.04] Seguridad de los equipos fuera de las instalaciones	Codificación compleja de la información en dispositivos móviles (ordenadores portátiles, tabletas, smartphones, etc.).	2	2			
05. Procesamiento para Terceros [TPP]							
I[TPP.01]3-01	[TPP.01] Procesamiento compartido	Cada entidad solo ejecuta procesos que tienen acceso a los datos de su entidad.	1	1	1		
09. Controles de Red [NC]							

I[NC.06]3-01	[NC.06] Controles para salvaguardar la integridad en redes públicas	Implementación de mecanismos criptográficos para detectar cambios en la información durante su transmisión.	1	1	1		
I[NC.06]3-03	[NC.06] Controles para salvaguardar la integridad en redes públicas	Solo se aceptan certificados de autoridades de certificación de confianza.	1	1	1		
I[NC.06]5-01	[NC.06] Controles para salvaguardar la integridad en redes públicas	Proveedor para implementar DNSSEC.	2				
I[NC.06]5-03	[NC.06] Controles para salvaguardar la integridad en redes públicas	Los sistemas de información que proporcionan colectivamente servicios de resolución de nombres/direcciones están a prueba de fallos e implementan la separación de funciones internas/externas.	2				
11. Controles de Acceso [AC]							
I[AC.08]3-01	[AC.08] Gestión de acceso de usuarios	El procedimiento de control de acceso implica: · Buscar, eliminar o bloquear anualmente identificaciones de usuarios y cuentas redundantes. · Acceso "denegado para todos", a menos que se especifique lo contrario. · Autenticar todos los accesos a cualquier base de datos. Esto incluye todos los accesos de las aplicaciones, administradores y demás usuarios.	2	2	2		
I[AC.08]2-01	[AC.08] Gestión de acceso de usuarios	Existe un procedimiento de registro de usuarios oficial establecido para otorgar y revocar el acceso a todos los sistemas de información y servicios que: · Comprueban que el usuario posee la autorización del propietario del sistema para el uso del sistema de información o servicio. · Comprueban que el nivel de acceso otorgado es apropiado al objetivo empresarial y cumple con la política de seguridad de la organización. · Restringen los derechos de acceso a las identificaciones de usuarios privilegiados a los privilegios mínimos necesarios para realizar las responsabilidades del trabajo. · Asignan privilegios atendiendo a la clasificación y función individual del personal de trabajo. · Los controles de acceso se implementan mediante un sistema de control de acceso automático. · Verifican la identidad del usuario antes de restablecer contraseñas. · Mantienen un registro oficial de todas las personas registradas para usar el servicio. · Revocan inmediatamente el acceso de usuarios que cesan su trabajo.	3	3	3	3	

I[AC.08]4-01	[AC.08] Gestión de acceso de usuarios	El procedimiento de control de acceso incluye: · No hay identificaciones de grupos, ni siquiera para la administración de usuarios (root). · No usar cuentas y contraseñas grupales, compartidas o genéricas, u otros métodos de autenticación. · Revocar o eliminar inmediatamente los derechos de acceso de los usuarios que han cambiado de funciones o trabajos o han abandonado la organización. · Buscar, eliminar o bloquear mensualmente identificaciones de usuarios y cuentas redundantes. · Garantizar que las identificaciones de usuarios redundantes no se otorgan a otros usuarios.	2	2			
I[AC.10]2-01	[AC.10] Gestión de privilegios	Hay un procedimiento de autorización oficial establecido.	3	3	3	3	
I[AC.10]3-03	[AC.10] Gestión de privilegios	El derecho de acceso de los usuarios se revisa y reasigna cuando cambian de un puesto de trabajo a otro.	2	2	2		
14. Criptografía [CR]							
I[CR.01]2-01	[CR.01] Gestión principal	Definición y aprobación de la política sobre el uso de controles criptográficos.	3	3	3	3	

5.4. Controles relacionadas con la disponibilidad

Referencia	Sección	Control	A	B	C	D	E
02. Operación de Sistemas [SO]							
A[ICS.13]2-01	[ICS.13] Modo seguro/protegido	El sistema de información, cuando se detectan condiciones definidas por la organización, entra en modo seguro. Por ejemplo, solo permite determinadas funciones que podrían llevarse a cabo con poca energía o con un ancho de banda de comunicaciones reducido.				1	
A[ICS.13]3-01	[ICS.13] Modo seguro/protegido	El sistema de información entra en modo de suspensión segura si se produce un fallo operativo en un dispositivo de protección.		1	1		
A[ICS.13]3-02	[ICS.13] Modo seguro/protegido	El sistema de información entra en un estado conocido y definido por la organización para preservar la información del estado del sistema con fallos.		1	1		
A[ICS.13]5-01	[ICS.13] Modo seguro/protegido	El sistema de información: · Verifica el correcto funcionamiento de las funciones de seguridad definidas por la organización; · Notifica al personal o las funciones definidos por la organización acerca de los análisis de verificación de seguridad fallidos, y · Apaga el sistema de información/reinicia el sistema de información cuando se detectan anomalías.	1				

A[ICS.13]5-02	[ICS.13] Modo seguro/protegido	El sistema de información automáticamente apaga el sistema de información/reinicia el sistema de información cuando se detectan violaciones de la integridad.	1				
04. Seguridad de la Instalación [FS]							
A[ICS.18]2-01	[ICS.18] Alimentación de emergencia	Fuente de energía alterna de larga duración para el sistema de información autónoma, no dependiente de la generación de energía externa y capaz de mantenerse en caso de pérdida prolongada de la fuente de energía primaria.	1	1	1	1	
A[ICS.19]5-01	[ICS.19] Protección contra daños por agua	La organización emplea mecanismos automáticos para detectar la presencia de agua cerca del sistema de información y alerta de ello.	2				
05. Procesamiento para Terceros [TPP]							
A[TPP.02]1-01	[TPP.02] Seguridad de la cadena de suministro	Se han producido comunicaciones iniciales con partes externas en relación a la ciberresiliencia y se han realizado algunos análisis.					1
A[TPP.02]2-01	[TPP.02] Seguridad de la cadena de suministro	Los mecanismos de comunicación no registrados (informales) establecidos con partes externas en materia de ciberresiliencia que pueden ser examinados.				1	
A[TPP.02]3-01	[TPP.02] Seguridad de la cadena de suministro	Documentos actualizados y mecanismos de comunicación examinados establecidos con partes externas en materia de ciberresiliencia.			1		
A[TPP.02]4-01	[TPP.02] Seguridad de la cadena de suministro	La organización coordina su plan de contingencia con los planes de contingencia de proveedores de servicios externos para garantizar que se puedan satisfacer los requisitos de contingencia (incluyendo los elementos de ciberresiliencia).	1	1			
A[TPP.02]5-01	[TPP.02] Seguridad de la cadena de suministro	Aplicación de acciones de mejora de las comunicaciones con partes externas en materia de ciberresiliencia.	3				
06. Resiliencia [RE]							
A[RE.02]2-04	[RE.02] Protección contra riesgos externos y ambientales	El sitio de procesamiento alterno ofrece garantías de seguridad de la información equivalentes a las del sitio principal.	2	2	2	2	
A[RE.04]1-01	[RE.04] Copia de seguridad de la información	Copias de seguridad realizadas a nivel de usuario y de sistema, información incluida en el sistema de información y documentación del sistema de información.	2	2	2	2	2
A[RE.04]2-04	[RE.04] Copia de seguridad de la información	Los datos copiados se almacenan, como mínimo, a 1 km de distancia.				1	
A[RE.04]2-05	[RE.04] Copia de seguridad de la información	El sitio de almacenamiento alterno ofrece garantías de seguridad de la información equivalentes a las del sitio principal.	2	2	2	2	

A[RE.04]2-06	[RE.04] Copia de seguridad de la información	La copia de seguridad se realiza una vez a la semana.				1	
A[RE.04]3-02	[RE.04] Copia de seguridad de la información	Los datos copiados se almacenan, como mínimo, a 10 km de distancia.			1		
A[RE.04]3-03	[RE.04] Copia de seguridad de la información	La recuperación de datos de la copia de seguridad se examina, al menos, cada 3 meses, comprobando su fiabilidad y la integridad de la información.			1		
A[RE.04]3-04	[RE.04] Copia de seguridad de la información	Establecimiento de políticas y procedimientos para la retención y almacenamiento de datos e implementación de mecanismos de copias de datos o mecanismos de redundancia para asegurar el cumplimiento con los requisitos reglamentarios, legales, contractuales y empresariales.	2	2	3		
A[RE.04]3-05	[RE.04] Copia de seguridad de la información	La copia de seguridad se realiza una vez al día.			2		
A[RE.04]3-06	[RE.04] Copia de seguridad de la información	Las copias de seguridad se almacenan en un establecimiento diferente o en un depósito resistente al fuego separado del sistema operativo.	2	2	2		
A[RE.04]3-07	[RE.04] Copia de seguridad de la información	El sistema de información implementa la recuperación de transacciones para sistemas basados en transacciones (por ejemplo, la reversión o registro de transacciones).					
A[RE.04]4-01	[RE.04] Copia de seguridad de la información	Los datos copiados se almacenan, como mínimo, a 10 km de distancia.		1			
A[RE.04]4-05	[RE.04] Copia de seguridad de la información	Se realizan dos (2) copias de seguridad diariamente.		1			
A[RE.04]5-01	[RE.04] Copia de seguridad de la información	Los datos copiados se almacenan, como mínimo, a 15 km de distancia.	1				
A[RE.04]5-04	[RE.04] Copia de seguridad de la información	Las copias de seguridad se realizan en línea.	1				

A[RE.06]1-01	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Inicio de la elaboración del Plan de Continuidad de Negocio, incluyendo la definición y comunicación de las funciones y responsabilidades.					2
A[RE.06]1-02	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Se han realizado algunas pruebas al plan de continuidad de negocio.					2
A[RE.06]1-03	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Realización parcial de un análisis de impacto sobre el negocio.					1
A[RE.06]1-04	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Inicio del proceso para identificar los servicios/procesos empresariales de los objetivos de tiempo de recuperación (RTO) y de los objetivos de puntos de recuperación (RPO).					1
A[RE.06]2-01	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	La organización desarrolla, disemina y revisa/actualiza una política de planificación de contingencia oficial y registrada que abarca el propósito, el alcance, las funciones, las responsabilidades, el compromiso con la gestión, la coordinación entre las entidades de la organización y el cumplimiento.	3	3	3	3	
A[RE.06]2-02	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	La organización desarrolla un plan de contingencia para el sistema de información que identifica los principales objetivos y funciones empresariales, proporciona objetivos de recuperación, abarca las funciones y responsabilidades de la contingencia, así como la restauración final y completa del sistema de información sin deteriorar las garantías de seguridad; plan que es aprobado.	2	2	2	2	
A[RE.06]2-03	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Comprender el riesgo que la organización está asumiendo en relación a la probabilidad e impacto en el tiempo, incluyendo la identificación y priorización de los procesos empresariales críticos (Análisis de Impacto sobre el Negocio – BIA, por sus siglas en inglés).	1	1	1	1	

A[RE.06]2-04	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Identificación de todos los activos implicados en los procesos empresariales críticos.	2	2	2	2	
A[RE.06]2-08	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	RPO – 7 días.				1	
A[RE.06]2-09	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	RTO – 72 horas.				1	
A[RE.06]2-10	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Distancia al sitio secundario > 1 km.				1	
A[RE.06]2-11	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	99,67% de disponibilidad (28,8 horas de interrupción al año).				1	
A[RE.06]3-01	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Los planes de contingencia se revisan y actualizan anualmente, y se coordinan con los elementos de la organización responsables de los planes relacionados.	1	1	1		
A[RE.06]3-03	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Identificación de los recursos financieros, organizativos, técnicos y ambientales necesarios para abordar los requisitos de seguridad de la información identificados.	2	2	2		

A[RE.06]3-06	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Establecimiento de un único marco de planes de continuidad de negocios para garantizar que todos los planes son sólidos y para identificar las prioridades de los análisis, así como el mantenimiento del mismo (condiciones para activar los planes, procedimientos operativos y de reanudación urgentes, recurrentes y temporales; programa de mantenimiento, actividades de formación, educación y concienciación, responsabilidades de los individuos, activos y recursos críticos necesarios).	2	2	2		
A[RE.06]3-08	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	El proveedor ha categorizado las prioridades para la recuperación, así como las prioridades de cada cliente final (por ejemplo, ALTA/MEDIA/BAJA).	2	2	2		
A[RE.06]3-09	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Identificación y tratamiento de las dependencias relativas al proceso de restauración.	2	2	2		
A[RE.06]3-10	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	RPO – 24 horas.			1		
A[RE.06]3-11	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	RTO – 24 horas.			1		
A[RE.06]3-12	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Distancia al sitio secundario > 10 km.			1		
A[RE.06]3-13	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	99,75% de disponibilidad (22 horas de interrupción al año).			1		

A[RE.06]4-02	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Anualmente, se evalúan los planes, los análisis de impacto sobre el negocio, los RTO, los RPO, las funciones, las responsabilidades y los procesos.		1			
A[RE.06]4-03	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	La organización evalúa el plan de contingencia en el sitio de procesamiento alterno, incluyendo una prueba de la copia de seguridad de la información en la restauración.		1			
A[RE.06]4-04	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	El plan de continuidad de operaciones se incorpora en los procesos y estructura de la organización. La responsabilidad se asigna a un nivel apropiado de la organización.	2	2			
A[RE.06]4-05	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	La organización planifica y se prepara ante circunstancias que impidan que se pueda regresar al sitio de procesamiento principal.		2			
A[RE.06]4-06	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Gestión, actualización y verificación de los Análisis de Impacto sobre el Negocio, los RTO y los RPO.		1			
A[RE.06]4-07	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	RPO – 12 horas.		1			
A[RE.06]4-08	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	RTO – 4 horas.		1			

A[RE.06]4-09	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Distancia al sitio secundario > 60 km.		1			
A[RE.06]4-10	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	99,98% de disponibilidad (1,6 horas de interrupción al año).		1			
A[RE.06]5-02	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Dos veces al año, se evalúan y actualizan los planes, los análisis de impacto sobre el negocio, los RTO, los RPO, las funciones, las responsabilidades y los procesos.	1				
A[RE.06]5-03	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	La organización incluye una completa recuperación y reconstitución del sistema de información a un estado conocido como parte del análisis del plan de contingencia.	1				
A[RE.06]5-04	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	La organización prepara el sitio de procesamiento alterno de forma que el sitio esté listo para ser usado como sitio operativo que refuerza los principales objetivos y funciones empresariales.	1				
A[RE.06]5-05	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Se dispondrá de personal alternativo en caso de incidente. Estarán sujetos a las mismas condiciones que el personal habitual.	1				
A[RE.06]5-06	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	RPO – 1 hora.	1				

A[RE.06]5-07	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	RTO – 1 hora.	1				
A[RE.06]5-08	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	Distancia al sitio secundario > 100 km.	1				
A[RE.06]5-09	[RE.06] Aspectos de la seguridad de la información del Plan de Continuidad de Operaciones (BCM)	99,99% de disponibilidad (0,8 horas de interrupción al año).	1				
A[RE.07]2-01	[RE.07] Mantenimiento de sistemas	La organización desarrolla, disemina y revisa/actualiza una política de mantenimiento del sistema de información oficial y registrada.				3	
A[RE.07]2-04	[RE.07] Mantenimiento de sistemas	La organización programa, realiza, registra y revisa los registros, mantenimientos y reparaciones de los componentes del sistema de información de acuerdo con las especificaciones del fabricante o vendedor.	2	2	2	2	
A[RE.07]3-01	[RE.07] Mantenimiento de sistemas	La organización desarrolla, disemina y revisa/actualiza los procedimientos oficiales y registrados para facilitar la implementación de la política de mantenimiento del sistema de información y los controles de mantenimiento del sistema asociados.			3		
A[RE.07]3-03	[RE.07] Mantenimiento de sistemas	Revisión de todos los controles de seguridad que hayan podido sufrir impactos para verificar que los controles siguen funcionando.	1	1	1		
A[RE.07]4-01	[RE.07] Mantenimiento de sistemas	La organización produce registros actualizados, precisos, completos y disponibles de todas las acciones de mantenimiento y reparación necesarias, en proceso y finalizadas.	2	2			
A[RE.07]4-02	[RE.07] Mantenimiento de sistemas	Aprobación, control y monitorización de las herramientas de mantenimiento del sistema de información.		2			
A[RE.07]4-03	[RE.07] Mantenimiento de sistemas	La organización audita sesiones de mantenimiento y diagnóstico no locales y revisa los registros de mantenimiento de las sesiones.	1	1			
A[RE.07]5-01	[RE.07] Mantenimiento de sistemas	Todas las herramientas de mantenimiento que el personal de mantenimiento lleva a una instalación son inspeccionadas para detectar modificaciones inadecuadas evidentes.	1				

A[RE.07]5-02	[RE.07] Mantenimiento de sistemas	Todos los medios que contienen programas de diagnóstico y análisis se revisan para detectar código malicioso antes de ser usado en el sistema de información y se evita la eliminación no autorizada de equipos de mantenimiento que contienen información de la organización, de la siguiente forma: (a) Verificando que los equipos no contienen información de la organización; (b) Desinfectando y destruyendo los equipos; (c) Reteniendo los equipos en la instalación; o (d) Obteniendo una exención del personal o cargos definidos por la organización que autorice explícitamente la extracción de los equipos de la instalación.	1				
A[RE.07]5-03	[RE.07] Mantenimiento de sistemas	La organización exige la realización de servicios de mantenimiento y diagnóstico no locales en un sistema de información que implemente una capacidad de seguridad comparable a la capacidad implementada en el sistema receptor de los servicios.	2				
A[RE.07]5-04	[RE.07] Mantenimiento de sistemas	Un solo fallo de cualquier capacidad del sistema, capacidad de los componentes o elementos de distribución no afectará el sistema.	1				
A[RE.08]1-XXX	[RE.08] Resiliencia operativa	Inicio de la identificación de los requisitos de la ciberresiliencia.					2
A[RE.08]2-06	[RE.08] Resiliencia operativa	Requisitos de la ciberresiliencia definidos pero no registrados.				2	
A[RE.08]3-06	[RE.08] Resiliencia operativa	Registro y actualización de los requisitos de la ciberresiliencia.			1		
A[RE.08]4-02	[RE.08] Resiliencia operativa	Gestión, actualización y verificación de los requisitos de la ciberresiliencia.		1			
A[RE.08]5-02	[RE.08] Resiliencia operativa	Los requisitos de la ciberresiliencia están sometidos a un plan de mejora continua.	2				
A[ICS.25]5-01	[ICS.25] Protección de Fallos Predecibles	La organización: a. Determina el tiempo medio antes del fallo (MTTF) para los componentes del sistema de información SCI; y b. Proporciona componentes del sistema de información de sustitución y un medio para intercambiar componentes activos y componentes en modo de espera atendiendo a los criterios de sustitución del MTTF definidos por la organización.	1				
A[ICS.28]1-01	[ICS.28] Acuerdos de ciberresiliencia	Contactos iniciales para establecer un acuerdo de ayuda mutua, cooperación e intercambio de información con organizaciones públicas.					1
A[ICS.28]1-02	[ICS.28] Acuerdos de ciberresiliencia	Contactos iniciales para establecer un acuerdo de ayuda mutua, cooperación e intercambio de información con organizaciones privadas.					1

A[ICS.28]2-01	[ICS.28] Acuerdos de ciberresiliencia	Acuerdo informal de ayuda mutua, cooperación e intercambio de información con organizaciones públicas.				1	
A[ICS.28]2-02	[ICS.28] Acuerdos de ciberresiliencia	Acuerdo informal de ayuda mutua, cooperación e intercambio de información con organizaciones privadas.				1	
A[ICS.28]3-01	[ICS.28] Acuerdos de ciberresiliencia	Registro, aprobación por parte de la Dirección y actualización de un acuerdo formal de ayuda mutua, cooperación e intercambio de información con organizaciones públicas.			1		
A[ICS.28]3-02	[ICS.28] Acuerdos de ciberresiliencia	Registro, aprobación por parte de la Dirección y actualización de un acuerdo formal de ayuda mutua, cooperación e intercambio de información con organizaciones privadas.			1		
A[ICS.28]4-01	[ICS.28] Acuerdos de ciberresiliencia	Gestión, actualización y verificación de un acuerdo formal de ayuda mutua, cooperación e intercambio de información con organizaciones públicas.		1			
A[ICS.28]4-02	[ICS.28] Acuerdos de ciberresiliencia	Gestión, actualización y verificación de un acuerdo formal de ayuda mutua, cooperación e intercambio de información con organizaciones privadas.		1			
A[ICS.28]5-01	[ICS.28] Acuerdos de ciberresiliencia	Aplicación de acciones de mejora a acuerdos formales de ayuda mutua, cooperación e intercambio de información con organizaciones públicas.	1				
A[ICS.28]5-02	[ICS.28] Acuerdos de ciberresiliencia	Aplicación de acciones de mejora a acuerdos formales de ayuda mutua, cooperación e intercambio de información con organizaciones privadas.	1				
A[ICS.30]1-01	[ICS.30] Gestión de dependencias	Inicio de las dependencias de servicios públicos.					1
A[ICS.30]1-02	[ICS.30] Gestión de dependencias	Inicio de las dependencias de proveedores de infraestructuras.					1
A[ICS.30]2-01	[ICS.30] Gestión de dependencias	Dependencias de servicios públicos identificadas, pero no registradas.				1	
A[ICS.30]2-02	[ICS.30] Gestión de dependencias	Dependencias de proveedores de infraestructuras identificadas, pero no registradas.				1	
A[ICS.30]3-01	[ICS.30] Gestión de dependencias	Identificación, registro y actualización de las dependencias de servicios públicos.			1		
A[ICS.30]3-02	[ICS.30] Gestión de dependencias	Identificación, registro y actualización de las dependencias de proveedores de infraestructuras.			1		
A[ICS.30]4-01	[ICS.30] Gestión de dependencias	Gestión, actualización y verificación de las dependencias de servicios públicos.		1			
A[ICS.30]4-02	[ICS.30] Gestión de dependencias	Gestión, actualización y verificación de las dependencias de proveedores de infraestructuras.		1			

A[ICS.30]5-01	[ICS.30] Gestión de dependencias	Aplicación de acciones de mejora en la identificación de las dependencias de servicios públicos.	1				
A[ICS.30]5-02	[ICS.30] Gestión de dependencias	Aplicación de acciones de mejora en la identificación de las dependencias de proveedores de infraestructuras.	1				
09. Controles de Red [NC]							
A[NC.07]3-01	[NC.07] Disponibilidad de los servicios de red	La organización establece servicios de telecomunicaciones alternativos, incluyendo los acuerdos necesarios para permitir la reanudación de las operaciones del sistema de información para los principales objetivos y funciones empresariales cuando las capacidades de telecomunicaciones no están disponibles ni en los sitios de procesamiento o almacenamiento principales ni en los alternos.			1		
A[NC.07]3-02	[NC.07] Disponibilidad de los servicios de red	Uso de soluciones tecnológicas para prevenir ataques DDoS conocidos.			1		
A[NC.07]4-01	[NC.07] Disponibilidad de los servicios de red	La organización obtiene servicios de telecomunicaciones alternativos teniendo en cuenta la reducción de la probabilidad de intercambiar un único punto de fallo con los servicios de telecomunicaciones principales.		1			
A[NC.07]4-03	[NC.07] Disponibilidad de los servicios de red	Controles empleados para mitigar los ataques DDoS: · Defensa en profundidad - análisis profundos de paquetes, aceleramiento de tráfico, ocultación de paquetes, etc. · Defensas contra ataques “internos” y externos.	1	1			
A[NC.07]5-01	[NC.07] Disponibilidad de los servicios de red	La organización obtiene proveedores de servicios de telecomunicaciones alternativos diferentes a los proveedores de servicios principales para reducir la susceptibilidad a los mismos peligros.	2				
A[NC.07]5-02	[NC.07] Disponibilidad de los servicios de red	La organización exige a los proveedores de servicios de telecomunicaciones, principales y alternativos, tener planes de contingencia y presentar pruebas de los análisis/formación de contingencia.	1				
12. Desarrollo Seguro [SD]							
A[ICS.10]5-01	[ICS.10] Entornos de pruebas separados	La organización analiza los cambios en los sistemas de información en un entorno de prueba separado antes de implementarlos en un entorno operativo, en busca de impactos en la seguridad provocados por fallos, debilidades, incompatibilidades o actividades maliciosas intencionadas.	1				
13. Gestión de Incidentes [IH]							
A [ICS.15]3-01	[ICS.15] Política y procedimientos para la respuesta a incidentes	La capacidad de respuesta a los incidentes del sistema de información se analiza, al menos, anualmente.	1	1	1		

A [ICS.15]3-02	[ICS.15] Política y procedimientos para la respuesta a incidentes	La organización coordina el análisis de respuesta a los incidentes con los elementos de la organización responsables de los planes relacionados.	1	1	1		
A[ICS.29]5-01	[ICS.29] Notificación de incidentes	Aplicación de acciones de mejora en la notificación de incidentes a las Fuerzas de Seguridad del Estado.	1				
14. Criptografía [CR]							
A[CR.01]3-01	[CR.01] Gestión principal	Mantenimiento de la disponibilidad de la información en caso de pérdida de claves criptográficas (por ejemplo, mediante mecanismos de custodia).	1	2	2		

6. REFERENCIAS

[1] Gobierno de España, “ESTRATEGIA DE SEGURIDAD NACIONAL,” 2013. [Online]. Available: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf.

[2] Gobierno de España, “ESTRATEGIA NACIONAL DE CIBERSEGURIDAD,” 2013. [Online]. Available: http://www.dsn.gob.es/es/file/146/download?token=KI839vHG

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

certsi_

CERT DE SEGURIDAD E INDUSTRIA