

SCV365[®] SOLUTIONS



COMPLIANCE
MANAGEMENT



WORKFORCE
CLEARANCE



CONTRACTS
MANAGEMENT



IT
ASSETS



CYBER
BI

*_

Transformación Digital

Holística, Segura, Robusta y Efectiva

Simplificando la gestión integral de GRC y ciberseguridad reduciendo la exposición a riesgo y sanciones.

Gobernanza, Riesgo y Cumplimiento (GRC)

Educación

Políticas, Procesos y Controles

Cadena
Suministro

Autorización
Individuos

Manejo de
Riesgo

Activos IT

Controles
Técnicos

Controles
Físicos

Planes de
Contingencia

Manejo de
Quejas

Manejo de
Incidentes

Registros y
Archivos



SCV365[®]

Multifactor
authentication for
remote access and
admin/privileged
controls



SCV365[®]

Endpoint Detection
and Response (EDR)



SCV365[®]

Secured, encrypted,
and tested backups



SCV365[®]

Privileged Access
Management (PAM)



SCV365[®]

Email filtering and web
security



SCV365[®]

Patch management and
vulnerability
management



SCV365[®]

Cyber incident response
planning and testing



SCV365[®]

Cybersecurity
awareness training and
phishing testing



SCV365[®]

Hardening techniques,
including Remote
Desktop Protocol (RDP)
mitigation



SCV365[®]

Logging and
monitoring/network
protections



SCV365[®]

End-of-life systems
replaced or protected



SCV365[®]

Vendor/digital supply
chain risk management

Hablemos sobre como potenciamos la transformación digital.

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com



COMPLIANCE
MANAGEMENT



WORKFORCE
CLEARANCE



CONTRACTS
MANAGEMENT



IT
ASSETS



CYBER
BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
GOBIERNO (GV)	La estrategia, expectativas y políticas de gestión de riesgos en ciberseguridad de la organización se establecen, comunican y monitorizan.	
Contexto Organizativo (GV.OC) • NIST SP 800-53 Rev. 4 CP-2, CP-8, CP-11, PE-9, PE-11, PM-8, PM-11, SA-12, SA-14 • NIST SP 800-171 Rev. 2: AC 3.1.4; RA 3.11.1, PS 3.9.1; CM 3.4.1 • ISO/IEC 27001:2013 A.11.1.4, A.11.2.2, A.11.2.3, A.12.1.3, A.15.1.3, A.15.2.1, A.15.2.2, A.17.1.1, A.17.1.2, A.17.2.1 • ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 • COBIT 5 APO02.01, APO02.06, APO03.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, DSS04.02 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(4)(ii), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(8), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314, 164.316 • RGPD Art. 1 (1-3); Art. 3 (1-3); Art. 14 (2) (a-g); Art. 28 (1-4); Art. 29; Art. 37 (1-7); Art. 38 (1-6); Art. 39 (1-2); Art. 40 (1-11)	Se comprenden las circunstancias —misión, expectativas de los grupos de interés, dependencias y requisitos legales, regulatorios y contractuales— que rodean las decisiones de gestión de riesgos de ciberseguridad de la organización. GV. OC-01: Se entiende y se informa de la misión organizativa en la gestión de riesgos de ciberseguridad. GV. OC-02: Se entienden a los interesados internos y externos, y se comprenden y consideran sus necesidades y expectativas respecto a la gestión de riesgos en ciberseguridad. GV. OC-03: Se entienden y gestionan los requisitos legales, regulatorios y contractuales relativos a la ciberseguridad, incluidas las obligaciones de privacidad y libertades civiles. GV. OC-04: Se comprenden y comunican los objetivos, capacidades y servicios críticos de los que dependen o esperan de la organización. GV. OC-05: Se entienden y comunican los resultados, capacidades y servicios de los que depende la organización.	✓ COMPLIANCE ✓ SUPPLY CHAIN ✓ CONTRACTS ✓ DOCUMENT MANAGEMENT
Estrategia de Gestión de Riesgos (GV.RM) • NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, PM-4, PM-9, PM-11, PM-12, PM-16, RA-2, RA-3, RA-5, SA-5, SA-11, SA-14, SI-2, SI-4, SI-5 • NIST SP 800-171 Rev. 2: CM 3.4.1; SA 3.12.1 – 3.12.4; AT 3.2.1 – 3.2.2 • ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 • ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • CCS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO13.02, DSS04.02 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(iii)(A), 164.308(a)(a)(6), 164.308(a)(7)(ii)(D), 164.308(a)(7)(iii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(a), 164.316(b)(2)(iii), 164.312(c), 164.312(e), 164.314, 164.316	Las prioridades, restricciones, declaraciones de tolerancia al riesgo y apetito, así como las suposiciones, se establecen, comunican y utilizan para apoyar las decisiones operativas de riesgo. GV. RM-01: Los objetivos de gestión de riesgos se establecen y acuerdan por los interesados organizativos. GV. RM-02: Se establecen, comunican y mantienen las declaraciones de apetito al riesgo y tolerancia al riesgo. GV. RM-03: Las actividades y resultados de gestión de riesgos en ciberseguridad se incluyen en los procesos de gestión de riesgos empresariales. GV. RM-04: Se establece y comunica una dirección estratégica que describe las opciones adecuadas de respuesta al riesgo. GV. RM-05: Se establecen líneas de comunicación en toda la organización para los riesgos de ciberseguridad, incluidos los riesgos de proveedores y otros terceros.	✓ COMPLIANCE ✓ IT ASSETS ✓ CYBER BI ✓ SUPPLY CHAIN ✓ CONTRACTS ✓ PROPERTY DOCUMENT MANAGEMENT

Hablemos sobre como potenciamos la transformación digital.

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com





COMPLIANCE
MANAGEMENT



WORKFORCE
CLEARANCE



CONTRACTS
MANAGEMENT



IT
ASSETS



CYBER
BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
GOBIERNO (GV)	La estrategia, expectativas y políticas de gestión de riesgos en ciberseguridad de la organización se establecen, comunican y monitorizan.	
• RGPD Art. 28 (1-4); Art. 29; Art. 32 (1-4); Art. 35 (1-6); Art. 77 80; 82-83	GV. RM-06: Se establece y comunica un método estandarizado para calcular, documentar, categorizar y priorizar riesgos de ciberseguridad. GV. RM-07: Se caracterizan y se incluyen oportunidades estratégicas (es decir, riesgos positivos) en las discusiones organizativas sobre riesgos de ciberseguridad.	
Roles, responsabilidades y autoridades (GV. RR) • NIST SP 800-53 Rev. 4 controles de todas las familias • NIST SP 800-171 Rev. 2: AT 3.2.1, 3.2.3; RA 3.11.1; IR 3.6.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.18.1 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3, 4.4.3.7 • COBIT 5 APO13.12, DSS04.02, MEA03.01, MEA03.04 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b), 164.310, 164.312, 164.314, 164.316 • RGPD Art. 6 (1-4) (a); Art. 10; Art. 15 (1-4); Art. 28 (1-4); Art. 29; Art. 32 (3-4); Art. 33 (1-5); Art. 34 (1-4); Art. 37 (1-7); Art. 38 (1-6); Art. 39 (1-2); Art. 40 (1-11); Art. 64-66; Art. 84-86	Se establecen y comunican los roles, responsabilidades y autoridades en ciberseguridad para fomentar la rendición de cuentas, la evaluación del desempeño y la mejora continua. GV. RR-01: El liderazgo organizativo es responsable y responsable del riesgo de ciberseguridad y fomenta una cultura consciente del riesgo, ética y en constante mejora. GV. RR-02: Se establecen, comunican, comprenden y hacen cumplir los roles, responsabilidades y autoridades relacionadas con la gestión de riesgos en ciberseguridad. GV. RR-03: Se asignan recursos adecuados de acuerdo con la estrategia, roles, responsabilidades y políticas de riesgos de ciberseguridad.. GV. RR-04: La ciberseguridad está incluida en las prácticas de recursos humanos.	✓ COMPLIANCE ✓ IT ASSETS ✓ WORKFORCE ✓ SUPPLY CHAIN ✓ CONTRACTS ✓ DOCUMENT MANAGEMENT
Política (GV. PO) • NIST SP 800-53 Rev. 4 controles de todas las familias • NIST SP 800-171 Rev. 2: AT 3.2.1, 3.2.3; RA 3.11.1; IR 3.6.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.18.1 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3, 4.4.3.7 • COBIT 5 APO13.12, DSS04.02, MEA03.01, MEA03.04 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b), 164.310, 164.312, 164.314, 164.316 • RGPD Art. 6 (1-4) (a); Art. 10; Art. 15 (1-4); Art. 28 (1-4); Art. 29; Art. 32 (3-4); Art. 33 (1-5); Art. 34 (1-4); Art. 37 (1-7); Art. 38 (1-6); Art. 39 (1-2); Art. 40 (1-11); Art. 64-66; Art. 84-86	Se establece, comunica y aplica la política de ciberseguridad organizacional GV. PO-01: La política para la gestión de riesgos de ciberseguridad se establece en función del contexto organizativo, la estrategia y las prioridades de ciberseguridad, y se comunica y aplica. GV. PO-02: Se revisa, actualiza, comunica y aplica la política para gestionar los riesgos de ciberseguridad para reflejar los cambios en los requisitos, amenazas, tecnología y misión organizativa.	✓ COMPLIANCE ✓ IT ASSETS ✓ DOCUMENT MANAGEMENT

Hablemos sobre como potenciamos la transformación digital.

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com





COMPLIANCE
MANAGEMENT



WORKFORCE
CLEARANCE



CONTRACTS
MANAGEMENT



IT
ASSETS



CYBER
BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
GOBIERNO (GV)	La estrategia, expectativas y políticas de gestión de riesgos en ciberseguridad de la organización se establecen, comunican y monitorizan.	
Supervisión (GV. OV) • NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, PM-4, PM-9, PM-11, PM-12, PM-16, RA-2, RA-3, RA-5, SA-5, SA-11, SA-14, SI-2, SI-4, SI-5 • NIST SP 800-171 Rev. 2: CM 3.4.1; SA 3.12.1 – 3.12.4; AT 3.2.1 – 3.2.2 • ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 • ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • CCS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO13.02, DSS04.02 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.308(a)(a)(6), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(a), 164.316(b)(2)(iii), 164.312(c), 164.312(e), 164.314, 164.316 • RGPD Art. 28 (1-4); Art. 29; Art. 32 (1-4); Art. 35 (1-6); Art. 77 80; 82-83	Los resultados de las actividades y el rendimiento de gestión de riesgos en ciberseguridad a nivel organizacional se utilizan para informar, mejorar y ajustar la estrategia de gestión de riesgos. GV. OV-01: Se revisan los resultados de la estrategia de gestión de riesgos en ciberseguridad para informar y ajustar la estrategia y la dirección. GV. OV-02: Se revisa y ajusta la estrategia de gestión de riesgos en ciberseguridad para garantizar la cobertura de los requisitos y riesgos organizativos. GV. OV-03: Se evalúa y revisa el rendimiento de gestión de riesgos de ciberseguridad organizacional para detectar los ajustes necesarios.	✓ COMPLIANCE ✓ IT ASSETS ✓ WORKFORCE ✓ SUPPLY CHAIN ✓ CONTRACTS ✓ DOCUMENT MANAGEMENT
Gestión de Riesgos en la Cadena de Suministro (GV. SC) • NIST SP 800-53 Rev. 4 CP-2, CP-8, CP-11, PE-9, PE-11, PM-8, PM-11, SA-12, SA-14 • NIST SP 800-171 Rev. 2: AC 3.1.4; RA 3.11.1, PS 3.9.1; CM 3.4.1 • ISO/IEC 27001:2013 A.11.1.4, A.11.2.2, A.11.2.3, A.12.1.3, A.15.1.3, A.15.2.1, A.15.2.2, A.17.1.1, A.17.1.2, A.17.2.1 • ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 • COBIT 5 APO02.01, APO02.06, APO03.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, DSS04.02 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(4)(ii), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(8), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314, 164.316 • RGPD Art. 1 (1-3); Art. 3 (1-3); Art. 14 (2) (a-g); Art. 28 (1-4); Art. 29; Art. 37 (1-7); Art. 38 (1-6); Art. 39 (1-2); Art. 40 (1-11)	Los procesos de gestión de riesgos en la cadena de suministro cibernética son identificados, establecidos, gestionados, supervisados y mejorados por los interesados organizativos. GV. SC-01: Se establece y acuerda un programa de gestión de riesgos en la cadena de suministro en ciberseguridad, la estrategia, los objetivos, las políticas y los procesos por parte de los interesados de la organización. GV. SC-02: Se establecen, comunican y coordinan los roles y responsabilidades de ciberseguridad para proveedores, clientes y socios tanto interna como externamente. GV. SC-03: La gestión de riesgos en la cadena de suministro en ciberseguridad se integra en la gestión de riesgos empresariales, en la gestión de riesgos y en los procesos de mejora y análisis de riesgos. GV. SC-04: Los proveedores son conocidos y priorizados por la criticidad.	✓ WORKFORCE ✓ SUPPLY CHAIN ✓ CONTRACTS

Hablemos sobre como potenciamos la transformación digital.

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com





COMPLIANCE
MANAGEMENT



WORKFORCE
CLEARANCE



CONTRACTS
MANAGEMENT



IT
ASSETS



CYBER
BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
GOBIERNO (GV)	La estrategia, expectativas y políticas de gestión de riesgos en ciberseguridad de la organización se establecen, comunican y monitorizan.	
	GV. SC-05: Se establecen, priorizan e integran los requisitos para abordar los riesgos de ciberseguridad en las cadenas de suministro en contratos y otros tipos de acuerdos con proveedores y otros terceros relevantes. GV. SC-06: Se realiza planificación y debida diligencia para reducir riesgos antes de establecer relaciones formales con proveedores u otros terceros. GV. SC-07: Los riesgos que plantea un proveedor, sus productos y servicios, y otros terceros se comprenden, registran, priorizan, evalúan, responden y monitorizan a lo largo de la relación. GV. SC-08: Los proveedores relevantes y otros terceros están incluidos en las actividades de planificación, respuesta y recuperación de incidentes. GV. SC-09: Las prácticas de seguridad en la cadena de suministro se integran en programas de ciberseguridad y gestión de riesgos empresariales, y su rendimiento se supervisa a lo largo del ciclo de vida del producto y servicio tecnológico. GV. SC-10: Los planes de gestión de riesgos en la cadena de suministro en ciberseguridad incluyen disposiciones para actividades que ocurren tras la firma de una asociación o acuerdo de servicio.	

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
IDENTIFICACIÓN (ID)	Se comprenden los riesgos actuales de ciberseguridad de la organización.	
Gestión de Activos (ID.AM) • NIST SP 800-53 Rev. 4 CM-8, AC-20, CP-2, RA-2, SA-9, SA-14, PS-7, PM-11 • NIST SP 800-171 Rev. 2: CM 3.4.1 • ISO/IEC 27001:2013 A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6 • ISA 62443-2-1:2009 4.2.3.4, 4.2.3.6, 4.3.2.3.3 • ISA 62443-3-3:2013 SR 7.8 • CCS CSC 1, CSC 2	Se identifican y gestionan los activos (por ejemplo, datos, hardware, software, sistemas, instalaciones, servicios, personas) que permiten a la organización alcanzar los objetivos empresariales de acuerdo con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización ID.AM-01: Se mantienen inventarios de hardware gestionados por la organización	✓ IT ASSETS ✓ CYBER BI

Hablemos sobre como potenciamos la transformación digital.

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com





COMPLIANCE
MANAGEMENT



WORKFORCE
CLEARANCE



CONTRACTS
MANAGEMENT



IT
ASSETS



CYBER
BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
IDENTIFICACIÓN (ID)	Se comprenden los riesgos actuales de ciberseguridad de la organización.	
• COBIT 5 APO01.02, APO02.02, APO03.03, APO03.04, BAI09.01, BAI09.02, BAI09.05, DSS06.03 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(a)(7)(ii)(E), 164.308(b), 164.310(a)(2)(ii), 164.310(d) 164.314(a)(1), 164.314(a)(2)(i)(B), 164.314(a)(2)(ii), 164.316(b)(2) • RGPD Art. 35-39	ID.AM-02: Se mantienen inventarios de software, servicios y sistemas gestionados por la organización ID.AM-03: Se mantienen representaciones de la comunicación autorizada en la red de la organización y de los flujos de datos internos y externos de la red ID.AM-04: Se mantienen inventarios de los servicios prestados por los proveedores ID.AM-05: Los activos se priorizan según la clasificación, la criticidad, los recursos y el impacto en la misión ID.AM-07: Se mantienen inventarios de datos y metadatos correspondientes para los tipos de datos designados ID.AM-08: Sistemas, hardware, software, servicios y datos se gestionan a lo largo de sus ciclos de vida	
Evaluación de Riesgos (ID.RA) • NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, PM-4, PM-9, PM-11, PM-12, PM-16, RA-2, RA-3, RA-5, SA-5, SA-11, SA-14, SI-2, SI-4, SI-5 • NIST SP 800-171 Rev. 2: CM 3.4.1; SA 3.12.1 – 3.12.4; AT 3.2.1 – 3.2.2 • ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 • ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • CCS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO13.02, DSS04.02 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(iii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.308(a)(a)(6), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(a), 164.316(b)(2)(iii), 164.312(c), 164.312(e), 164.314, 164.316 • RGPD Art. 28 (1-4); Art. 29; Art. 32 (1-4); Art. 35 (1-6); Art. 77 80; 82-83	El riesgo de ciberseguridad para la organización, los activos y las personas es comprendido por la organización. ID.RA-01: Se identifican, validan y registran vulnerabilidades en los activos. ID.RA-02: La inteligencia sobre amenazas cibernéticas se recibe de foros y fuentes de intercambio de información. ID.RA-03: Se identifican y registran amenazas internas y externas a la organización. ID.RA-04: Se identifican y registran los posibles impactos y probabilidades de amenazas que explotan vulnerabilidades. ID.RA-05: Se utilizan amenazas, vulnerabilidades, probabilidades e impactos para comprender el riesgo inherente e informar la priorización de la respuesta al riesgo. ID.RA-06: Se eligen, priorizan, planifican, rastrean y comunican las respuestas al riesgo. ID.RA-07: Se gestionan, evalúan el impacto en el riesgo, se registran y se registran y se rastrean los cambios y excepciones. ID.RA-08: Se establecen procesos para recibir, analizar y responder a divulgaciones de vulnerabilidades.	✓ COMPLIANCE ✓ IT ASSETS ✓ CYBER BI ✓ WORKFORCE ✓ SUPPLY CHAIN

Hablemos sobre como potenciamos la transformación digital.

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com





COMPLIANCE
MANAGEMENT



WORKFORCE
CLEARANCE



CONTRACTS
MANAGEMENT



IT
ASSETS



CYBER
BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
IDENTIFICACIÓN (ID)	Se comprenden los riesgos actuales de ciberseguridad de la organización.	
	ID.RA-09: Se evalúa la autenticidad e integridad del hardware y el software antes de la adquisición y uso. ID.RA-10: Se evalúan los proveedores críticos antes de la adquisición.	
Mejora (ID.IM) • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • NIST SP 800-171 Rev. 2: IR 3.6.1, 3.6.3 • ISO/IEC 27001:2013 A.16.1.6 • ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 • COBIT 5 BAI01.13 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii) • RGPD Art. 32 (1.d) (2)	Se identifican mejoras en los procesos, procedimientos y actividades de gestión de riesgos de ciberseguridad organizacional en todas las funciones del CSF. ID.IM-01: Se identifican mejoras a partir de las evaluaciones. ID.IM-02: Se identifican mejoras a partir de pruebas y ejercicios de seguridad, incluyendo aquellos realizados en coordinación con proveedores y terceros relevantes. ID.IM-03: Se identifican mejoras a partir de la ejecución de procesos, procedimientos y actividades operativas. ID.IM-04: Se establecen, comunican, mantienen y mejoran los planes de respuesta a incidentes y otros planes de ciberseguridad que afectan a las operaciones.	✓ COMPLIANCE ✓ IT ASSETS ✓ CYBER BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
PROTECT (PR)	Se utilizan salvaguardas para gestionar los riesgos de ciberseguridad de la organización.	
Gestión de Identidad, Autenticación y Control de Acceso (PR. AA) • NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16, AC-17, AC-19, AC-20, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9, IA Familia • NIST SP 800-171 Rev. 2: AC 3.1.1, 3.1.2, 3.1.5; CM 3.4.1, 3.4.6; MP 3.8.1-3.8.2, 3.8.5, 3.8.8; PP 3.10.1-3.10.5; PS 3.9.1 – 3.9.2; IA 3.5.1- 3.5.2 • ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.6.6, 4.3.3.7.3, 4.3.3.3.8, 4.3.3.5.1 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.13, SR 2.1, SR 2.6 • ISO/IEC 27001:2013 A.6.1.2, A.6.2.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.3.1, A.9.4.1,	El acceso a activos físicos y lógicos está limitado a usuarios autorizados, servicios y hardware, y se gestiona de acuerdo con el riesgo evaluado de acceso no autorizado. PR. AA-01: Las identidades y credenciales de usuarios, servicios y hardware autorizados son gestionados por la organización. PR. AA-02: Las identidades se revisan y vinculan a las credenciales según el contexto de las interacciones. PR. AA-03: Usuarios, servicios y hardware están autenticados PR. AA-04: Las afirmaciones de identidad están protegidas, transmitidas y verificadas.	✓ IT ASSETS ✓ CYBER BI ✓ WORKFORCE ✓ PROPERTY

Hablemos sobre como potenciamos la transformación digital.

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com





COMPLIANCE
MANAGEMENT



WORKFORCE
CLEARANCE



CONTRACTS
MANAGEMENT



IT
ASSETS



CYBER
BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
PROTECT (PR)	Se utilizan salvaguardas para gestionar los riesgos de ciberseguridad de la organización.	
A.9.4.2, A.9.4.3, A.9.4.4, A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.13.1.1, A.13.2.1 • CCS CSC 12, 15, 16 • COBIT 5 APO13.01, DSS01.04, DSS05.04, DSS06.03, DSS05.05 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(b)(1), 164.308(b)(3), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d), 164.312(e)(1), 164.312(e)(2)(ii) • RGPD Art. 5(1) (a-f); Art. 25 (1-3); Art. 89 (1-4);	PR. AA-05: Los permisos de acceso, derechos y autorizaciones se definen en una política, se gestionan, hacen cumplir y revisan, e incorporan los principios de privilegio mínimo y separación de funciones. PR. AA-06: El acceso físico a los activos se gestiona, supervisa y se hace cumplir en función del riesgo.	
Concienciación y Formación (PR. AT) • NIST SP 800-53 Rev. 4 AT-2, AT-3, PM-13, PS-7, SA-9 • NIST SP 800-171 Rev. 2: AT 3.2.1 - 3.2.3 • ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • COBIT 5 APO07.02, APO07.03, APO10.04, APO10.05, BAI05.07, DSS06.03 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5), 164.308(b), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii), 164.530(b)(1) • RGPD Art. 28 (1-4); Art. 29; Art. 32 (3-4)	El personal de la organización recibe formación y concienciación en ciberseguridad para que puedan realizar sus tareas relacionadas con la ciberseguridad. PR. AT-01: Se proporciona al personal la concienciación y formación para que posean los conocimientos y habilidades necesarios para realizar tareas generales teniendo en cuenta los riesgos de ciberseguridad. PR. AT-02: A las personas en roles especializados se les proporciona concienciación y formación para que posean los conocimientos y habilidades necesarios para realizar tareas relevantes teniendo en cuenta los riesgos de ciberseguridad.	✓ WORKFORCE ✓ E-LEARNING
Seguridad de Datos (PR.DS) • NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16 • NIST SP 800-171 Rev. 2: AT 3.2.1; AC 3.1.1, 3.1.2, 3.1.4-3.1.6; CM 3.4.1; MP 3.8.1-3.8.3, 3.8.5, 3.8.8 • ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 • ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 • ISA 62443-3-3:2013 SR 4.2 • COBIT 5 BAI09.03 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2) • RGPD Art. 5 (1-2); Art. 32 (1) (a-b); 32(2); Art. 42-44; Art. 45 (1-8); Art. 46 (1-5)	Los datos se gestionan de acuerdo con la estrategia de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de la información. PR. DS-01: La confidencialidad, integridad y disponibilidad de los datos en reposo están protegidas. PR. DS-02: Se protege la confidencialidad, integridad y disponibilidad de los datos en tránsito. PR. DS-10: Se protege la confidencialidad, integridad y disponibilidad de los datos en uso. PR. DS-11: Se crean, protegen, mantienen y prueban copias de seguridad de los datos.	✓ IT ASSETS ✓ CYBER BI
Seguridad de Plataforma (PR.PS)	El hardware, software (por ejemplo, firmware, sistemas operativos, aplicaciones) y servicios de plataformas físicas y virtuales se gestionan de acuerdo con la	✓ IT ASSETS ✓ CYBER BI

Hablemos sobre como potenciamos la transformación digital.

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com





COMPLIANCE
MANAGEMENT



WORKFORCE
CLEARANCE



CONTRACTS
MANAGEMENT



IT
ASSETS



CYBER
BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
PROTECT (PR)	Se utilizan salvaguardas para gestionar los riesgos de ciberseguridad de la organización.	
• NIST SP 800-53 Rev. 4 Familia UA, AC-3, AC-4, AC-17, AC-18, CM-7, CP-8, MP-2, MP-4, MP-5, MP-7, SC-7 • CCS CSC 14 • NIST SP 800-171 Rev. 2: AC 3.1.1-3.1.2, 3.1.8; EN 3.2.1; MP 3.8.4-3.8.6, 3.8.8; SA 3.12.4; AA 3.3.3-3.3.7; PP 3.10.4 - 3.10.5; • ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.1.2, A.11.2.9, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, A.13.1.1, A.13.2.1 • ISA 62443-2-1:2009 4.009 3.3.3.9, 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • COBIT 5 APO11.04, APO13.01, DSS05.02 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(C), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv), 164.312(b) • RGPD Art. 25 (1-3); Art. 30 (1-5); Art. 42-44; Art. 45 (1-8); Art. 46 (1-5)	estrategia de riesgos de la organización para proteger su confidencialidad, integridad y disponibilidad. PR. PS-01: Se establecen y aplican las prácticas de gestión de configuración. PR. PS-02: El software se mantiene, reemplaza y elimina en función del riesgo. PR. PS-03: El hardware se mantiene, reemplaza y elimina en función del riesgo. PR. PS-04: Se generan registros de registro y se ponen a disposición para monitorización continua. PR. PS-05: Se impide la instalación y ejecución de software no autorizado. PR. PS-06: Las prácticas seguras de desarrollo de software se integran y su rendimiento se supervisa a lo largo del ciclo de vida del desarrollo de software.	
Resiliencia de la infraestructura tecnológica (PR. IR)	Las arquitecturas de seguridad se gestionan con la estrategia de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de los activos, así como la resiliencia organizativa.	✓ IT ASSETS ✓ CYBER BI
• NIST SP 800-53 Rev. 4 Familia UA, AC-3, AC-4, AC-17, AC-18, CM-7, CP-8, MP-2, MP-4, MP-5, MP-7, SC-7 • CCS CSC 14 • NIST SP 800-171 Rev. 2: AC 3.1.1-3.1.2, 3.1.8; EN 3.2.1; MP 3.8.4-3.8.6, 3.8.8; SA 3.12.4; AA 3.3.3-3.3.7; PP 3.10.4 - 3.10.5; • ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.1.2, A.11.2.9, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, A.13.1.1, A.13.2.1 • ISA 62443-2-1:2009 4.009 3.3.3.9, 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR	PR. IR-01: Las redes y entornos están protegidos contra accesos y usos lógicos no autorizados. PR. IR-02: Los activos tecnológicos de la organización están protegidos frente a amenazas medioambientales. PR. IR-03: Se implementan mecanismos para alcanzar los requisitos de resiliencia en situaciones normales y adversas. PR. IR-04: Capacidad adecuada de recursos para garantizar la disponibilidad.	

Hablemos sobre como potenciamos la transformación digital.

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com





COMPLIANCE
MANAGEMENT



WORKFORCE
CLEARANCE



CONTRACTS
MANAGEMENT



IT
ASSETS



CYBER
BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
PROTECT (PR)	Se utilizan salvaguardas para gestionar los riesgos de ciberseguridad de la organización.	
2.4, SR 2.5, SR 2.6, SR 2.7, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • COBIT 5 APO11.04, APO13.01, DSS05.02 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(C), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 164.312(b) • RGPD Art. 25 (1-3); Art. 30 (1-5); Art. 42-44; Art. 45 (1-8); Art. 46 (1-5);		

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
DETECTAR (DE)	Se detectan y analizan posibles ataques y compromisos de ciberseguridad.	
Monitorización Continua (DE. CM) • NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-3, CM-8, CM-10, CM-11, PE-3, PE-6, PE-20, SI-4 • NIST SP 800-171 Rev. 2: AA 3.3.3-3.3.6 • ISA 62443-3-3:2013 SR 6.2 • ISO/IEC 27001:2013 A.12.4.1 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e) • RGPD Art. 32 (1.b)	Se monitorizan los activos para detectar anomalías, indicadores de compromiso y otros eventos potencialmente adversos. DE. CM-01: Se monitorizan las redes y los servicios de red para detectar posibles eventos adversos. DE. CM-02: Se monitoriza el entorno físico para detectar posibles eventos adversos. DE. CM-03: Se monitoriza la actividad del personal y el uso de tecnología para detectar posibles eventos adversos. DE. CM-06: Se monitorizan las actividades y servicios de los proveedores externos para detectar posibles eventos adversos. DE. CM-09: Se monitorizan el hardware y software informático, los entornos de ejecución y sus datos para detectar posibles eventos adversos.	✓ IT ASSETS ✓ CYBER BI
Análisis de Eventos Adversos (DE. AE) • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, RA-3, SI-4 • NIST SP 800-171 Rev. 2: AA 3.3.3-3.3.6; AC 3.1.2-3.2.5 • ISA 62443-2-1:2009 4.2.3.10 • ISA 62443-3-3:2013 SR 6.1	Se analizan anomalías, indicadores de compromiso y otros eventos potencialmente adversos para caracterizar los eventos y detectar incidentes de ciberseguridad. DE. AE-02: Se analizan los posibles eventos adversos para comprender mejor las actividades asociadas. DE. AE-03: La información está correlacionada de múltiples fuentes.	✓ COMPLIANCE ✓ IT ASSETS ✓ CYBER BI

Hablemos sobre como potenciamos la transformación digital.

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com





COMPLIANCE
MANAGEMENT



WORKFORCE
CLEARANCE



CONTRACTS
MANAGEMENT



IT
ASSETS



CYBER
BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
DETECTAR (DE)	Se detectan y analizan posibles ataques y compromisos de ciberseguridad.	
• COBIT 5 APO12.06 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(i), 164.308(a)(6)(ii), 164.308(a)(8), 164.310(d)(2)(iii), 164.312(b), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii) • RGPD Art. 32 (2); Art. 35 (1-2)	DE. AE-04: Se entiende el impacto estimado y el alcance de los eventos adversos. DE. AE-06: Se proporciona información sobre eventos adversos al personal y herramientas autorizados. DE. AE-07: La inteligencia sobre amenazas cibernéticas y otra información contextual se integran en el análisis. DE. AE-08: Los incidentes se declaran cuando los eventos adversos cumplen los criterios definidos de incidente.	

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
RESPONDER (RS)	Se toman medidas respecto a un incidente de ciberseguridad detectado.	
Gestión de Incidentes (RS. MA) • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8 • NIST SP 800-171 Rev. 2: IR 3.6.1-3.6.3 • ISO/IEC 27001:2013 A.16.1.5 • ISA 62443-2-1:2009 4.3.4.5.1 • COBIT 5 BAI01.10 • CCS CSC 18 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.312(a)(2)(ii) • RGPD Art. 32 (1.b); Art. 32 (1.d); Art. 32 (2)	Se gestionan las respuestas a incidentes de ciberseguridad detectados. RS. MA-01: El plan de respuesta a incidentes se ejecuta en coordinación con terceros relevantes una vez declarado un incidente. RS. MA-02: Los informes de incidentes se validan. RS. MA-03: Los incidentes se categorizan y priorizan RS. MA-04: Los incidentes se escalan o elevan según sea necesario RS. MA-05: Se aplican los criterios para iniciar la recuperación de incidentes	✓ COMPLIANCE ✓ IT ASSETS
Análisis de incidentes (RS. AN) • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8 • NIST SP 800-171 Rev. 2: IR 3.6.1-3.6.2 • ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E) • RGPD Art. 32 (1.d); Art. 33-34	Se realizan investigaciones para garantizar una respuesta eficaz y apoyar las actividades forenses y de recuperación. RS. AN-03: Se realiza un análisis para establecer qué ha ocurrido durante un incidente y la causa raíz del mismo. RS. AN-06: Se registran las acciones realizadas durante una investigación y se preservan la integridad y procedencia de los registros. RS. AN-07: Se recopilan los datos y metadatos de incidentes, y se preservan su integridad y procedencia. RS. AN-08: Se estima y valida la magnitud de un incidente.	✓ COMPLIANCE ✓ IT ASSETS ✓ CYBER BI
Informes y comunicación de respuesta a incidentes (RS.CO) • NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8	Las actividades de respuesta se coordinan con partes interesadas internas y externas según lo requieran las leyes, normativas o políticas.	✓ COMPLIANCE ✓ WORKFORCE

Hablemos sobre como potenciamos la transformación digital.

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com





COMPLIANCE
MANAGEMENT



WORKFORCE
CLEARANCE



CONTRACTS
MANAGEMENT



IT
ASSETS



CYBER
BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
RESPONDER (RS)	Se toman medidas respecto a un incidente de ciberseguridad detectado.	
• NIST SP 800-171 Rev. 2: IR 3.6.1-3.6.2 • ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 • ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(6)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.312(a)(2)(ii) • RGPD Art. 33-34; 37-38	RS. CO-02: Se notifica a los interesados internos y externos de los incidentes. RS. CO-03: La información se comparte con partes interesadas internas y externas designadas.	✓ SUPPLY CHAIN
Mitigación de Incidentes (RS.MI) • NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5 • NIST SP 800-171 Rev. 2: IR 3.6.1-3.6.2 • ISO/IEC 27001:2013 A.12.6.1 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii) • RGPD Art. 32 (1.d); Art. 32 (2); Art. 33-34	Se realizan actividades para evitar la expansión de un evento y mitigar sus efectos. RS. MI-01: Los incidentes están contenidos. RS. MI-02: Se erradican los incidentes.	✓ COMPLIANCE ✓ IT ASSETS ✓ CYBER BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
RECOVER (RC)	Se restauran los activos y operaciones afectados por un incidente de ciberseguridad.	
Ejecución del Plan de Recuperación de Incidentes (RC. RP) • NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8 • NIST SP 800-171 Rev. 2: IR 3.6.1 - 3.6.2; AT 3.2.2 • ISO/IEC 27001:2013 A.16.1.5 • CCS CSC 8 • COBIT 5 DSS02.05, DSS03.04 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(7), 164.310(a)(2)(i) • RGPD Art. 32 (1.c);	Se realizan actividades de restauración para garantizar la disponibilidad operativa de los sistemas y servicios afectados por incidentes de ciberseguridad. RC. RP-01: La parte de recuperación del plan de respuesta a incidentes se ejecuta una vez iniciada desde el proceso de respuesta a incidentes. RC. RP-02: Las acciones de recuperación se seleccionan, alcanzan, priorizan y se realizan. RC. RP-03: Se verifica la integridad de las copias de seguridad y otros activos de restauración antes de usarlos para restauración. RC. RP-04: Las funciones críticas de la misión y la gestión de riesgos de ciberseguridad se consideran para establecer normas operativas post-incidentes. RC. RP-05: Se verifica la integridad de los activos restaurados, se restauran los sistemas y servicios, y se confirma el estado operativo normal. RC. RP-06: Se declara el fin de la recuperación de incidentes según criterios y se completa la documentación relacionada con el incidente.	✓ COMPLIANCE ✓ IT ASSETS ✓ SUPPLY CHAIN

Hablemos sobre como potenciamos la transformación digital.

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com





COMPLIANCE
MANAGEMENT



WORKFORCE
CLEARANCE



CONTRACTS
MANAGEMENT



IT
ASSETS



CYBER
BI

MARCO NORMATIVO DE CIBERSEGURIDAD INTERNACIONAL FUNCIONES DE NIST CSF 2.0		SC365 [®] SOLUCIONES
RECOVER (RC)	Se restauran los activos y operaciones afectados por un incidente de ciberseguridad.	
Comunicación de Recuperación de Incidentes (RC.CO) • NIST SP 800-53 Rev. 4 CP-2, IR-4 • NIST SP 800-171 Rev. 2: IR 3.6.1 – 3.6.2 • Regla de Seguridad HIPAA 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(ii)(B), 164.308(a)(7)(iii)(C), 164.310(a)(2)(i), 164.314(a)(2)(i)(C) • RGPD Art. 32 (1.c);	Las actividades de restauración se coordinan con partes internas y externas. RC. CO-03: Las actividades de recuperación y el progreso en la restauración de capacidades operativas se comunican a los interesados internos y externos designados. RC. CO-04: Las actualizaciones públicas sobre la recuperación de incidentes se comparten utilizando métodos y mensajes aprobados.	✓ COMPLIANCE ✓ WORKFORCE ✓ SUPPLY CHAIN

Hablemos sobre como potenciamos la transformación digital.

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com

