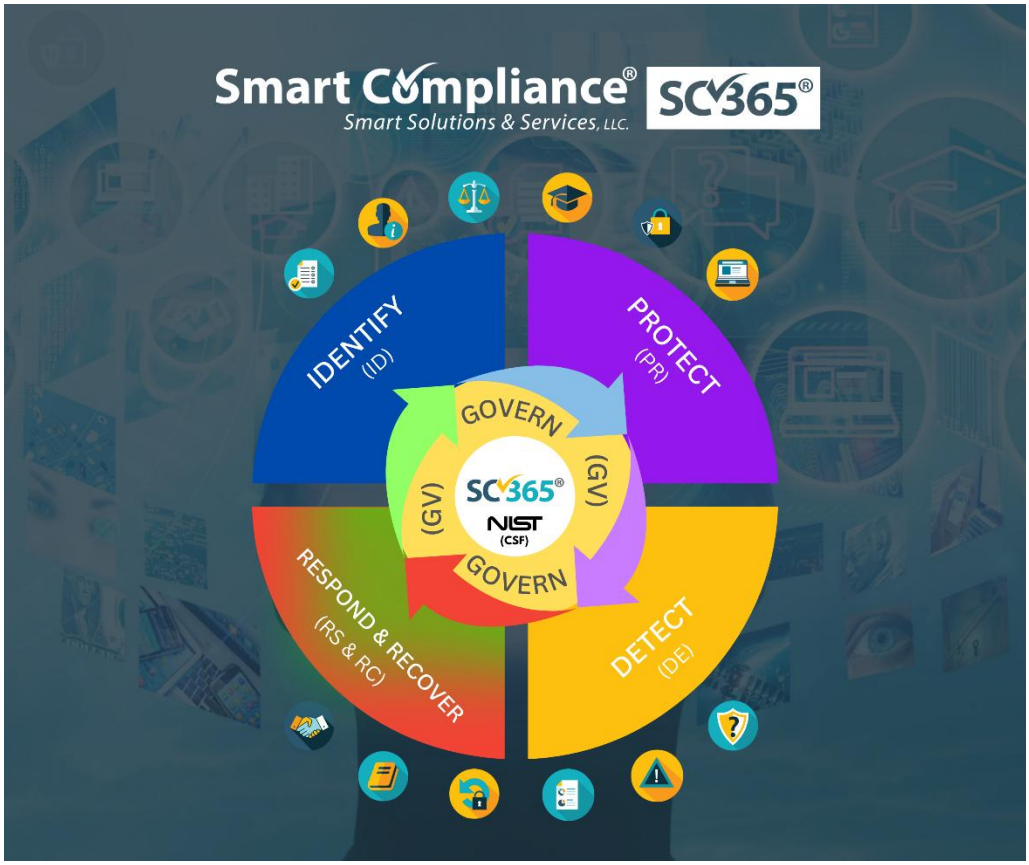
Smart Compliance®
Smart Solutions & Services, LLC.
SC365®

SC365® SOLUTIONS

COMPLIANCE MANAGEMENT
WORKFORCE CLEARANCE
CONTRACTS MANAGEMENT
IT ASSETS
CYBER BI

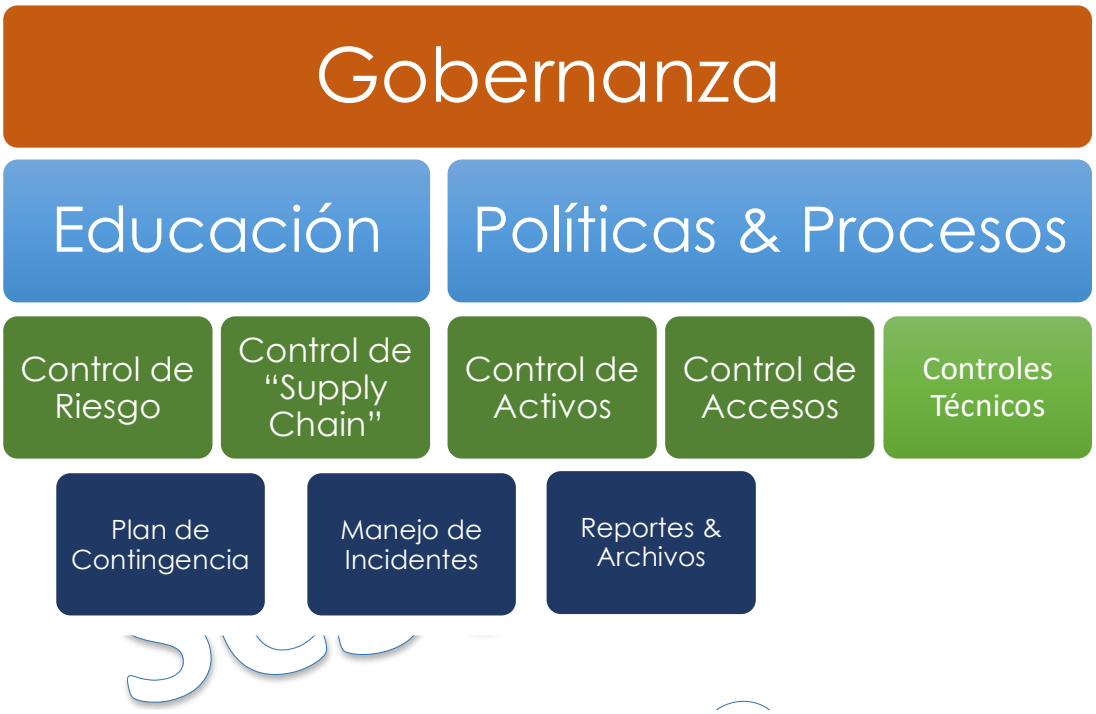
Soluciones Integradas de Ciberseguridad

Marco de ciberseguridad con controles administrativos, físicos, y técnicos.



Marco de Ciberseguridad

Programa de Gobernanza y Control de Riesgo holístico y confiable.



Póliza de Seguro Cibernético

Demuestre diligencia para garantizar su cobertura en un evento cibernético.

- **Multifactor authentication for remote access and admin/privileged controls**
- **Endpoint Detection and Response (EDR)**
- **Secured, encrypted, and tested backups**
- **Privileged Access Management (PAM)**
- **Email filtering and web security**
- Patch management and vulnerability management
- Cyber incident response planning and testing
- Cybersecurity awareness training and phishing testing
- Hardening techniques, including Remote Desktop Protocol (RDP) mitigation
- Logging and monitoring/network protections
- End-of-life systems replaced or protected
- Vendor/digital supply chain risk management

REGLAS INTERNACIONALES DE SEGURIDAD ALINEADAS AL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 / NIS2		SC365® SOLUCIONES
GOBERNANZA (GV)	**La estrategia, las expectativas y la política de gestión de riesgos de ciberseguridad de la organización se establecen, comunican y monitorean.**	
Contexto Organizacional (GV.OC) • ***NIST SP 800-53*** *Rev. 4 CP-2, CP-8, CP-11, PE-9, PE-11, PM-8, 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 de 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) ; Apartado a) a g) del párrafo 2 del Art. 14; 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 las partes interesadas, dependencias y requisitos legales, reglamentarios y contractuales) que rodean las decisiones de gestión de riesgos de ciberseguridad de la organización** GV. OC-01: Se entiende la misión organizacional e informa la gestión de riesgos de ciberseguridad GV. OC-02: Se comprenden las partes interesadas internas y externas, y se comprenden y consideran sus necesidades y expectativas con respecto a la gestión de riesgos de ciberseguridad GV. OC-03: Se comprenden y gestionan los requisitos legales, reglamentarios y contractuales relacionados con 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 las partes interesadas externas GV. OC-05: Se comprenden y comunican los resultados, capacidades y servicios de los que depende la organización	✓ Compliance ✓ Contracts
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; EN 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 de 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) (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); Arts. 77 a 80; 82-83*	**Las prioridades, restricciones, declaraciones de tolerancia al riesgo y apetito de la organización, y los supuestos se establecen, comunican y utilizan para respaldar las decisiones de riesgo operativo** GV. RM-01: Los objetivos de gestión de riesgos son establecidos y acordados por las partes interesadas de la organización GV. RM-02: Se establecen, comunican y mantienen las declaraciones de apetito y tolerancia al riesgo GV. RM-03: Las actividades y los resultados de la gestión de riesgos de ciberseguridad se incluyen en los procesos de gestión de riesgos empresariales GV. RM-04: Se establece y comunica la dirección estratégica que describe las opciones apropiadas 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 los proveedores y otros terceros GV. RM-06: Se establece y comunica un método estandarizado para calcular, documentar, categorizar y priorizar los riesgos de ciberseguridad	✓ Compliance ✓ IT Assets ✓ Cyber BI ✓ Workforce ✓ Contracts ✓ Property

REGLAS INTERNACIONALES DE SEGURIDAD ALINEADAS AL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 / NIS2		SC365® SOLUCIONES
GOBERNANZA (GV)	**La estrategia, las expectativas y la política de gestión de riesgos de ciberseguridad de la organización se establecen, comunican y monitorean.**	
	GV. RM-07: Las oportunidades estratégicas (es decir, los riesgos positivos) se caracterizan y se incluyen en las discusiones sobre riesgos de ciberseguridad de la organización	
Funciones, responsabilidades y autoridades (GV. RR) • ***NIST SP 800-53*** *Rev. 4 controles de todas las familias* • ***NIST SP 800-171*** *Rev. 2: EN 3.2.1, 3.2.3; RA 3.11.1; RI 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 de HIPAA*** *45 CFR §§ 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 ; Párrafos 1 a 4 del Art. 15; Art. 28 (1-4); Art. 29; Art. 32 (3-4); Art. 33 (1-5); Párrafos 1 a 4 del Art. 34; Art. 37 (1-7); Art. 38 (1-6); Art. 39 (1-2); Art. 40 (1-11); Arts. 64 a 66; Arts. 84 a 86*	**Se establecen y comunican funciones, responsabilidades y autoridades de ciberseguridad para fomentar la rendición de cuentas, la evaluación del desempeño y la mejora continua** GV. RR-01: El liderazgo organizacional es responsable del riesgo de ciberseguridad y fomenta una cultura consciente del riesgo, ética y que mejora continuamente GV. RR-02: Se establecen, comunican, comprenden y aplican las funciones, responsabilidades y autoridades relacionadas con la gestión de riesgos de ciberseguridad GV. RR-03: Se asignan recursos adecuados acordes con la estrategia, las funciones, las responsabilidades y las políticas de riesgo de ciberseguridad GV. RR-04: La ciberseguridad está incluida en las prácticas de recursos humanos	✓ Compliance ✓ IT Assets ✓ Workforce ✓ Contracts
Política (GV. PO) • ***NIST SP 800-53*** *Rev. 4 controles de todas las familias* • ***NIST SP 800-171*** *Rev. 2: EN 3.2.1, 3.2.3; RA 3.11.1; RI 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 de HIPAA*** *45 CFR §§ 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; Párrafos 1 a 4 del Art. 15; Art. 28 (1-4); Art. 29; Art. 32 (3-4)); Art.33 (1-5); Párrafos 1 a 4 del Art. 34; Art. 37 (1-7); Art. 38 (1-6); Art. 39 (1-2); Art. 40 (1-11); Arts. 64 a 66; Arts. 84 a 86*	**Se establece, comunica y aplica la política de ciberseguridad de la organización** GV. PO-01: La política para la gestión de riesgos de ciberseguridad se establece en función del contexto organizacional, la estrategia y las prioridades de ciberseguridad y se comunica y aplica GV. PO-02: La política para gestionar los riesgos de ciberseguridad se revisa, actualiza, comunica y aplica para reflejar los cambios en los requisitos, las amenazas, la tecnología y la misión de la organización	✓ Compliance ✓ IT Assets

REGLAS INTERNACIONALES DE SEGURIDAD ALINEADAS AL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 / NIS2		SC365® SOLUCIONES
GOBERNANZA (GV)	**La estrategia, las expectativas y la política de gestión de riesgos de ciberseguridad de la organización se establecen, comunican y monitorean.**	
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; EN 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 de 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) (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); Arts. 77 a 80; 82-83*	**Los resultados de las actividades y el rendimiento de la gestión de riesgos de ciberseguridad en toda la organización 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 de ciberseguridad para informar y ajustar la estrategia y la dirección GV. OV-02: Se revisa y ajusta la estrategia de gestión de riesgos de ciberseguridad para garantizar la cobertura de los requisitos y riesgos de la organización GV. OV-03: El desempeño de la gestión de riesgos de ciberseguridad organizacional se evalúa y revisa para los ajustes necesarios	✓ Compliance ✓ IT Assets ✓ Cyber BI ✓ Workforce ✓ Contracts ✓ Property

REGLAS INTERNACIONALES DE SEGURIDAD ALINEADAS AL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 / NIS2		SC365® SOLUCIONES
GOBERNANZA (GV)	**La estrategia, las expectativas y la política de gestión de riesgos de ciberseguridad de la organización se establecen, comunican y monitorean.**	
Gestión de riesgos de la cadena de suministro de ciberseguridad (GV. SC) • ***NIST SP 800-53*** *Rev. 4 CP-2, CP-8, CP-11, PE-9, PE-11, PM-8, 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 de 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);(a) a g) del párrafo 2 del Art. 14; Art. 28 (1-4); Artí29; Art. 37 (1-7); Art. 38 (1-6); Art. 39 (1-2); Art. 40 (1-11)*	**Los procesos de gestión de riesgos de la cadena de suministro cibernética son identificados, establecidos, administrados, monitoreados y mejorados por las partes interesadas de la organización** GV. SC-01: Las partes interesadas de la organización establecen y acuerdan un programa, estrategia, objetivos, políticas y procesos de gestión de riesgos de la cadena de suministro de ciberseguridad GV. CE-02: Se establecen, comunican y coordinan interna y externamente las funciones y responsabilidades de ciberseguridad para proveedores, clientes y socios GV. CE-03: La gestión de riesgos de la cadena de suministro de ciberseguridad se integra en la ciberseguridad y la gestión de riesgos empresariales, la evaluación de riesgos y los procesos de mejora GV. SC-04: Los proveedores son conocidos y priorizados por criticidad GV. CE-05: Se establecen, priorizan e integran 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. CE-06: La planificación y la debida diligencia se realizan para reducir los riesgos antes de establecer relaciones formales con proveedores u otros terceros GV. CE-07: Los riesgos planteados por un proveedor, sus productos y servicios, y otros terceros se entienden, registran, priorizan, evalúan, responden y monitorean 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. CE-09: Las prácticas de seguridad de la cadena de suministro se integran en los 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 de la cadena de suministro de ciberseguridad incluyen disposiciones para las actividades que ocurren después de la conclusión de un acuerdo de asociación o servicio	✓ Contracts ✓ Workforce

REGLAS INTERNACIONALES DE SEGURIDAD ALINEADAS AL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 / NIS2		SC365® SOLUCIONES
IDENTIFICAR (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*** • ***COBIT 5*** *APO01.02, APO02.02, APO03.03, APO03.04, BAI09.01, BAI09.02, BAI09.05, DSS06.03* • ***Regla de Seguridad de 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*** *Arts. 35-39*	**Los activos (por ejemplo, datos, hardware, software, sistemas, instalaciones, servicios, personas) que permiten a la organización lograr los propósitos comerciales se identifican y administran de acuerdo con su importancia relativa para los objetivos organizacionales y la estrategia de riesgo de la organización** ID.AM-01: Se mantienen los inventarios de hardware gestionado por la organización ID.AM-02: Se mantienen inventarios de software, servicios y sistemas administrados por la organización ID.AM-03: Se mantienen las representaciones de la comunicación de red autorizada de la organización y los flujos de datos de red internos y externos ID.AM-04: Se mantienen inventarios de servicios prestados por proveedores ID.AM-05: Los activos se priorizan en función de la clasificación, la criticidad, los recursos y el impacto en la misión ID.AM-07: Se mantienen los inventarios de datos y los metadatos correspondientes para los tipos de datos designados ID.AM-08: Los sistemas, el hardware, el software, los servicios y los datos se gestionan a lo largo de sus ciclos de vida	✓ IT Assets ✓ Cyber BI
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; EN 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 de 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*	**La organización comprende el riesgo de ciberseguridad para la organización, los activos y las personas** ID.RA-01: Se identifican, validan y registran las vulnerabilidades en los activos ID.RA-02: La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información ID.RA-03: Se identifican y registran las amenazas internas y externas a la organización ID.RA-04: Se identifican y registran los posibles impactos y probabilidades de las amenazas que explotan las vulnerabilidades ID.RA-05: Las amenazas, vulnerabilidades, probabilidades e impactos se utilizan para comprender el riesgo	✓ Compliance ✓ IT Assets ✓ Cyber BI ✓ Contracts

REGLAS INTERNACIONALES DE SEGURIDAD ALINEADAS AL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 / NIS2		SC365® SOLUCIONES
IDENTIFICAR (ID)	**Se comprenden los riesgos actuales de ciberseguridad de la organización**	
(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); Arts. 77 a 80; 82-83*	inherente e informar la priorización de la respuesta al riesgo ID.RA-06: Las respuestas al riesgo se eligen, priorizan, planifican, rastrean y comunican ID.RA-07: Los cambios y excepciones se gestionan, evalúan el impacto del riesgo, se registran y se rastrean ID.RA-08: Se establecen procesos para recibir, analizar y responder a la divulgación de vulnerabilidades	
	ID.RA-09: La autenticidad e integridad del hardware y el software se evalúan antes de su adquisición y uso ID.RA-10: Los proveedores críticos se evalúan 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 de 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 de la organización en todas las funciones de 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, incluidos los 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

REGLAS INTERNACIONALES DE SEGURIDAD ALINEADAS AL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 / NIS2		SC365® SOLUCIONES
PROTEGER (PR)	**Se utilizan salvaguardas para gestionar los riesgos de ciberseguridad de la organización**	
Gestión de identidades, 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; PÁGS. 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, 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 de 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 (b), 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);*	**El acceso a los activos físicos y lógicos se limita a los usuarios, servicios y hardware autorizados y se administra de acuerdo con el riesgo evaluado de acceso no autorizado** PR. AA-01: La organización administra las identidades y credenciales de los usuarios, servicios y hardware autorizados PR. AA-02: Las identidades se prueban y se vinculan a las credenciales en función del contexto de las interacciones PR. AA-03: Se autentican los usuarios, los servicios y el hardware PR. AA-04: Las afirmaciones de identidad están protegidas, transmitidas y verificadas PR. AA-05: Los permisos de acceso, los derechos y las autorizaciones se definen en una política, se administran, se aplican y se revisan, e incorporan los principios de privilegios mínimos y separación de funciones PR. AA-06: El acceso físico a los activos se administra, monitorea y aplica de acuerdo con el riesgo	✓ IT Assets ✓ Workforce ✓ Cyber BI ✓ Property
Sensibilización y capacitación (PR. AT) • ***NIST SP 800-53*** *Rev. 4 AT-2, AT-3, PM-13, PS-7, SA-9* • ***NIST SP 800-171*** *Rev. 2: EN 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 de 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 formación en ciberseguridad para que pueda realizar sus tareas relacionadas con la ciberseguridad** PR. AT-01: Se proporciona al personal la sensibilización y formación para que posea los conocimientos y habilidades para realizar tareas generales teniendo en cuenta los riesgos de ciberseguridad PR. AT-02: Se proporciona a las personas en roles especializados conciencia y capacitación para que posean el conocimiento y las habilidades para realizar tareas relevantes teniendo en cuenta los riesgos de ciberseguridad	✓ Workforce

REGLAS INTERNACIONALES DE SEGURIDAD ALINEADAS AL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 / NIS2		SC365® SOLUCIONES
PROTEGER (PR)	**Se utilizan salvaguardas para gestionar los riesgos de ciberseguridad de la organización**	
Seguridad de datos (PR.DS) • ***NIST SP 800-53*** *Rev. 4 CM-8, MP-6, PE-16* • ***NIST SP 800-171*** *Rev. 2: EN 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 y 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 de 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); Apartados a) a b) del párrafo 1 del Art. 32; 32(2); Art. 42-44; Art. 45 (1-8); Art. 46 (1-5);*	**Los datos se gestionan de acuerdo con la estrategia de riesgo 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: La confidencialidad, integridad y disponibilidad de los datos en tránsito están protegidas PR. DS-10: La confidencialidad, integridad y disponibilidad de los datos en uso están protegidas PR. DS-11: Se crean, protegen, mantienen y prueban copias de seguridad de datos	✓ IT Assets ✓ Cyber BI
Seguridad de la plataforma (PR.PS) • ***NIST SP 800-53*** *Rev. 4 Familia AU, 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; PÁGS. 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*** *4.3.3.3.9, 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, 4.3.3.6.9, 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 de 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)*	**El hardware, el software (por ejemplo, firmware, sistemas operativos, aplicaciones) y los servicios de las plataformas físicas y virtuales se gestionan de acuerdo con la estrategia de riesgo de la organización para proteger su confidencialidad, integridad y disponibilidad** PR. PS-01: Se establecen y aplican las prácticas de gestión de la configuración PR. PS-02: El software se mantiene, reemplaza y elimina de acuerdo con el riesgo PR. PS-03: El hardware se mantiene, reemplaza y retira de acuerdo con el riesgo PR. PS-04: Se generan registros y se ponen a disposición para su supervisión continua PR. PS-05: Se evita la instalación y ejecución de software no autorizado PR. PS-06: Se integran prácticas seguras de desarrollo de software y se monitorea su desempeño a lo largo del ciclo de vida del desarrollo de software	✓ IT Assets ✓ Cyber BI

REGLAS INTERNACIONALES DE SEGURIDAD ALINEADAS AL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 / NIS2		SC365® SOLUCIONES
PROTEGER (PR)	**Se utilizan salvaguardas para gestionar los riesgos de ciberseguridad de la organización**	
Resiliencia de la infraestructura tecnológica (PR. IR) • ***NIST SP 800-53*** *Rev. 4 Familia AU, 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; PÁGS. 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*** *4.3.3.3.9, 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, 4.3.3.6.9, 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 de 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);*	**Las arquitecturas de seguridad se gestionan con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de los activos, y la resiliencia de la organización** PR. IR-01: Las redes y los entornos están protegidos contra el acceso y el uso lógicos no autorizados PR. IR-02: Los activos tecnológicos de la organización están protegidos de las amenazas ambientales PR. IR-03: Se implementan mecanismos para lograr los requisitos de resiliencia en situaciones normales y adversas PR. IR-04: Capacidad de recursos adecuada para garantizar que se mantenga la disponibilidad	✓ IT Assets ✓ Cyber BI

REGLAS INTERNACIONALES DE SEGURIDAD ALINEADAS AL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 / NIS2		SC365® SOLUCIONES
DETECTAR (DE)	**Se encuentran y analizan posibles ataques y compromisos de ciberseguridad**	
Monitoreo continuo (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 de 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)*	**Los activos se monitorean para encontrar anomalías, indicadores de compromiso y otros eventos potencialmente adversos** DE. CM-01: Las redes y los servicios de red se monitorean para encontrar eventos potencialmente adversos DE. CM-02: Se monitorea el entorno físico para encontrar eventos potencialmente adversos DE. CM-03: Se monitorea la actividad del personal y el uso de la tecnología para encontrar eventos potencialmente adversos DE. CM-06: Se monitorean las actividades y servicios de los proveedores de servicios externos para encontrar eventos potencialmente adversos DE. CM-09: El hardware y el software informáticos, los entornos de tiempo de ejecución y sus datos se monitorean para encontrar eventos potencialmente 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* • ***COBIT 5*** *APO12.06* • ***Regla de Seguridad de 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)*	**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 eventos potencialmente adversos para comprender mejor las actividades asociadas DE. AE-03: La información se correlaciona de múltiples fuentes DE. AE-04: Se comprenden el impacto estimado y el alcance de los eventos adversos DE. AE-06: Se proporciona información sobre eventos adversos al personal y las herramientas autorizadas DE. AE-07: La inteligencia de amenazas cibernéticas y otra información contextual se integran en el análisis DE. AE-08: Los incidentes se declaran cuando los eventos adversos cumplen con los criterios de incidentes definidos	✓ Compliance ✓ IT Assets ✓ Cyber BI

REGLAS INTERNACIONALES DE SEGURIDAD ALINEADAS AL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 / NIS2		SC365® SOLUCIONES
RESPONDER (RS)	**Se toman medidas con 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 de 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)* • *Art. 32 (1.b) del RGPD; Art. 32 (1.d); Art. 32 (2)*	**Se gestionan las respuestas a los incidentes de ciberseguridad detectados** RS. MA-01: El plan de respuesta a incidentes se ejecuta en coordinación con terceros relevantes una vez que se declara un incidente RS. MA-02: Los informes de incidentes se clasifican y validan RS. MA-03: Se categorizan y priorizan los incidentes 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 ✓ Incidente
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 de 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); Arts. 33 y 34*	**Las investigaciones se llevan a cabo para garantizar una respuesta eficaz y apoyar las actividades forenses y de recuperación** RS. AN-03: Se realiza un análisis para establecer lo que ha ocurrido durante un incidente y la causa raíz del incidente RS. AN-06: Se registran las acciones realizadas durante una investigación y se preserva la integridad y procedencia de los registros RS. AN-07: Se recopilan datos y metadatos de incidentes, y se preserva 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* • ***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 de 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*** *Arts. 33-34; 37-38*	**Las actividades de respuesta se coordinan con las partes interesadas internas y externas según lo exijan las leyes, regulaciones o políticas** RS. CO-02: Se notifican las incidencias a los grupos de interés internos y externos RS. CO-03: La información se comparte con las partes interesadas internas y externas designadas	✓ Compliance ✓ Workforce ✓ Contracts
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 de 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); Párrafo 2 del Art. 32; Arts. 33 y 34*	**Las actividades se realizan 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

REGLAS INTERNACIONALES DE SEGURIDAD ALINEADAS AL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 / NIS2		SC365® SOLUCIONES
RECUPERAR (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; EN 3.2.2* • ***ISO/IEC 27001:2013*** *A.16.1.5* • ***CCS CSC 8*** • ***COBIT 5*** *DSS02.05, DSS03.04* • ***Regla de Seguridad de HIPAA*** *45 CFR §§ 164.308 (a) (7), 164.310 (a) (2) (i)* • ***RGPD*** *Art. 32 (1.c);*	**Las actividades de restauración se realizan 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: Se seleccionan, delimitan, priorizan y realizan acciones de recuperación RC. RP-03: Se verifica la integridad de las copias de seguridad y otros activos de restauración antes de usarlos para la restauración RC. RP-04: Se considera que las funciones de misión crítica y la gestión de riesgos de ciberseguridad establecen normas operativas posteriores al incidente 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 final de la recuperación de incidentes en función de los criterios y se completa la documentación relacionada con los incidentes	✓ Compliance ✓ IT Assets ✓ Contracts
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 de HIPAA*** *45 C.F.R. §§ 164.308 (a) (6) (ii), 164.308 (a) (7) (ii) (B), 164.308 (a) (7) (ii) (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 el restablecimiento de las capacidades operativas se comunican a las partes interesadas internas y externas designadas RC. CO-04: Las actualizaciones públicas sobre la recuperación de incidentes se comparten mediante métodos y mensajes aprobados	✓ Compliance ✓ Workforce ✓ Contracts