Una Guía para Definir la Ciberseguridad Razonable

Versión 1.1

Abril 2026

CIS Center for Internet Security®

CIS Controls®

Agradecimientos

CIS desea reconocer a las siguientes personas y organizaciones por su apoyo en la creación de esta guía. Su tiempo y experiencia fueron un componente vital para completar este importante trabajo.

Autores principales

Aaron Charfoos, Paul Hastings LLP

Chris Cronin, HALOCK Security Labs

Brian de Vallance, Crosscut Consulting, LLC

Curtis Dukes, Center for Internet Security

Kirk M. Herath, CyberOhio, State of Ohio

Phyllis Lee, Center for Internet Security

Brian Ray, Leon M. and Gloria Plevin Professor of Law, Cleveland State University

Tony Sager, Center for Internet Security

Sharon Shoemaker, Center for Internet Security

Samuel A. Thumma, Phoenix, Arizona

Ira Victor, Chief Forensic Analyst, Discovery Technician

Revisores y colaboradores de la comunidad

Jennifer D. Bailey, Circuit Court Judge, Miami, FL (ret.)

Jay Billington, Center for Internet Security Shay Cleary, National Center for State Courts

Rick Doten, VP, Information Security, Healthplan CISO, Centene

Steven Fugelsang, Program Director, Cybersecurity, National Governors Association

Casey Kennedy, Director, Information Services, Texas Office of Court Administration

Robin Regnier, Center for Internet Security

Contents

SECCIÓN 1

Resumen Ejecutivo

En los Estados Unidos, no existe una norma nacional, legal ni intersectorial mínima para la seguridad de la información.[1] Ninguna ley nacional define qué se considera una seguridad razonable en casos relacionados con violaciones de datos. El gobierno federal y los gobiernos estatales cuentan con diversos estatutos, regulaciones, políticas y jurisprudencia que abarcan elementos de la ciberseguridad, como la notificación de violaciones de datos y la privacidad de los datos.

Pero todos estos esfuerzos no especifican lo que una organización debe hacer para cumplir con el estándar de ciberseguridad razonable.

El propósito de esta guía es precisamente ese.

En colaboración con expertos reconocidos en ciberseguridad técnica y en derecho, el independiente y sin fines de lucro Center for Internet Security® (CIS®) publica esta guía para brindar orientación práctica y específica a organizaciones que buscan desarrollar un programa de ciberseguridad que cumpla con el estándar general de ciberseguridad razonable. Esto, a su vez, podría ser un recurso valioso para ayudar a profesionales de ciberseguridad, asesores legales, auditores, reguladores, empresas y consumidores, así como a abogados y tribunales, a evaluar si el programa de una organización cumple con este mismo estándar cuando la vulneración de información protegida da lugar a litigios o acciones regulatorias. Un objetivo igualmente importante de la publicación de esta guía es reducir los litigios derivados de violaciones de datos. Basándose en leyes y regulaciones actualmente vigentes, esta guía identifica lo que es mínimamente adecuado, en ausencia de una ley expresa que rija las circunstancias, para protecciones de seguridad de la información acordes al riesgo y la magnitud del daño que podría resultar de una violación de datos.

Los autores de esta guía consideraron leyes federales y estatales, regulaciones existentes, diversas prácticas recomendadas de la industria y marcos de ciberseguridad, y otros recursos para derivar y proponer una metodología que determine lo que debe considerarse una ciberseguridad razonable para evitar violaciones de datos. Aunque no existe una ley integral en EE. UU. que defina la ciberseguridad razonable en todos los contextos, esta guía ofrece principios que pueden usarse para interpretar y aplicar las leyes que sí existen.

Por último, esta guía proporciona, como ejemplo, cómo un marco —los Controles de Seguridad Críticos del CIS® (CIS Controls®)[2] — puede implementarse de forma prescriptiva y de una manera que permita a todos los que usan y dependen del ecosistema tecnológico evaluar si se tomaron medidas razonables de ciberseguridad.

SECCIÓN 2

Introducción

"El responsable del tratamiento de datos deberá '[e]stablecer, implementar y mantener prácticas de seguridad de datos administrativas, técnicas y físicas razonables para proteger la confidencialidad, integridad y accesibilidad de los datos personales."

The Virginia Consumer Data Protection Act[3]

"¿Qué DIABLOS Significa Realmente la Seguridad Razonable de Datos?"

Michael Buckbee[4]

La ciberseguridad ha pasado rápidamente de ser un campo técnico especializado a formar parte del proceso principal de toma de decisiones basadas en riesgos en todas las organizaciones. Los cambios rápidos en la complejidad y conectividad también significan que las decisiones de una empresa individual pueden afectar al ecosistema en general. Por lo tanto, incluso las soluciones técnicas bien definidas deben operar en una red compleja de preocupaciones empresariales, económicas y sociales para ser efectivas.

Los marcos tradicionales de ciberseguridad han intentado poner orden a través de extensos catálogos de controles técnicos y de procesos, cada uno respaldado por una amplia variedad de procesos y certificaciones. Sin embargo, hay docenas de estos marcos, desarrollados de forma independiente con buenas intenciones en contextos específicos, y van desde voluntarios hasta obligatorios, desde descriptivos hasta prescriptivos, y desde sectoriales hasta generales.

No existe una norma nacional, legal ni intersectorial mínima sobre seguridad de la información en Estados Unidos. Ninguna ley nacional define qué se consideraría seguridad razonable en casos relacionados con violaciones de datos. Dada esta falta de un estándar nacional, los reclamos por negligencia bajo la ley común de los distintos estados se han vuelto una base frecuente de litigios relacionados con violaciones de datos. Este tipo de reclamos generalmente requieren probar que la persona u organización que causó el daño tenía una obligación legal, es decir, debía un deber de cuidado a la persona que reclama negligencia, y no cumplió con dicha obligación, es decir, no ejerció un nivel de cuidado que una persona razonable proporcionaría.

Además, todos los estados han promulgado leyes de notificación de violaciones cibernéticas. Casi el 40 % de los estados han ido más allá al promulgar leyes de privacidad de datos que exigen una ciberseguridad razonable. Y cinco estados han aprobado leyes que ayudan a definir la ciberseguridad razonable.

En este entorno complejo, el progreso requerirá la convergencia de la tecnología, la política pública y la economía. Las leyes y regulaciones

son casi unánimes en exigir que los controles de ciberseguridad sean razonables. Al considerar las leyes estatales emergentes sobre privacidad y leyes de puerto seguro, acuerdos regulatorios recientes, así como estándares de ciberseguridad de la industria existentes, esta guía propone que puede derivarse, articularse y emplearse una definición de ciberseguridad razonable utilizando conceptos existentes del derecho y la comunidad de ciberseguridad.

Esta guía también identifica que, para apoyar esta convergencia, los estándares de ciberseguridad deben tener propiedades específicas, incluyendo valor demostrado contra amenazas, ser medibles, transparentes, accesibles, prácticos y contar con el apoyo de un ecosistema de herramientas y formación. Aunque existen estudios y reportes valiosos como el "Comentario del Sedona Conference sobre una Prueba de Seguridad Razonable"[5], que muestran cómo evaluar la razonabilidad después de un incidente, esta guía describe la necesidad de establecer la razonabilidad antes de un incidente utilizando estándares específicos, prescriptivos y priorizados. Los Controles de Seguridad Críticos del CIS son uno de esos estándares y son aplicables ampliamente a las operaciones técnicas de cualquier organización. Además, los Controles del CIS están respaldados por un método complementario de evaluación de riesgos, CIS-RAM.[6] CIS-RAM es accesible y práctico para guiar a una empresa a través del proceso de toma de decisiones de riesgo al implementar controles de seguridad (y las acciones y salvaguardas de apoyo) para determinar que el riesgo de daño a otras partes sea proporcional a los pasos tomados para reducir el riesgo.

La determinación de la razonabilidad de los controles de ciberseguridad sirve a múltiples públicos y debe ser significativa para esas comunidades. Las leyes mencionadas anteriormente son un claro indicador de que el programa de ciberseguridad de una empresa no solo debe proteger a su propia organización, sino que debe proporcionar ciberseguridad razonable para mitigar el daño a otros.

Los reguladores, para mantener la confianza y credibilidad públicas, deben ser capaces de articular lo que significan sus regulaciones cuando exigen salvaguardas razonables. Los litigantes deben poder presentar argumentos claros en interés de sus clientes sobre prácticas razonables sin ceder ante una confusa "batalla de expertos". Y quizás lo más importante, el público debe contar con algún estándar para determinar cuándo las acciones y políticas de una organización reflejan un nivel adecuado de cuidado en apoyo de sus fines legítimos que sirven al público. Aprovechar los conceptos de esta guía responde a todos estos objetivos, con un resultado adicional previsto: reducir los litigios.

SECCIÓN 3

Resumen de la Legislación Actual sobre Ciberseguridad en Estados Unidos

Si bien una ley federal reciente exige que las organizaciones de infraestructura crítica informen los incidentes cibernéticos al Departamento de Seguridad Nacional (DHS)[7] y a la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), la regulación de la ciberseguridad incluye cada vez más requisitos específicos para organizaciones en sectores determinados, o para organizaciones que buscan hacer negocios con entidades federales específicas. Como resultado, la regulación federal sigue siendo sectorial, inconsistente e incompleta.

Mientras tanto, todos los estados de EE. UU. requieren que las organizaciones notifiquen a las personas[8] afectadas, y a menudo a los reguladores, cuando ocurre una violación de datos, y casi el 40 % de los estados han añadido requisitos para que las entidades cubiertas tomen medidas proactivas de seguridad de datos para proteger la información de identificación personal (PII). Como se mencionó anteriormente, cinco estados hacen referencia a prácticas recomendadas específicas de la industria como estándares de seguridad razonables. Si bien estas leyes estatales siguen una tendencia similar hacia requisitos cada vez más específicos para la ciberseguridad, también son incompletas y, en ocasiones, contradictorias. Además, el derecho consuetudinario estatal (es decir, el conjunto de leyes basadas en decisiones judiciales en lugar de en códigos o estatutos) también es relevante para definir lo que significa razonable, y esto varía de un estado a otro.

A continuación se presenta un resumen abreviado del mosaico de leyes y regulaciones federales y estatales existentes en la actualidad. Muchas de estas leyes no han podido mantenerse al ritmo del crecimiento y la complejidad de la tecnología y su uso en la sociedad. Además, el lector notará que no existe una guía clara y coherente que defina lo que constituye una ciberseguridad razonable.

Resumen de la Legislación Federal

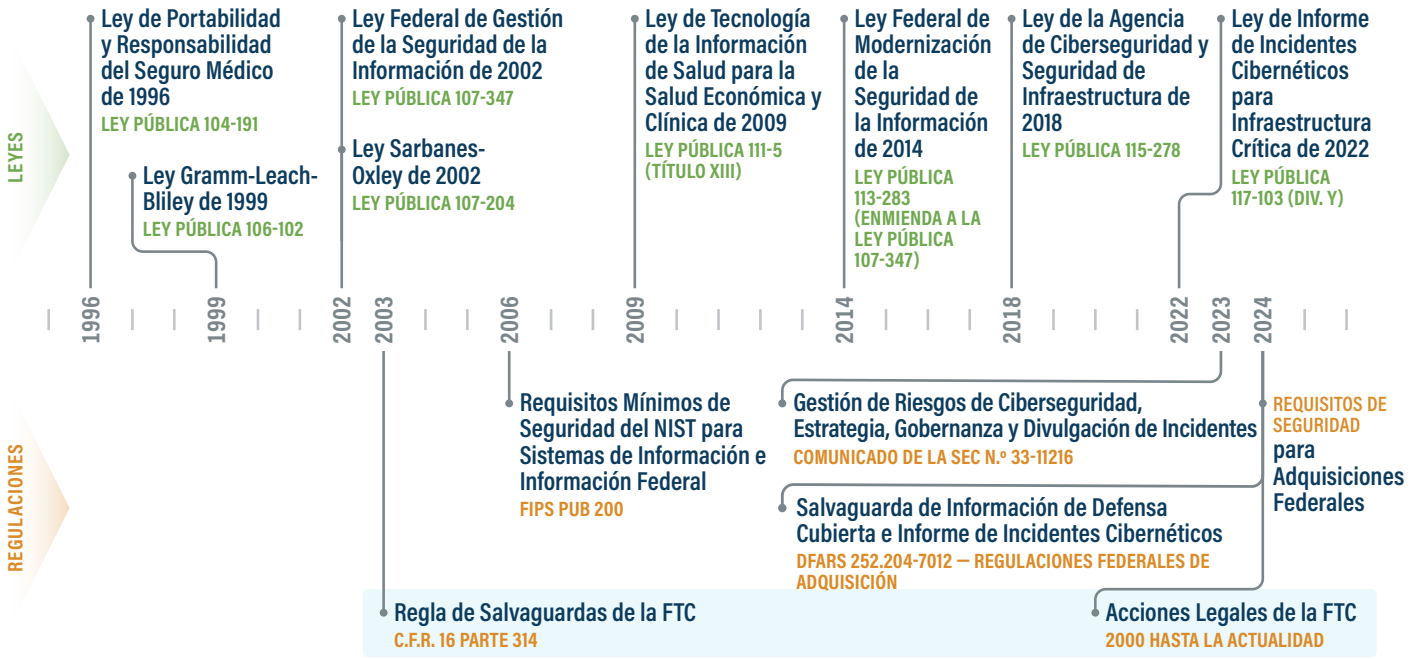
La legislación federal sobre ciberseguridad en Estados Unidos ha adoptado diferentes formas en distintos momentos. La Figura 1 muestra un resumen abreviado de ese mosaico de estatutos y regulaciones. Para más detalles sobre los requisitos federales en esta línea de tiempo, véase el Apéndice K.

Resumen de la Legislación Estatal

Los 50 estados más el Distrito de Columbia, Guam, Puerto Rico y las Islas Vírgenes de EE. UU. tienen leyes de notificación de violaciones de seguridad que exigen a las organizaciones notificar a los consumidores o ciudadanos si su PII ha sido comprometida.[9]

Los estados han adoptado cada vez más leyes específicas de seguridad de datos o han incluido requisitos de seguridad de datos como parte de estatutos más amplios sobre privacidad de datos del consumidor. Como se

Figure 1: Cronología de Regulaciones Federales



mencionó anteriormente y se señala en los Apéndices B y C, estas leyes, representadas en las Figuras 2 y 3, abordan las siguientes categorías de temas:

- Leyes generales que exigen medidas razonables de seguridad de datos expresadas en términos amplios
- Leyes más prescriptivas que exigen que las organizaciones desarrollen, implementen y mantengan medidas específicas de seguridad de datos, en algunos casos incluyendo controles específicos y/o programas de seguridad de datos escritos y completos
- Leyes integrales de privacidad de datos del consumidor que incorporan requisitos de seguridad de datos, a menudo expresados en términos amplios de seguridad razonable pero en algunos casos con requisitos más específicos
- Leyes de puerto seguro que brindan incentivos para que las organizaciones adopten programas de seguridad de datos integrales. Permiten, por ejemplo, que las empresas aleguen una defensa afirmativa o limiten los daños punitivos en litigios de ciberseguridad cuando la empresa ha implementado estándares ampliamente reconocidos y adoptados como mejores prácticas, incluyendo el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) y los Controles del CIS requirements
- Leyes que se enfocan en industrias o actividades específicas, incluyendo leyes sobre dispositivos conectados que imponen requisitos específicos de seguridad de datos

A la fecha de publicación de esta guía, 19 estados han promulgado leyes integrales de privacidad de datos o de privacidad de datos de salud que exigen a las organizaciones que

Figure 2: State Comprehensive and Health Data Privacy Statutes

Leyes Estatales Integrales de Privacidad de Datos

California. Ley de Privacidad del Consumidor de California, enmendada por la Ley de Derechos de Privacidad de California

Colorado. S. B. 21-190, Ley de Privacidad de Colorado

Connecticut. S. B. 6: Ley sobre Privacidad de Datos Personales y Monitoreo en Línea

Delaware. H. B. 154, Ley de Privacidad de Datos Personales de Delaware

Florida. S. B. 262, Declaración de Derechos Digitales de Florida

Indiana. S. B. 5, Protección de Datos del Consumidor

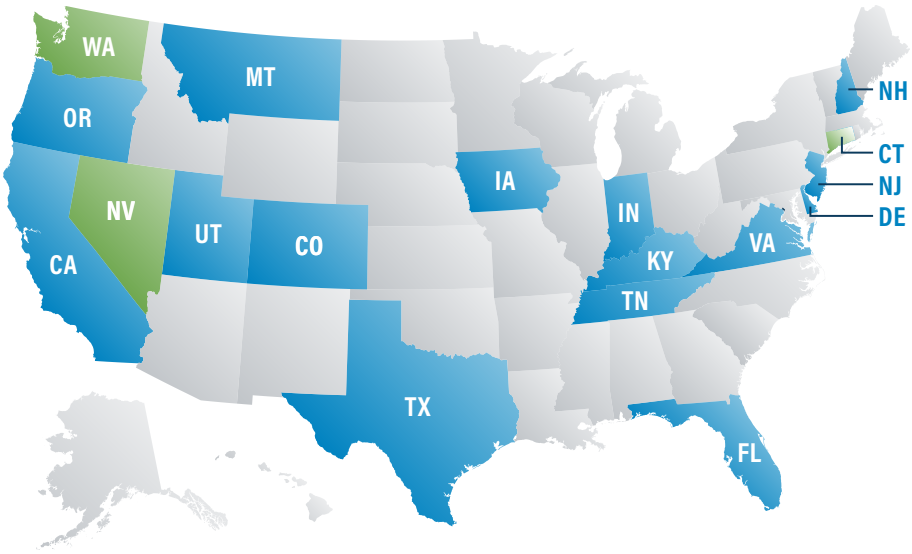
Iowa. S. F. 262, Ley de Protección de Datos del Consumidor

Kentucky. H. B. 15, Ley de Protección de Datos del Consumidor de Kentucky

Montana. S. B. 384, Ley de Privacidad de Datos del Consumidor

New Hampshire. S. B. 255, Expectativa de Privacidad del Consumidor

New Jersey. S. 332, Ley sobre Sitios Web Comerciales de Internet, Consumidores e Información de Identificación Personal



Oregon. S. B. 619, Ley Relativa a las Protecciones de Datos Personales de los Consumidores

Tennessee. H. B. 1181, Ley de Protección de la Información de Tennessee

Texas. H. B. 4, Ley de Privacidad y Seguridad de Datos de Texas

Utah. S. B. 227, Ley de Privacidad del Consumidor

Virginia. Ley de Protección de Datos del Consumidor

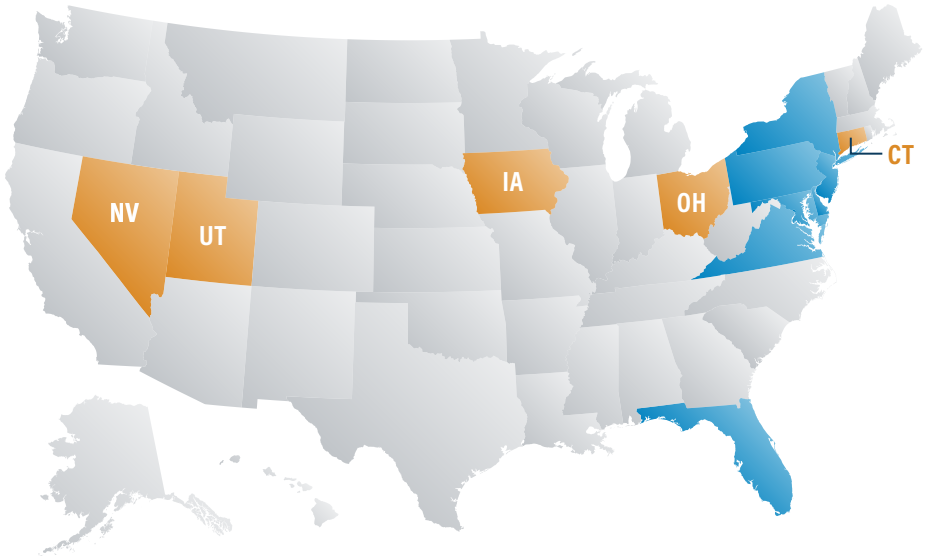
Leyes Estatales de Privacidad de Datos de Salud

Connecticut. S. B. 3, Ley sobre Privacidad en Línea, Datos y Protecciones de Seguridad

Nevada. S. B. 370, Ley de Privacidad de Datos de Salud

Washington. H. B. 1155, Ley de Washington: Mi Salud, Mis Datos

Figure 3: States Leading the Way to Achieve Reasonable Cybersecurity*



Connecticut. Ley de Incentivos para la Adopción de Estándares de Ciberseguridad para Empresas

Iowa. Defensas Afirmativas para Entidades que Utilizan Programas de Ciberseguridad

Nevada. Uso estatal de "medidas de seguridad razonables" para proteger la Información de Identificación Personal

Ohio. Ley de Protección de Datos

Utah. Ley de Defensa Afirmativa en Ciberseguridad

Decretos de Consentimiento del Fiscal General: Delaware, Florida, Maryland, New Jersey, Nueva York, Pensilvania, Virginia, Washington D.C.

***See Appendix C and Appendix J for more information**

controlan información privada proteger esos datos en sus redes informáticas mediante seguridad razonable, pero sin proporcionar criterios para lograrlo. Además, cinco estados (algunos coinciden con los 19 anteriores) han emitido leyes que indican que seguir uno de los marcos de referencia de la industria identificados expresamente en dichas leyes constituye evidencia concluyente de ciberseguridad razonable. De esos cinco, cuatro son leyes de "puerto seguro" que incentivan la adopción voluntaria de ciertas mejores prácticas de ciberseguridad. La quinta ley, de Nevada, es un estatuto relacionado con la información personal recopilada por agencias gubernamentales. Todas estas cinco leyes citan ejemplos como el Marco de Ciberseguridad del NIST o los Controles Críticos de Seguridad del CIS, aunque no exigen un marco específico ni indican cómo deben interpretarse o implementarse dichos marcos para demostrar la debida diligencia. Véanse las Figuras 2 y 3.

Aparte de estas promulgaciones legislativas, las regulaciones y directivas del poder ejecutivo estatal, decisiones y recomendaciones de mejores prácticas de otras autoridades se han vuelto más comunes. A continuación se citan algunos ejemplos.

Un ejemplo es que en 2009, Massachusetts promulgó varios requisitos sustantivos para las entidades cubiertas, incluyendo un programa integral de seguridad de la información por escrito que contiene controles administrativos, técnicos y físicos.[10]

Otro ejemplo es la regulación cibernética del Departamento de Servicios Financieros del Estado de Nueva York (NYDFS). Con vigencia a partir del 1 de noviembre de 2023, NYDFS enmendó sus regulaciones existentes sobre ciberseguridad para garantizar aún más que la ciberseguridad esté integrada en la planificación empresarial, toma de decisiones y gestión continua del riesgo de las entidades reguladas.[11] En particular, las nuevas reglas:

- Refuerzan los requisitos de gobernanza
- Exigen controles adicionales para prevenir el acceso no autorizado a los sistemas de información y para prevenir o mitigar la propagación de un ataque
- Requieren evaluaciones más frecuentes de riesgos y vulnerabilidades, así como planes más sólidos de respuesta a incidentes y recuperación ante desastres
- Actualizan los requisitos de notificación existentes, incluyendo un nuevo requisito para reportar pagos por ransomware
- Actualizan los requisitos para programas anuales de capacitación y concientización en ciberseguridad

Otro ejemplo es que en 2017, la Conferencia de Supervisores Bancarios Estatales (una organización nacional de reguladores financieros y bancarios) publicó sus recomendaciones en una guía de recursos de ciberseguridad para ejecutivos bancarios, identificando estándares reconocidos por la industria sobre mejores prácticas de ciberseguridad actualmente utilizadas en el sector de servicios financieros y un enfoque organizacional utilizado por NIST.[12]

Más recientemente, varios fiscales generales estatales han firmado decretos de consentimiento con empresas que han sufrido una violación. Estos acuerdos de cumplimiento estipulan que la empresa debe desarrollar, implementar y mantener un programa de

ciberseguridad diseñado para proteger la seguridad de la PII. Véase el Apéndice J para más detalles.

En litigios civiles relacionados con violaciones de datos, los reclamos por responsabilidad extracontractual (torts) bajo el derecho consuetudinario generalmente incluyen alegaciones que requieren probar que una organización no tomó medidas razonables para proteger la información comprometida. Por lo general, esto significa que el demandante contrataría a un experto en ciberseguridad que testificaría que lo que proporcionó la empresa no fue razonable (es decir, carecía de capacidades o prácticas clave de seguridad), y la empresa, a su vez, contrataría a su propio experto en ciberseguridad que testificaría que lo que proporcionó fue razonable.

Aunque este campo del derecho está evolucionando hacia la exigencia de medidas de seguridad de datos más específicas para algunas organizaciones en algunos contextos (por ejemplo, PCI DSS para minoristas, FFIEC CAT para bancos, NIST 800-171 para contratistas federales), las organizaciones fuera de estas áreas todavía enfrentan el desafío de identificar por sí mismas qué constituye una ciberseguridad razonable. E incluso en áreas donde la ley estatal o federal prescribe ciertas medidas, al enfrentarse a un litigio o una investigación regulatoria, una organización debe ser capaz de articular por qué las medidas que tomó (o no tomó) para proteger información sensible fueron razonables.

SECCIÓN 4

Uso de Leyes de Puerto Seguro y Marcos de la Industria para Definir la Ciberseguridad Razonable

"Esperamos que las medidas de seguridad razonables incluyan medidas que comúnmente son objeto de buenas prácticas."[13]

Federal Communication Commission

"En ausencia de una orientación clara por parte de los tribunales, las organizaciones deben apoyarse en una variedad de fuentes para determinar el estándar razonable de cuidado en ciberseguridad, incluyendo las mejores prácticas de la industria, las regulaciones gubernamentales y las opiniones de expertos."

James Lewis, Senior Vice President and Director of the Center for Strategic and International Studies

Las organizaciones generalmente miran hacia adentro para determinar el impacto de los incidentes de ciberseguridad, considerando costos menos visibles y mejor entendidos como interrupciones laborales, investigaciones técnicas, mejoras en ciberseguridad, notificaciones de violación y protecciones posteriores para los consumidores, así como costos regulatorios y de recuperación, multas, tarifas y acuerdos.[14] A menudo olvidan incluir en su análisis de riesgos el daño que pueden causar a otros. (Véase el Apéndice I para una discusión de dos metodologías para evaluar la ciberseguridad razonable.)

Los estados están comenzando a señalar soluciones al identificar y aceptar mejores prácticas de la industria y al hacer referencia a marcos publicados como constitutivos de una seguridad razonable. El Fiscal General de California, en un Informe sobre Violaciones de Datos, concluyó que no implementar todos los Controles Críticos del CIS relevantes "constituye una falta de seguridad razonable."[15]

Además, la ley de Nevada exige que las agencias gubernamentales estatales que mantengan información de identificación personal (PII) de residentes implementen y mantengan medidas de seguridad razonables publicadas por el NIST o el Center for Internet Security relacionadas con la recopilación, difusión y mantenimiento de registros que contienen información personal.[16]

Varios fiscales generales estatales también están definiendo la ciberseguridad razonable en sus acuerdos de resolución de violaciones. Estos acuerdos citan el método de evaluación de riesgos del CIS (CIS RAM) y reiteran sus tres factores para determinar la razonabilidad de los controles (ver Apéndice J). Los principios del CIS RAM (y el Análisis de Riesgo por Deber de Cuidado en que se basa) exigen que las

organizaciones consideren el riesgo para todas las partes, que solo acepten riesgos cuando no se requiera un remedio para ninguna parte, y cuando la carga de una salvaguarda no sea mayor que el riesgo resultante de no implementarla. Estos tres factores pueden servir como punto de partida para cualquier análisis de riesgo cibernético.

Además, como se resume en la Sección 3, varios estados han aprobado leyes de puerto seguro, que proporcionan una forma común de identificar la ciberseguridad razonable. (Véase el Apéndice C para una lista de estas leyes). Aunque varían ligeramente, estas leyes siguen una estructura similar. Tomando como ejemplo la ley de Ohio, pionera entre las leyes de puerto seguro, su estatuto concluye que la escala y alcance del programa de ciberseguridad de una empresa "es apropiado si se basa en todos los siguientes factores":[17]

- El tamaño y complejidad de la empresa
- La naturaleza y alcance de las actividades de la empresa
- La sensibilidad de la información que debe protegerse
- El costo y la disponibilidad de herramientas para mejorar la seguridad de la información y reducir vulnerabilidades
- Los recursos disponibles para la empresa

Después de identificar estos cinco factores, la ley de Ohio aclara aún más que se considerarán razonables las defensas basadas en:[18]

- El Marco para la Mejora de la Ciberseguridad de Infraestructuras Críticas del NIST
- NIST Publicación Especial 800-171
- NIST Publicaciones Especiales 800-53 y 800-53a
- El Marco de Evaluación de Seguridad de FedRAMP
- Los Controles Críticos de Seguridad del CIS
- La familia ISO/IEC 27000 – Sistemas de Gestión de Seguridad de la Información

Para organizaciones en sectores específicos, estas leyes también ofrecen orientación sectorial, concluyendo que una empresa ha implementado seguridad razonable si se ajusta a las normas vigentes aplicables:[19]

- Requisitos de seguridad de HIPAA
- Título V de la Ley Gramm-Leach-Bliley
- FISMA, modificado en 2014
- Ley HITECH
- Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)

Un aspecto importante es que estos estándares tienen supervisión y aplicación regulatoria activa sobre las entidades cubiertas.

Al identificar un conjunto de estándares de la industria más específicos, prescriptivos y priorizados, estas leyes pueden contribuir a una definición más clara de lo que constituye "seguridad razonable" en general, en otras jurisdicciones y contextos fuera del ámbito de las leyes sectoriales.

Donde no se apliquen normas sectoriales ni regulaciones estatales específicas, las siguientes consideraciones pueden ayudar a definir mejor la ciberseguridad razonable.

Aunque la mayoría de estos marcos proporcionan orientación relativamente específica para realizar evaluaciones, no establecen un estándar definitivo de cumplimiento. Por ejemplo, el NIST 800-53 enfatiza que el cumplimiento requiere "usar toda la información apropiada como parte de un programa de gestión de riesgos a nivel organizacional" y el uso efectivo de "la orientación de adaptación y flexibilidad inherente en las publicaciones del NIST para que los controles seleccionados documentados en los planes de seguridad organizacionales satisfagan las necesidades de la misión y negocio."[20] Implementar estos estándares en una organización requiere pericia considerable y juicio sólido.

Los diversos marcos mencionados en esta guía ofrecen una gama de acciones defensivas prescriptivas y flexibles. Algunos son estándares de políticas (por ejemplo, el NIST CSF), otros estándares de datos (como PCI[21] o salud e ISO[22]). Los Controles del CIS, citados en las leyes de puerto seguro y en los estatutos de Nevada, son estándares operativos. Aunque existen otros marcos respetados, esta guía considera los Controles del CIS como un estándar emergente, de facto y práctico (véase Apéndice D). La siguiente sección se enfoca específicamente en los Controles del CIS y agrupa sus acciones subyacentes en categorías comprensibles para permitir una aplicación más directa.

Los lectores interesados en otros marcos pueden consultar los mapeos detallados en el Apéndice F.

SECCIÓN 5

Cómo una Organización Debe Implementar Correctamente Salvaguardas Cibernéticas para Lograr una Ciberseguridad Razonable

Los líderes organizacionales deben hacerse un conjunto básico de preguntas sobre la salud de su ciberseguridad, incluyendo:

- ¿Cuál es el alcance de nuestra misión, obligaciones y partes interesadas?
- ¿Sabemos qué está conectado a nuestros sistemas y redes?
- ¿Sabemos qué se está ejecutando o intenta ejecutarse en nuestros sistemas y redes?
- ¿Comprendemos los datos que fluyen por nuestros sistemas y su sensibilidad relativa?
- ¿Estamos limitando y gestionando el número de personas con privilegios en nuestros sistemas y redes?
- ¿Hemos establecido procesos para revisar la salud de nuestras redes, capacitar a empleados y recuperarnos de posibles violaciones?
- ¿Cuáles son nuestras brechas y qué riesgos representan?

Al abordar estas (y otras) preguntas, las organizaciones pueden demostrar que han establecido y mantienen activamente un programa de ciberseguridad que incluye protecciones acordes con el riesgo y la magnitud del daño que podría resultar de una violación. Una de las formas más efectivas de demostrar esto es alineándose con un marco de ciberseguridad reconocido y midiendo la conformidad y el progreso en la implementación de los criterios de seguridad de ese marco. Además, las organizaciones deben identificar recursos, realizar auditorías o evaluaciones periódicas de su programa (como evaluaciones de riesgos y evaluaciones independientes para verificar la precisión y suficiencia del programa de ciberseguridad) y abordar las brechas identificadas. Generalmente, las organizaciones no pueden implementar todos los controles de una vez. Ni pueden la mayoría de ellas aplicar todos los controles a todos los sistemas y activos como los presentan los estándares. Las evaluaciones de riesgos ayudan a las organizaciones a priorizar la implementación de controles. Todos estos pasos deben repetirse según lo definido por el programa de ciberseguridad. (Véase el Apéndice L para una Lista de Verificación de Políticas de Razonabilidad.)

Existen múltiples marcos de ciberseguridad para elegir, y muchos de ellos brindan recomendaciones de seguridad confiables. Independientemente del marco que elija una organización, es importante entender que "no se trata solo de la lista (criterios)". Igualmente importante es el ecosistema que respalda esa lista. Las organizaciones deben poder: obtener formación, acceder a guías de implementación de colegas, medir el progreso o la madurez, y mostrar alineación con cualquier marco

normativo y de cumplimiento requerido. En esta guía, nos enfocamos en los Controles Críticos del CIS como guía para que una organización demuestre (y en estados con leyes de puerto seguro, se beneficie de ello) que ha tomado medidas razonables de ciberseguridad. Véase el Apéndice D para conocer por qué los Controles del CIS se están convirtiendo en un estándar de facto global. Los Controles del CIS son, de forma deliberada, muy detallados. Sin embargo, pueden dividirse en los siguientes componentes de sentido común:

1. Conocer su entorno
2. Gestión de cuentas y configuración
3. Herramientas de seguridad
4. Recuperación de datosrecovery
5. Concientización en seguridad
6. Procesos de negocio y subcontratación (véase el Apéndice G para más detalle)

Los controles de seguridad aplicados a una empresa deben defenderse contra y/o mitigar los efectos de ataques reales. Además, una organización debe establecer controles y procesos adicionales para responder y recuperarse de un ataque. Estos controles combinados conforman una seguridad razonable. (Para una descripción completa de las actividades prescriptivas y priorizadas que las organizaciones deben tomar para defender su empresa, véase el Apéndice H.)

Conocer su Entorno

Lo primero que debe hacer una organización al implementar un marco de ciberseguridad es "conocer su entorno". Debe saber qué activos (hardware y software) hay en su red. También debe identificar los datos en la empresa que están obligados a proteger. Luego, para minimizar su superficie de ataque, puede priorizar la aplicación de controles de seguridad a los activos donde residen los datos de mayor valor.

Gestión de Cuentas y Configuración

Una vez que se entienden los activos del entorno empresarial, el siguiente paso es realizar una gestión de cuentas y configuración. Esto incluye definir procesos y reglas para crear y revocar cuentas, y determinar qué accesos tienen las cuentas a los recursos del sistema y de la empresa. Esta gobernanza de cuentas es esencial porque una vía común de ataque es comprometer cuentas y aprovechar el acceso que tienen en la red.

Otra forma altamente efectiva de mitigar y detectar actividad maliciosa es aplicar y mantener una configuración segura en todos los activos de hardware y software empresarial. Esto incluye la infraestructura de red. Habilitar el parcheo automático y mantener el software actualizado es una forma primaria en que las organizaciones pueden defenderse. También es clave configurar la recopilación, agregación y revisión obligatoria de registros de auditoría, ya que esto ayuda a detectar y comprender un ataque.

Herramientas de Seguridads

Pueden utilizarse herramientas comerciales de ciberseguridad para proteger contra ataques comunes, como intrusiones específicas o malware. El malware puede ingresar a una organización a través de vulnerabilidades en la infraestructura de red, dispositivos de usuario final, archivos adjuntos de correo electrónico, páginas web, y más. Por eso, las protecciones en navegadores web y correos electrónicos son importantes para la defensa de red. Las organizaciones pueden desplegar herramientas para evitar que los usuarios accedan a sitios maliciosos conocidos y para bloquear archivos

adjuntos peligrosos. La monitorización continua mediante detección y respuesta en endpoints (EDR) también es importante para defenderse contra amenazas prioritarias.

Además, las herramientas de detección y prevención de intrusos en host y red son fundamentales para protegerse contra amenazas en toda la infraestructura y la base de usuarios de la empresa.

Recuperación de Datos

Dado el panorama actual de amenazas, todas las organizaciones, sin importar su tamaño o industria, deben contar con un plan de recuperación de datos como preparación para una violación. Como tal, deben implementarse prácticas recomendadas para recuperarse y responder ante incidentes. Las organizaciones deben implementar un proceso de recuperación de datos que incluya respaldos automáticos. Igualmente importante es establecer un programa para desarrollar y mantener una capacidad de respuesta a incidentes. Como mínimo, deben identificarse los roles y la información de contacto del personal clave responsable de coordinar y responder ante incidentes.

Concientización en Seguridad

Un programa eficaz de ciberseguridad implementa controles a través de personas, procesos y tecnología. Por lo tanto, una parte integral de cualquier programa es la educación en concientización de seguridad. Esta es la defensa más efectiva contra ataques de ingeniería social, donde los actores de amenazas se hacen pasar por una fuente confiable o engañan a los usuarios para que hagan clic en un enlace malicioso.

La ingeniería social también es un vector popular para entregar ransomware. Además de la capacitación, la concientización en seguridad puede incluir entender cuán resistente es la empresa a las intrusiones. Las organizaciones pueden probar la efectividad de los controles de seguridad realizando pruebas de penetración y corrigiendo vulnerabilidades.

Procesos de Negocio y Subcontratación

Muchas organizaciones subcontratan sus procesos de negocio. Por lo tanto, deben desarrollar procesos para evaluar y gestionar a los proveedores de servicios que manejan sus datos y funciones sensibles. Esto incluye hacer un inventario, clasificar y evaluar a dichos proveedores.

Implementar estas mejores prácticas permite a las organizaciones defenderse contra las principales amenazas. Estudios como el Informe de *Investigaciones de Violaciones de Datos de Verizon*[23] y el *Plan de Acción para la Mitigación, Respuesta y Recuperación ante Ransomware del Institute for Security and Technology*[24] brindan evidencia detallada de ello. Para más información sobre la efectividad de seguir un marco como este, consulte el Apéndice H con la implementación de los Controles Críticos del CIS y las acciones subyacentes que los respaldan.

SECCIÓN 6

Conclusión

Al abordar medidas de ciberseguridad razonables, es de vital importancia que una organización establezca y mantenga un programa de ciberseguridad que equilibre el alcance y la complejidad de los controles implementados frente al riesgo y las consecuencias de una violación de datos. Esta guía propone que esto puede lograrse implementando los Controles Críticos del CIS (uno de varios marcos conocidos y referenciados), y dividiendo ese marco en conjuntos de actividades que pueden aplicarse a otros marcos. Los conceptos tratados aquí, y ampliados en los apéndices, proporcionan una base crítica para ayudar a asesores legales, consultores de ciberseguridad, auditores y reguladores, así como abogados, litigantes y tribunales, a determinar qué constituye seguridad razonable en asuntos que involucran violaciones de datos.

APÉNDICE A

Glosario

Cuentas de administrador	Cuentas para usuarios que requieren privilegios elevados. Estas cuentas se utilizan para gestionar aspectos de una computadora, dominio o toda la infraestructura de tecnología de la información empresarial. Cada cuenta de administrador debe asignarse a un solo usuario. Los subtipos comunes de cuentas de administrador incluyen cuentas root, administrador local, cuentas de administrador de dominio y cuentas de administrador de dispositivos de red o seguridad.
Aplicación	Un programa, o un grupo de programas, que se ejecuta sobre un sistema operativo alojado en un activo empresarial. Ejemplos de tipos de aplicaciones incluyen aplicaciones web, de bases de datos, basadas en la nube y móviles. En este documento, las aplicaciones se consideran un activo de software.
Sistemas de autenticación	Un sistema o mecanismo utilizado para identificar a un usuario asociando una solicitud entrante con un conjunto de credenciales de identificación. Las credenciales proporcionadas se comparan con las registradas en una base de datos de información de usuarios autorizados en un sistema operativo local, un servicio de directorio de usuarios o dentro de un servidor de autenticación. Ejemplos de sistemas de autenticación pueden incluir directorio activo (Active Directory), autenticación multifactor (MFA), biometría y tokens.
Sistemas de autorización	Un sistema o mecanismo utilizado para determinar niveles de acceso o privilegios de usuario/cliente relacionados con recursos del sistema, incluyendo archivos, servicios, programas informáticos, datos y funciones de aplicaciones. Un sistema de autorización concede o deniega el acceso a un recurso basado en la identidad del usuario. Ejemplos de sistemas de autorización pueden incluir directorios activos, listas de control de acceso y listas de control de acceso basadas en roles.

Controles CIS	Los Controles Críticos de Seguridad del CIS son un conjunto integral de 18 medidas específicas de ciberseguridad, o controles, para proteger sistemas y gestionar riesgos cibernéticos. Un Control CIS individual es una práctica recomendada a nivel estratégico que, a su vez, está respaldada por múltiples Salvaguardas CIS. Véase, por ejemplo, el Control CIS 3: Desarrollar Procesos y Controles Técnicos para Identificar, Clasificar, Gestionar de Forma Segura, Conservar y Eliminar Datos.
Salvaguarda CIS	Una medida de seguridad técnica o procedimental prescriptiva que respalda un Control CIS más amplio para defender sistemas y datos contra amenazas cibernéticas. Las salvaguardas representan los pasos accionables requeridos para la implementación adecuada de un control. Ejemplos incluyen documentar un proceso de gestión de datos (3.1), eliminar de forma segura datos de todos los activos empresariales (3.5) y definir requisitos de sensibilidad de datos (3.7).
Ciberseguridad	Protección de sistemas, redes y la información contenida en ellos contra ataques digitales o electrónicos.
Evaluación de riesgo de ciberseguridad	Proceso mediante el cual se identifican los riesgos y se determina el impacto de dichos riesgos.
Base de datos	Colección organizada de datos, generalmente almacenados y accedidos electrónicamente desde un sistema informático. Las bases de datos pueden estar ubicadas remotamente o en sitio. Los Sistemas de Gestión de Bases de Datos (DMS) se utilizan para administrar bases de datos y no se consideran parte de una base de datos para este documento.
Privacidad de los datos	Subconjunto de las actividades de seguridad de datos destinadas a asegurar que los datos solo estén disponibles para quienes tienen acceso autorizado a ellos.

Seguridad de los datos	Protección de los datos (es decir, información: datos personales, operacionales y del sistema) contra acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para proporcionar integridad, confidencialidad y disponibilidad de dichos datos. (Análogo a seguridad de la información). A veces, esta definición también incluye la protección de los sistemas y redes donde residen los datos.
Deber de cuidado, Estándar de cuidado, Diligencia debida	El deber de cuidado es una obligación legal de evitar acciones u omisiones que podrían previsiblemente dañar a otros. El estándar de cuidado es el nivel específico de atención que se espera bajo el deber de cuidado. A menudo se mide por las acciones de una persona razonablemente prudente en circunstancias similares. La diligencia debida es un término para el cumplimiento del estándar de cuidado que implica actuar con la cautela necesaria para evitar riesgos previsibles. A menudo se denomina "cuidado ordinario" o "cuidado razonable" y es una referencia para evaluar si se ha incumplido un deber de cuidado.
Ecosistema	Procesos, información y apoyo relacionados con y que sustentan un tema o actividad particular.
Dispositivos de usuario final	Activos de tecnología de la información (TI) utilizados por los miembros de una empresa durante su jornada laboral o fuera de ella. Incluyen escritorios y estaciones de trabajo, así como dispositivos portátiles y móviles como laptops, teléfonos inteligentes y tabletas. Para efectos de este documento, los dispositivos de usuario final son un subconjunto de los activos empresariales.
Activos empresariales	Activos con el potencial de almacenar o procesar datos. Para efectos de este documento, los activos empresariales incluyen dispositivos de usuario final, dispositivos de red, dispositivos no informáticos/IoT y servidores, en entornos virtuales, basados en la nube y físicos.

Activos empresariales expuestos externamente	Hace referencia a activos empresariales que están orientados al público y pueden ser detectados mediante reconocimiento del sistema de nombres de dominio y escaneo de red desde Internet pública fuera de la red de la empresa.
Seguridad de la información	Ver Seguridad de los Datos. En terminología anterior, este término se refería a asegurar la disponibilidad, integridad y confidencialidad de los sistemas electrónicos y sus datos.
Activos empresariales internos	Se refiere a activos empresariales no orientados al público que solo pueden ser identificados mediante escaneos de red y reconocimiento desde dentro de la red empresarial mediante acceso autenticado o no autenticado autorizado.
Biblioteca (library)	Un código precompilado y compartible que incluye clases, procedimientos, scripts, datos de configuración, y más, utilizado para desarrollar programas y aplicaciones de software. Las bibliotecas están diseñadas para asistir tanto al programador como al compilador del lenguaje de programación en la construcción y ejecución de software de manera más eficiente.
Dispositivos de red	Dispositivos electrónicos necesarios para la comunicación e interacción entre dispositivos en una red informática. Incluyen puntos de acceso inalámbricos, firewalls, puertas de enlace físicas/virtuales, enrutadores y conmutadores. Estos dispositivos pueden ser de hardware físico, así como virtuales y basados en la nube. Para efectos de este documento, los dispositivos de red son un subconjunto de los activos empresariales. Cabe destacar que también cumplen un doble papel como parte de la Clase de Activos de Red cuando se relacionan con la comunicación a través de una red.
Infraestructura de red	Hace referencia a todos los recursos de una red que hacen posible la conectividad a red o a Internet, la gestión, las operaciones comerciales y la comunicación. Consiste en hardware y software, sistemas y dispositivos, y permite la computación y comunicación entre usuarios, servicios, aplicaciones y procesos. La infraestructura de red puede ser en la nube, física o virtual.

Sistema operativo	Software en los activos empresariales que gestiona los recursos de hardware y software del ordenador y proporciona servicios comunes para los programas. Ejemplos de sistemas operativos incluyen Windows, Ubuntu, MacOS, Android y z/OS. Los sistemas operativos se consideran activos de software.
Información de identificación personal (PII)	Información que puede usarse para distinguir o rastrear la identidad de una persona, ya sea sola o combinada con otra información que esté vinculada o sea vinculable a una persona específica, NIST SP 800-63-3.
Entorno físico	Partes físicas de hardware que componen una red, incluyendo cables y enrutadores. El hardware es necesario para la comunicación e interacción entre dispositivos en una red.
Ciberseguridad razonable	Medidas destinadas a proteger contra la pérdida, el uso indebido o el acceso o modificación no autorizados de sistemas técnicos, información o datos, basadas en el estándar de cuidado apropiado sobre cómo actuaría una persona razonablemente prudente en las mismas o similares circunstancias. Las consideraciones incluyen, entre otras: ▪ Tamaño y complejidad de la organización ▪ Naturaleza y alcance de las actividades de la organización ▪ Sensibilidad de la información y sistemas a proteger ▪ Costo y disponibilidad de herramientas para mejorar la seguridad de la información y reducir vulnerabilidades ▪ Recursos disponibles para la organización Algunas leyes estatales sostienen que implementar razonablemente prácticas recomendadas específicas de la industria constituye ciberseguridad razonable.
Dispositivos remotos	Cualquier activo empresarial capaz de conectarse a una red de forma remota, usualmente desde Internet pública. Esto puede incluir activos empresariales como dispositivos de usuario final, dispositivos de red, dispositivos no informáticos/IoT y servidores.

Servidores	Un dispositivo o sistema que proporciona recursos, datos, servicios o programas a otros dispositivos en una red de área local o red de área amplia. Los servidores pueden proporcionar y consumir recursos de otro sistema al mismo tiempo. Pueden estar ubicados en centros de datos, entornos de nube pública/privada/híbrida, incluyendo contenedores temporales o cargas de trabajo sin servidor. Ejemplos de servidores incluyen servidores web, servidores de aplicaciones, servidores de correo y servidores de archivos. Para efectos de este documento, los servidores son un subconjunto de los activos empresariales.
Cuentas de servicio	Una cuenta de servicio se crea específicamente para ejecutar aplicaciones, servicios y tareas automatizadas en un sistema operativo. También pueden crearse simplemente para ser propietarias de datos y archivos de configuración. Cada cuenta de servicio debe usarse para un servicio o función específica y debe tener un responsable asignado que sea responsable de su uso. Las cuentas de servicio no deben usarse para tareas informáticas generales.
Servicios	Programas especializados que realizan tareas críticas bien definidas para el sistema operativo. Los servicios generalmente se inician con el sistema operativo, se ejecutan en segundo plano y pueden ser detenidos e iniciados por los usuarios. Ejemplos de servicios incluyen la gestión de comunicaciones de red, usuarios, permisos de archivos, seguridad del sistema e interacción con dispositivos.
Ingeniería social	Hace referencia a una amplia gama de actividades maliciosas logradas mediante interacciones humanas en varias plataformas, como correo electrónico o teléfono. Se basa en la manipulación psicológica para engañar a los usuarios y que cometan errores de seguridad o revelen información sensible.
Activos de software	También denominados software en este documento, son los programas y otra información operativa utilizada dentro de un activo empresarial. Los activos de software incluyen sistemas operativos y aplicaciones.

Cuentas de usuario	Una identidad compuesta por un conjunto de credenciales (por ejemplo, nombre de usuario, contraseña) que define a un usuario en un sistema informático. Una cuenta de usuario lleva un registro de la información y configuraciones del usuario, controla los archivos, carpetas y recursos a los que puede acceder, así como las tareas que puede realizar. Para efectos de este documento, las cuentas de usuario se refieren a cuentas de usuario "estándar" con privilegios limitados y se utilizan para tareas generales.

APÉNDICE B

Leyes Estatales de Privacidad de Datos

Leyes Estatales Integrales de Privacidad de Datos

Los siguientes 16 estados de EE. UU. han adoptado leyes integrales de privacidad de datos. Estas leyes otorgan derechos a los consumidores, como el derecho a acceder, corregir inexactitudes, eliminar, obtener una copia de sus datos personales, y optar por no permitir el procesamiento de dichos datos por parte de entidades que no estén cubiertas por leyes sectoriales específicas. También imponen obligaciones a los controladores, como la obligación de brindar protección razonable de los datos y un propósito razonable en su procesamiento.

Kentucky: H. B. 15, Ley de Protección de Datos del Consumidor de Kentucky

- **Resumen:** Esta es una ley integral de privacidad de datos. No otorga derecho de acción privada.
- **Estado:** Firmada por el gobernador el 4 de abril de 2024. Fecha de vigencia: 1 de enero de 2026.
- **Enlace:** https://apps.legislature.ky.gov/record/24RS/hb15.html

---

New Hampshire: S. B. 255, Expectativa del Consumidor de Privacidad

- **Resumen:** Esta es una ley integral de privacidad de datos. No otorga derecho de acción privada.
- **Estado:** Firmada por el gobernador el 6 de marzo de 2024. Fecha de vigencia: 1 de enero de 2025.
- **Enlace:** https://gencourt.state.nh.us/bill_status/billinfo.aspx?id=865&inflect=1

New Jersey: S. 332, Ley sobre Sitios Web Comerciales, Consumidores e Información Personalmente Identificable

- **Resumen:** Esta es una ley integral de privacidad de datos. No otorga derecho de acción privada.
- **Estado:** Firmada por el gobernador el 16 de enero de 2024. Fecha de vigencia: 16 de enero de 2025.
- **Enlace:** https://www.njleg.state.nj.us/bill-search/2022/S332

Delaware: H. B. 154, Ley de Privacidad de Datos Personales de Delaware

- **Resumen:** Esta es una ley integral de privacidad de datos. No otorga derecho de acción privada.
- **Estado:** Fecha de vigencia: 1 de enero de 2025.
- **Enlace:** https://legis.delaware.gov/BillDetail/140388

Oregon: S. B. 619, Relativa a la Protección de Datos Personales de los Consumidores

- **Resumen:** Esta es una ley integral de privacidad de datos. No otorga derecho de acción privada.
- **Estado:** Firmada por el gobernador el 18 de julio de 2023. Fecha de vigencia: 1 de julio de 2024.
- **Enlace:** https://olis.oregonlegislature.gov/liz/2023R1/Measures/Overview/SB619

Texas: H. B. 4, Ley de Privacidad y Seguridad de Datos de Texas

- **Resumen:** Esta es una ley integral de privacidad de datos. No otorga derecho de acción privada.
- **Estado:** Firmada por el gobernador el 18 de julio de 2023. Fecha de vigencia: 1 de julio de 2024.
- **Enlace:** https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB4

Florida: S. B. 262, Declaración de Derechos Digitales de Florida

- **Resumen:** Algunos no la consideran una ley integral de privacidad de datos debido a su alcance limitado por la definición de "controlador"; sin embargo, otorga los mismos derechos a los consumidores y responsabilidades a los controladores. Aplica solo si el controlador es una entidad con fines de lucro que genera más de $1,000 millones de ingresos anuales y cumple ciertos criterios adicionales. No otorga derecho de acción privada.
- **Estado:** Firmada por el gobernador el 6 de junio de 2023. Fecha de vigencia: 1 de julio de 2024.
- **Enlace:** https://www.flsenate.gov/Session/Bill/2023/262/

Montana: S. B. 384, Ley de Privacidad de Datos del Consumidor

- **Resumen:** Esta es una ley integral de privacidad de datos. No otorga derecho de acción privada.
- **Estado:** Firmada por el gobernador el 19 de mayo de 2023. Fecha de vigencia: 1 de octubre de 2024.
- **Enlace:** https://leg.mt.gov/bills/2023/billpdf/SB0384.pdf

Tennessee: H. B. 1181, Ley de Protección de Información de Tennessee

- **Resumen:** Esta es una ley integral de privacidad de datos. No otorga derecho de acción privada.
- **Estado:** Firmada por el gobernador el 11 de mayo de 2023. Fecha de vigencia: 1 de julio de 2025.
- **Enlace:** https://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=HB1181

Indiana: S. B. 5, Protección de Datos del Consumidor

- **Resumen:** Esta es una ley integral de privacidad de datos. No otorga derecho de acción privada.
- **Estado:** Firmada por el gobernador el 1 de mayo de 2023. Fecha de vigencia: 1 de enero de 2026.
- **Enlace:** https://iga.in.gov/legislative/2023/bills/senate/5

Iowa: S. F. 262, Ley de Protección de Datos del Consumidor

- **Resumen:** Esta es una ley integral de privacidad de datos. No otorga derecho de acción privada.
- **Estado:** Firmada por el gobernador el 28 de marzo de 2023. Fecha de vigencia: 1 de enero de 2025.
- **Enlace:** https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=sf262

Connecticut: S. B. 6: Ley sobre la Privacidad de Datos Personales y la Supervisión en Línea

- **Resumen:** Antes de la entrada en vigor de esta ley, Connecticut ya contaba con una ley integral de privacidad de datos que otorgaba derechos a los consumidores e imponía responsabilidades a los controladores respecto a los datos de salud.
- **Estado:** Firmada por el gobernador el 10 de mayo de 2022. Fecha de vigencia: 1 de enero de 2023.
- **Enlace:** https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF

Utah: S. B. 227, Ley de Privacidad del Consumidor

- **Resumen:** Esta es una ley integral de privacidad de datos. No otorga derecho de acción privada.
- **Estado:** Firmada por el gobernador el 24 de marzo de 2022. Fecha de vigencia: 31 de diciembre de 2023.
- **Enlace:** https://le.utah.gov/~2022/bills/static/SB0227.html

Colorado: S. B. 21-190, Ley de Privacidad de Colorado

- **Resumen:** Esta es una ley integral de privacidad de datos. No otorga derecho de acción privada.
- **Estado:** Firmada por el gobernador el 7 de julio de 2021. Fecha de vigencia: 1 de julio de 2023.
- **Enlace:** https://leg.colorado.gov/bills/sb21-190

Virginia: Ley de Protección de Datos del Consumidor

- **Resumen:** Esta es una ley integral de privacidad de datos. No otorga derecho de acción privada.
- **Estado:** Fecha de vigencia: 1 de enero de 2023.
- **Enlace:** https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

California: Ley de Privacidad del Consumidor de California (CCPA), enmendada por la Ley de Derechos de Privacidad de California (CPRA)

- **Resumen:** La CCPA otorgó muchos de los derechos y requisitos de una ley integral de privacidad de datos y fue enmendada por la CPRA para ser completamente integral, incluyendo disposiciones como el derecho a corregir inexactitudes en los datos personales recopilados. Esta ley no otorga derecho de acción privada.
- **Estado:** CCPA (vigente desde el 1 de enero de 2020), CPRA (totalmente vigente desde el 1 de enero de 2023).
- **Enlace:** https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Leyes Estatales de Privacidad de Datos de Salud

Además, los siguientes tres estados han aprobado leyes de privacidad de datos que solo aplican a datos de salud. Estas leyes otorgan derechos similares a los consumidores y responsabilidades similares a los controladores, como las leyes integrales, pero se limitan al sector salud. Estas leyes también prohíben a los controladores vender datos de salud y requieren obtener consentimiento para recopilarlos.

Connecticut: : S. B. 3, Ley sobre Privacidad en Línea, Datos y Protecciones de Seguridad

- **Resumen:** Antes de la entrada en vigor de esta ley, Connecticut ya tenía una ley integral de privacidad que otorgaba derechos y responsabilidades relacionados con datos de salud. Esta ley agrega únicamente disposiciones específicas de privacidad de datos de salud que no estaban incluidas en la ley integral, como la prohibición de vender datos de salud y el requisito de consentimiento para su recopilación.
- **Estado:** Firmada por el gobernador el 26 de junio de 2023. Fecha de vigencia: 1 de julio de 2023.
- **Enlace:** https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00003&which_year=2023

Nevada: S. B. 370, Ley de Privacidad de Datos de Salud

- **Resumen:** Esta es una ley de privacidad de datos de salud.
- **Estado:** Firmada por el gobernador el 15 de junio de 2023. Fecha de vigencia: 31 de marzo de 2024.
- **Enlace:** https://www.leg.state.nv.us/App/NELIS/REL/82nd2023/Bill/10323/Overview

---

Washington: H. B. 1155, Ley "Mi Salud, Mis Datos" del Estado de Washington

- **Resumen:** Esta es una ley de privacidad de datos de salud.
- **Estado:** Firmada por el gobernador el 27 de abril de 2023. Fecha de vigencia: 23 de julio de 2023.
- **Enlace:** https://app.leg.wa.gov/billsummary?BillNumber=1155&Year=2023&Initiative=false

APÉNDICE C

Estados que Lideran el Camino hacia una Ciberseguridad Razonable

Varios estados han promulgado leyes que proporcionan una manera de identificar una seguridad razonable. Los siguientes cinco estados han aprobado estatutos que incentivan la adopción voluntaria de mejores prácticas de ciberseguridad mediante la creación de un puerto seguro (safe harbor) para las organizaciones que adopten uno de varios estándares de la industria, como los Controles Críticos de Seguridad del CIS (CIS Critical Security Controls). Estos estados incluyen:

Iowa: Defensas Afirmativas para Entidades que Usan Programas de Ciberseguridad

- **Resumen:** Incentiva la adopción voluntaria de mejores prácticas de ciberseguridad, incluidos los Controles Críticos de Seguridad del CIS, al crear defensas afirmativas en demandas resultantes de una violación de datos.
- **Estado:** Fecha de vigencia: 1 de julio de 2023.
- **Enlace:** Código de Iowa, Título XIII (Comercio), Capítulo 554G (Responsabilidad Civil—Programas de Ciberseguridad): https://www.legis.iowa.gov/law/iowaCode/sections?codeChapter=554G&year=2024

Connecticut: Ley para Incentivar la Adopción de Estándares de Ciberseguridad para Empresas

- **Resumen:** Incentiva la adopción voluntaria de mejores prácticas de ciberseguridad, incluidos los Controles Críticos de Seguridad del CIS, al establecer un límite a los daños punitivos en demandas resultantes de una violación de datos.
- **Estado:** : Fecha de vigencia: 1 de octubre de 2021.
- **Enlace:** Ley Pública N.º 21-119: https://www.cga.ct.gov/2021/ACT/PA/PDF/2021PA-00119-R00HB-06607-PA.PDF

Utah: Ley de Defensa Afirmativa de Ciberseguridad

- **Resumen:** Incentiva la adopción voluntaria de mejores prácticas de ciberseguridad, incluidos los Controles Críticos de Seguridad del CIS, al crear una defensa afirmativa contra demandas resultantes de una violación de datos.
- **Estado:** Fecha de vigencia: 5 de mayo de 2021.
- **Enlace:** Código de Utah, Título 78B (Código Judicial), Capítulo 4 (Limitaciones de Responsabilidad), Parte 7 (Ley de Defensa Afirmativa de Ciberseguridad): https://le.utah.gov/xcode/Title78B/Chapter4/C78B-4-P7_2021050520210505.pdf

Nevada: Uso Estatal de "Medidas de Seguridad Razonables" para Proteger la Información Personal Identificable (PII)

- **Resumen:** Requiere que los recopiladores de datos estatales cumplan con los Controles Críticos de Seguridad del CIS o con el Marco de Ciberseguridad del NIST en relación con la recopilación, difusión y mantenimiento de registros que contengan información personal de un residente de Nevada.
- **Estado:** Fecha de vigencia: 1 de enero de 2021.
- **Enlace:** : S.B. 302, Capítulo 412: https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6534/Overview

Ohio: Ley de Protección de Datos

- **Resumen:** Incentiva la adopción voluntaria de mejores prácticas de ciberseguridad, incluidos los Controles Críticos de Seguridad del CIS, al crear una defensa afirmativa contra demandas resultantes de una violación de datos.
- **Estado:** Fecha de vigencia: 1 de noviembre de 2018.
- **Enlace:** Proyecto de Ley del Senado 220, codificado en O.R.C. §§ 1354.01-1354.05: http://codes.ohio.gov/orc/1354

APÉNDICE D

Por qué los Controles de Seguridad Críticos del CIS se están convirtiendo en un estándar global de facto

Si bien existen algunos estándares limitados de políticas (por ejemplo, NIST CSF) y estándares de la industria o de datos (como PCI, HIPAA e ISO), no hay estándares operacionales específicos que abarquen todos los sectores económicos. Los Controles de Seguridad Críticos del CIS se están convirtiendo en el estándar razonable de facto a nivel global para la ciberseguridad operacional por seis razones contundentes.

1 **Prescriptivos y priorizados por expertos globales.** Los Controles del CIS, los cuales son compilados regularmente por expertos en ciberseguridad de todo el mundo, ayudan a implementar los objetivos del NIST CSF proporcionando un plan para que los operadores de red mejoren su ciberseguridad mediante acciones específicas, prescriptivas y en orden de prioridad, basadas en el estado actual de las amenazas cibernéticas globales. Mientras que el NIST CSF define el qué — es decir, las categorías de la ciberseguridad y una visión organizacional de la gestión del riesgo de seguridad—, los Controles del CIS se basan en cómo atacan los actores maliciosos y se actualizan regularmente. El resultado es la hoja de ruta más clara y definitiva sobre cómo proteger a una organización contra ciberataques.

2 **Extremadamente efectivos y medibles.** Los Controles del CIS son muy eficaces frente a los vectores de ataque más frecuentes en la actualidad, y esta eficacia ha sido cuantificada. El Modelo de Defensa Comunitaria (CDM) de CIS establece que los Controles del CIS mitigan aproximadamente el 86% de las técnicas de ataque identificadas en el Marco MITRE ATT&CK.[25]

3 **Escalables.** Los Controles del CIS pueden adaptarse según el tamaño de la organización que los implemente. Introducen el concepto de Grupos de Implementación (IGs), los cuales proporcionan tanto un punto de partida para organizaciones que recién comienzan, como una hoja de ruta hacia una mayor madurez en defensa cibernética mediante tres niveles. Estos IGs adaptan los controles al tamaño y madurez de la organización. Incluso en el nivel más básico, IG1, los Controles del CIS siguen siendo muy eficaces, protegiendo contra el 74% de los vectores de ataque identificados en el modelo MITRE ATT&CK.[26]

4 **Rentables.** Reconociendo que el costo de implementación es una gran incógnita en los programas de seguridad (especialmente para pequeñas y medianas empresas), CIS ha desarrollado herramientas, modelos y ayudas prácticas para ayudar a las organizaciones a comprender y gestionar el costo de su programa de ciberseguridad. Por ejemplo, el CDM establece el "valor en seguridad" de prácticas individuales,[27] lo cual ayuda a establecer prioridades y a delimitar la cuestión del costo a prácticas y herramientas específicas. También ayuda a las organizaciones a establecer el valor base de las tecnologías y prácticas que ya poseen. Además, CIS ha publicado un estudio que establece cuánto le costará a una organización implementar una ciberseguridad eficaz.[28]

5 **Mapeados con otros marcos globales de políticas y datos.** Los Controles del CIS están mapeados con muchos marcos existentes.[29] Muchas organizaciones deben reportar avances respecto a múltiples marcos o conjuntos de requisitos de seguridad, por lo que CIS desarrolla mapeos disponibles gratuitamente y validados por la industria, que conectan los productos de CIS con todos los marcos de seguridad principales (como el NIST CSF, NIST 800-53, PCI, etc.). Este mapeo de marcos también se encuentra disponible en el Apéndice F .

6 **Adoptados ampliamente a nivel global.**

- Los Controles de Seguridad Críticos del CIS han sido descargados más de 400,000 veces en los últimos años—más de la mitad por organizaciones fuera de los EE. UU.
- Adopciones y respaldos seleccionados de los Controles de Seguridad Críticos del CIS incluyen:
  - **NIST, "Framework for Improving Critical Infrastructure Cybersecurity Framework," Versión 1.1, 16 de abril de 2018.** Cita y mapea los "CIS CSC" a lo largo del Apéndice A, Framework Core de la página 22 a la 44. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
  - **Verizon, "DBIR Data Breach Investigations Report," 2024.** Recomienda los Controles del CIS y los relaciona con los desafíos y vulnerabilidades de la industria. https://www.verizon.com/business/resources/reports/dbir/
  - **National Aerospace Standard, NAS9933, "Controles de Seguridad Críticos para una Capacidad Eficaz en Defensa Cibernética", 29 de noviembre de 2018.** Basado en los Controles del CIS. https://store.accuristech.com/searches/41316943
  - **Federal Financial Institutions Examination Council, "FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness," 28 de agosto de 2019.** Recomienda los Controles de Seguridad Críticos como una de cuatro herramientas específicas. https://www.ffiec.gov/press/pr082819.htm
  - **Conference of State Bank Supervisors, "Cybersecurity 101, A Resource Guide for Bank Executives," 2017.** Recomienda el uso de los Controles de Seguridad Críticos en las páginas 8, 12 y 24. https://www.csbs.org/sites/default/files/cybersecurity101_2019_final_with_links.pdf
  - **FCC Notice of Proposed Rule Making, dic 2022-ene 2023:** La FCC propone medidas para proteger los sistemas de comunicaciones críticos de la nación contra amenazas cibernéticas adoptando la Línea Base de Ciberseguridad de CISA o los Controles del CIS. FCC NPRM, No.

22-82, Apéndice B, Sección E, párrafo 66, página 52. https://www.fcc.gov/document/fcc-acts-strengthen-security-nations-alerting-systems

- **FCC, CSRIC IV, WG3, "Emergency Alert System (EAS) Initial Security Subcommittee Report," mayo 2014.** Recomienda los Controles del CIS (entonces conocidos como "SANS 20 Controles de Seguridad Críticos"). https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-3_Initial-Report_061814.pdf
- **FCC, CSRIC III, WG11, "Consensus Cyber Security Controls Final Report," marzo 2013.** El informe señala que los miembros del grupo de usuarios prefieren que la FCC incentive el uso de los 20 Controles, por su eficacia para proteger la infraestructura crítica. https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG11_Report_March_%202013Final.pdf
- **NIST, U.S. Resilience Project, "Best Practices in Cyber Supply Chain Risk Management."** El equipo IS de Boeing afirmó que su "estándar principal son los Controles de Seguridad Críticos." https://www.nist.gov/system/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf
- **U.S. Department of Transportation, FHWA, "Transportation Management Center IT Security, Final Report," sep. 2019.** Cita los Controles del CIS como guía inicial para organizaciones con recursos y experiencia limitados. https://ops.fhwa.dot.gov/publications/fhwahop19059/fhwahop19059.pdf
- **Estado de California, "California Data Breach Report," feb. 2016.** El informe de la Fiscal General Kamala Harris advierte que no implementar los Controles relevantes constituye una falta de seguridad razonable. https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf . Análisis posterior cita el respaldo de los Controles como seguridad razonable: https://www.littler.com/publication-press/publication/employers-receive-last-minute-reprieve-most-onerous-ccpa-compliance?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original
- **Estado de Colorado, "Data Security Best Practices."** La guía del Fiscal General de Colorado recomienda los Controles del CIS como parte del paso 2: la política escrita de seguridad de la información. https://coag.gov/app/uploads/2022/01/Data-Security-Best-Practices.pdf
- **Foro Económico Mundial (WEF), "Global Agenda Council on Cybersecurity, White Paper," abril 2016.** Enumera los Controles del CIS como la primera práctica recomendada en la página 19 y como higiene cibernética en el Apéndice A, página 26. http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf
- **ENISA, "Technical Guidelines for the implementation of minimum security measures for Digital Service Providers," dic. 2016.** Cita los Controles del CIS como medio para cumplir la Directiva NIS (2016/1148) de la UE. https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/
- **ETSI (Instituto Europeo de Normas de Telecomunicaciones)** ETSI transcribió todos los Controles del CIS y mecanismos asociados en especificaciones internacionales. Estos

Controles fueron designados como el medio para implementar gran parte de las disposiciones de la NIS2 revisada de la UE.

- ETSI TR 103 305-1: https://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/04.01.02_60/tr_10330501v040102p.pdf
- ETSI TR 103 305-3: https://www.etsi.org/deliver/etsi_tr/103300_103399/10330503/02.01.01_60/tr_10330503v020101p.pdf
- ETSI TR 103 305-4: https://www.etsi.org/deliver/etsi_tr/103300_103399/10330504/02.01.01_60/tr_10330504v020101p.pdf
- ETSI TR 103 305-5: https://www.etsi.org/deliver/etsi_tr/103300_103399/10330505/02.01.01_60/tr_10330505v020101p.pdf
- ETSI TR 103 456: https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf
- ETSI TR 103 866: https://www.etsi.org/deliver/etsi_tr/103800_103899/103866/01.01.01_60/tr_103866v010101p.pdf

APÉNDICE E

Historial de Caso: Un Fabricante de Productos Ligeros con Sede en EE. UU

Identidad de la empresa reservada

La eficiencia, el servicio y la gestión inteligente del riesgo son fundamentales en el sector de la fabricación de productos ligeros. Las prácticas modernas requieren la integración de datos de clientes, incluyendo diseños, especificaciones de productos e identificadores de clientes. Una gobernanza de la información robusta es crucial para la seguridad y un buen servicio al cliente.

Este historial de caso destaca una empresa real de fabricación ligera en los Estados Unidos, los desafíos de seguridad de datos que enfrentaba y su adopción de los Controles CIS como solución continua.

Resumen de la Empresa (Anonyco, Inc.)

Para preservar la seguridad y la confidencialidad, la empresa será referida en este documento como Anonyco, un seudónimo. Anonyco es una operación de empresa a empresa ubicada en el suroeste de Estados Unidos, en una ciudad con una población superior al millón de habitantes. Sus clientes son entidades de empresa a consumidor en una amplia variedad de categorías.

En un momento dado, Anonyco tendrá entre 10 y 20 empleados. Tres están en funciones gerenciales, incluyendo al propietario y presidente de la empresa. El resto está en producción. Al menos un empleado trabaja desde casa. Hay una recepcionista que interactúa con clientes y personal de entregas.

Cabe destacar que el presidente de la empresa es un gerente sofisticado, y no un neófito tecnológico, teniendo al menos cierta experiencia en codificación y diseño de software. Este detalle es significativo porque la experiencia nos dice que a menudo no hay correlación entre la competencia empresarial y una buena gobernanza de la información.

Durante un período de dos a tres años, Anonyco experimentó una serie de eventos derivados de accesos no autorizados aparentes. En un evento particularmente costoso, un exempleado con acceso a datos de clientes consiguió un trabajo con un competidor de Anonyco, captando un cliente con un valor potencial a largo plazo de siete cifras.

Utilizando conocimiento sobre Anonyco y sus operaciones internas, el exempleado obtuvo acceso remoto a un sistema en las instalaciones de Anonyco. Fingiendo seguir siendo empleado de

Anonyco, interactuó con clientes. El contrato de siete cifras fue negociado (aparentemente en nombre de Anonyco) y aprobado, pero en el último momento el negocio fue referido al competidor donde el exempleado ahora trabajaba. Este incidente es un ejemplo ingenioso de acceso malicioso no autorizado, pero se omiten más detalles aquí por razones de seguridad empresarial.

Después de recibir una pista, el presidente de Anonyco revisó los registros de eventos y confirmó accesos no autorizados repetidos al sistema. Aún afectado por este golpe, continuó preocupado por la exposición de datos, interrupciones del negocio y pérdida de ingresos. El punto de inflexión llegó cuando la reputación de Anonyco creció y comenzó a negociar con industrias fuertemente reguladas bajo supervisión de agencias estatales y/o federales. Los requisitos de cumplimiento de los clientes incluían mandatos de seguridad de datos. Esto generó preocupaciones sobre la responsabilidad legal, y un reconocimiento por parte de Anonyco de que los descuidos en seguridad de datos podrían conllevar litigios costosos.

Riesgos de Gobernanza de la Información en la Fabricación Ligera

En el mundo interconectado de la fabricación moderna, existe una convergencia de tecnologías operativas, inteligencia artificial, internet de las cosas y una variedad de otras tecnologías de la información. El riesgo derivado de una mala gobernanza de la información es considerable. Una mala gobernanza puede provocar interrupciones en la producción y serios retrasos en las entregas a clientes. Existen riesgos básicos relacionados con datos sensibles de clientes y empleados, así como con las transacciones financieras de la empresa.

El riesgo legal es una consecuencia de una gestión de la información deficiente que a menudo se pasa por alto. Las pequeñas empresas rara vez contemplan el papel de la información almacenada—especialmente la información digital—en la defensa legal. Una mala gestión de la información complica enormemente el descubrimiento legal (eDiscovery), reduciendo la posibilidad de una defensa sólida e incrementando el tiempo y los costos de representación legal.

Introducción de Anonyco a los Controles CIS

La decisión de Anonyco de adoptar los Controles CIS surgió del deseo de establecer un marco integral de gobernanza de la información y ciberseguridad. Tras una discusión, la dirección de Anonyco entendió que los Controles CIS proporcionan un enfoque práctico y priorizado para fortalecer defensas, gestionar vulnerabilidades, responder eficazmente a incidentes cibernéticos y reducir los costos asociados con litigios y cumplimiento regulatorio.

La implementación de CIS por parte de Anonyco comenzó con una evaluación de riesgos, la cual reveló vulnerabilidades significativas, tales como:

- Configuraciones de red incorrectas
- Procesos de recursos humanos inadecuados, incluyendo incorporación y desvinculación, y capacitación en seguridad
- Acceso remoto no autorizado

- Políticas de autenticación inadecuadas
- Seguridad de correo electrónico deficiente

Durante varios meses, Anonyco procedió de la siguiente manera. Todas las medidas tomadas aumentan la seguridad y fortalecen proactivamente una defensa efectiva en caso de litigios:

1 **Inventario y Control de Activos de Información de Hardware.** La empresa comenzó catalogando y monitoreando minuciosamente todos los activos de hardware conectados a la red. Este paso brinda visibilidad a la infraestructura, reduciendo el riesgo de que dispositivos no autorizados comprometan datos u otros sistemas.

2 **Configuración Segura de Hardware y Software.** Siguiendo los principios de configuración segura establecidos por CIS, todos los componentes de hardware y software fueron configurados para la seguridad. Esto mitiga el riesgo de explotación cibernética debido a configuraciones incorrectas.

3 **Uso Controlado de Privilegios Administrativos.** Se priorizó restringir el acceso a sistemas e información sensibles mediante privilegios administrativos controlados. Este principio ayuda a prevenir accesos no autorizados y reduce la probabilidad de amenazas internas.

4 **Protección de Datos.** Los Controles CIS guían los esfuerzos para implementar medidas robustas de protección de datos. Se emplean cifrado, controles de acceso y respaldos de datos regulares para proteger la información crítica contra el acceso no autorizado, la pérdida de datos y la pérdida de integridad.

5 **Evaluación Continua de Vulnerabilidades.** Se están realizando evaluaciones regulares para identificar y abordar debilidades potenciales. Este enfoque proactivo ayuda a anticipar amenazas cibernéticas, minimizando el riesgo de explotación. Identificar vulnerabilidades también ayuda a proteger la integridad de los datos: la capacidad de confiar en la exactitud de los datos del negocio.

6 **Protección de Correo Electrónico y Navegadores Web.** Las protecciones de correo electrónico y navegadores web conformes a CIS reducen el riesgo de que los empleados sean víctimas de enlaces o archivos adjuntos maliciosos. El proceso incluye capacitación de usuarios y mecanismos fuertes de filtrado.

7 **Las actividades de correo electrónico e internet se usan frecuentemente como evidencia durante litigios.** Estas medidas ayudan a garantizar la integridad del correo electrónico cuando se producen litigios.

8 **Defensa Perimetral.** Una estrategia de defensa perimetral robusta monitorea y controla el tráfico de red entrante y saliente. Los Controles CIS promueven el establecimiento y monitoreo de perímetros de red para proteger el tráfico, evitando accesos no autorizados y amenazas potenciales.

9 **Respuesta y Gestión de Incidentes.** Anonyco ha desarrollado un plan de respuesta a incidentes alineado con los Controles CIS. El plan incluye procedimientos para detectar, responder y recuperarse de incidentes de ciberseguridad.

10 **Capacidades de Recuperación de Datos.** Anonyco ahora prueba regularmente sus capacidades de recuperación de datos, según las recomendaciones de CIS, para asegurar que las operaciones puedan reanudarse rápidamente con mínima interrupción.

11 **Capacitación en Seguridad de la Información.** Anonyco ha realizado y continuará realizando capacitaciones. Los Controles CIS enfatizan educar a las personas para que se conviertan en cortafuegos humanos contra los riesgos. Esto incluye capacitar al personal para usar sus habilidades cognitivas para reconocer y mitigar riesgos, practicar conductas seguras y fomentar una cultura de vigilancia y reducción de riesgos.

Cabe señalar que el personal de Anonyco mostró entusiasmo por la capacitación inicial, la cual se realizó durante un almuerzo organizado por la empresa. El personal hizo muchas buenas preguntas y se mostró complacido de contar con una ruta clara a seguir.

Conclusión

Al gobernar proactivamente los datos, abordar vulnerabilidades potenciales y estar consciente de las responsabilidades legales y regulatorias, Anonyco está mejor posicionado para crecer sirviendo a sus clientes. La implementación estratégica de los Controles CIS ha fortalecido las defensas de ciberseguridad de la empresa e instaurado una cultura de vigilancia y reducción de riesgos.

APÉNDICE F

Mapeo de Marcos de Referencia

Los Controles del CIS están mapeados con muchos marcos de referencia existentes. Muchas organizaciones deben reportar avances conforme a múltiples marcos de seguridad o conjuntos de requisitos. El CIS desarrolla mapeos, disponibles gratuitamente y validados por la industria, entre productos del CIS y todos los principales marcos de seguridad, incluyendo:

- "Essential Eight" de la Dirección de Señales de Australia (Australian Signals Directorate)
- Objetivos de Desempeño en Ciberseguridad Intersectoriales (CPGs) de CISA
- CMMC v2.0 (Modelo de Madurez de Ciberseguridad)
- Servicios de Información de Justicia Penal (CJIS)
- Matriz de Control en la Nube de la Cloud Security Alliance (CSA)
- Perfil del Instituto de Riesgos Cibernéticos (Cyber Risk Institute – CRI)
- Herramienta de Evaluación de Ciberseguridad del FFIEC (FFIEC CAT)
- Controles de Seguridad Básicos GSMA FS.31
- HIPAA (Ley de Portabilidad y Responsabilidad de Seguros de Salud)
- Objetivos de Desempeño en Ciberseguridad del Sector Salud Pública y Salud de HHS (HPH CPGs)
- ISACA COBIT 19
- ISO 27001:2022
- ISO/IEC 27002:2022
- Referencia de Seguridad de Microsoft (Microsoft Security Benchmark)
- MITRE ATT&CK v8.2
- NERC-CIP (Normas de Protección de Infraestructura Crítica de la Corporación de Confiabilidad Eléctrica de América del Norte)
- Manual de Seguridad de la Información de Nueva Zelanda
- Marco de Ciberseguridad del NIST (NIST CSF) versión 1.0
- Marco de Ciberseguridad del NIST (NIST CSF) versión 2.0
- NIST 800-53 Revisión 5
- NIST SP 800-171 Revisión 2
- Reglamento 23 NYCRR Parte 500 del Departamento de Servicios Financieros del Estado de Nueva York (NYS DFS)
- PCI DSS (Norma de Seguridad de Datos de la Industria de Tarjetas de Pago)
- SOC 2 (Controles de Organización de Servicios)
- Directiva de Seguridad de Oleoductos de la TSA
- Cyber Essentials v2.2 del Reino Unido
- Marco de Evaluación de Ciberseguridad (CAF) v3.1 del NCSC del Reino Unido

Details for the full list can be seen at this link under the tab titled "Mappings": https://www.cisecurity.org/controls/cis-controls-navigator/

APÉNDICE G

Controles Críticos de Seguridad CIS Agrupados como Componentes de Sentido Común

Los Controles Críticos de Seguridad CIS que se amplían en el Apéndice H pueden resumirse en grupos lógicos: conocimiento del entorno; gestión de cuentas y configuraciones; herramientas de seguridad; recuperación de datos; concientización sobre seguridad; y procesos empresariales y tercerización.

Las organizaciones deben conocer su entorno. Específicamente, deben:

- Gestionar activamente (inventariar, rastrear y corregir) todos los activos empresariales (dispositivos de usuario final, incluidos portátiles y móviles; dispositivos de red; dispositivos que no son computadoras/dispositivos del Internet de las Cosas (IoT); y servidores) conectados a la infraestructura, ya sea de forma física, virtual, remota o en entornos en la nube, para conocer con precisión la totalidad de activos que necesitan ser monitoreados y protegidos dentro de la empresa. Esto también ayudará a identificar activos no autorizados y no gestionados para eliminarlos o remediarlos.
- Gestionar activamente (inventariar, rastrear y corregir) todo el software (sistemas operativos y aplicaciones) en la red, de modo que solo el software autorizado esté instalado y pueda ejecutarse, y que el software no autorizado y no gestionado sea detectado y se impida su instalación o ejecución.
- Desarrollar procesos y controles técnicos para identificar, clasificar, manejar de manera segura, conservar y eliminar datos.

Las organizaciones también deben llevar a cabo gestión de cuentas y configuraciones. Específicamente, deben:

- Establecer y mantener la configuración segura de los activos empresariales (dispositivos de usuario final, incluidos portátiles y móviles; dispositivos de red; dispositivos no computacionales/IoT; y servidores) y del software (sistemas operativos y aplicaciones).
- Utilizar procesos y herramientas para asignar y gestionar autorizaciones para las credenciales de cuentas de usuario, incluidas cuentas de administrador, así como cuentas de servicio, para activos empresariales y software.
- Utilizar procesos y herramientas para crear, asignar, gestionar y revocar credenciales de acceso y privilegios para cuentas de usuario, administrador y servicio en los activos empresariales y software.

- Desarrollar un plan para evaluar y rastrear continuamente vulnerabilidades en todos los activos empresariales dentro de la infraestructura de la empresa, con el fin de remediarlas y minimizar la ventana de oportunidad para los atacantes. Monitorear fuentes públicas y privadas de la industria para obtener nueva información sobre amenazas y vulnerabilidades.
- Recopilar, alertar, revisar y conservar registros de auditoría de eventos que puedan ayudar a detectar, comprender o recuperarse de un ataque.
- Establecer, implementar y gestionar activamente (rastrear, informar, corregir) los dispositivos de red, a fin de evitar que los atacantes exploten servicios de red vulnerables y puntos de acceso.
- Gestionar el ciclo de vida de seguridad del software desarrollado internamente, alojado o adquirido para prevenir, detectar y remediar debilidades de seguridad antes de que puedan afectar a la empresa.
- Utilizar herramientas de seguridad comerciales para protegerse contra ataques comunes, como intrusiones específicas o malware.
- Mejorar las protecciones y detecciones de amenazas provenientes del correo electrónico y vectores web, ya que representan oportunidades para que los atacantes manipulen el comportamiento humano mediante interacción directa.
- Prevenir o controlar la instalación, propagación y ejecución de aplicaciones, código o scripts maliciosos en los activos empresariales.
- Operar procesos y herramientas para establecer y mantener un monitoreo de red integral y una defensa contra amenazas de seguridad en toda la infraestructura de red de la empresa y su base de usuarios.

Las organizaciones deben establecer un plan de recuperación de datos para responder y recuperarse de un incidente. Específicamente, deben:

- Establecer y mantener prácticas de recuperación de datos suficientes para restaurar los activos empresariales dentro del alcance a un estado previo al incidente y de confianza.
- Establecer un programa para desarrollar y mantener una capacidad de respuesta ante incidentes (por ejemplo, políticas, planes, procedimientos, roles definidos, capacitación y comunicaciones) para prepararse, detectar y responder rápidamente a un ataque.
- Las organizaciones deben implementar un programa de concientización sobre seguridad. Específicamente, deben.
- Establecer y mantener un programa de concientización sobre seguridad para influir en el comportamiento del personal y desarrollar habilidades adecuadas para reducir los riesgos de ciberseguridad para la empresa.
- Probar la efectividad y resiliencia de los activos empresariales mediante la identificación y explotación de debilidades en los controles (personas, procesos y tecnología), y la simulación de los objetivos y acciones de un atacante.

Las organizaciones deben implementar procesos para evaluar y monitorear a los proveedores de servicios. Específicamente, deben:

- Desarrollar un proceso para evaluar a los proveedores de servicios que manejan datos sensibles o que son responsables de plataformas o procesos críticos de TI de la empresa, para asegurar que estos proveedores protejan adecuadamente dichas plataformas y datos.

APÉNDICE H

Implementación de los 153 Controles de Seguridad Críticos del CIS

Lo siguiente proporciona una implementación completa de los Controles de Seguridad Críticos del CIS, y de las acciones subyacentes que respaldan dichos Controles; es decir, una descripción de las actividades prescriptivas y priorizadas que las organizaciones deben llevar a cabo para defender su entorno empresarial.

La prioridad descrita a continuación se derivó mediante un proceso de consenso comunitario que aprovechó la experiencia de especialistas en ciberseguridad del ámbito académico, gubernamental y corporativo.

En orden de prioridad, las organizaciones deben implementar cada uno de los 18 Controles del CIS, comenzando con el Control CIS 1:

1. Gestionar activamente (inventariar, rastrear y corregir) todos los activos empresariales (dispositivos de usuario final, incluidos los portátiles y móviles; dispositivos de red; dispositivos no computacionales/Internet de las cosas (IoT); y servidores) conectados a la infraestructura, ya sea de forma física, virtual, remota o en entornos en la nube, para conocer con precisión la totalidad de los activos que deben ser monitoreados y protegidos dentro de la empresa. Esto también ayudará a identificar activos no autorizados y no gestionados para su eliminación o remediación.
2. Gestionar activamente (inventariar, rastrear y corregir) todo el software (sistemas operativos y aplicaciones) en la red para que solo se instale y ejecute software autorizado, y se detecte y evite la instalación o ejecución de software no autorizado o no gestionado.
3. Desarrollar procesos y controles técnicos para identificar, clasificar, manejar de forma segura, conservar y eliminar los datos.
4. Establecer y mantener la configuración segura de los activos empresariales (dispositivos de usuario final, incluidos los portátiles y móviles; dispositivos de red; dispositivos no computacionales/IoT; y servidores) y del software (sistemas operativos y aplicaciones).
5. Usar procesos y herramientas para asignar y gestionar la autorización de credenciales para cuentas de usuario, incluidas cuentas de administrador, así como cuentas de servicio, para activos empresariales y software.
6. Usar procesos y herramientas para crear, asignar, gestionar y revocar credenciales de acceso y privilegios para cuentas de usuario, administrador y servicio en activos empresariales y software.

7 Desarrollar un plan para evaluar y rastrear continuamente las vulnerabilidades en todos los activos empresariales dentro de la infraestructura de la organización, con el fin de remediar y minimizar la ventana de oportunidad para los atacantes. Monitorear fuentes de información públicas y del sector privado sobre nuevas amenazas y vulnerabilidades.

8 Recopilar, alertar, revisar y conservar los registros de auditoría de eventos que puedan ayudar a detectar, comprender o recuperarse de un ataque.

9 Mejorar la protección y detección de amenazas provenientes de vectores de correo electrónico y web, ya que estos representan oportunidades para que los atacantes manipulen el comportamiento humano mediante interacción directa.

10 Prevenir o controlar la instalación, propagación y ejecución de aplicaciones maliciosas, código o scripts en los activos empresariales.

11 Establecer y mantener prácticas de recuperación de datos que sean suficientes para restaurar los activos empresariales cubiertos al estado anterior al incidente y de confianza.

12 Establecer, implementar y gestionar activamente (es decir, rastrear, reportar y corregir) los dispositivos de red, para evitar que los atacantes exploten servicios de red y puntos de acceso vulnerables.

13 Operar procesos y herramientas para establecer y mantener un monitoreo integral de red y defensa contra amenazas de seguridad a través de la infraestructura de red de la organización y la base de usuarios.

14 Establecer y mantener un programa de concientización en seguridad para influir en el comportamiento del personal, fomentando una actitud consciente de la seguridad y habilidades adecuadas para reducir los riesgos de ciberseguridad en la organización.

15 Desarrollar un proceso para evaluar a los proveedores de servicios que manejan datos sensibles o son responsables de plataformas o procesos críticos de TI de la organización, para asegurar que estos proveedores protejan adecuadamente dichas plataformas y datos.

16 Gestionar el ciclo de vida de seguridad del software desarrollado internamente, alojado o adquirido, para prevenir, detectar y remediar debilidades de seguridad antes de que impacten a la organización.

17 Establecer un programa para desarrollar y mantener una capacidad de respuesta ante incidentes (por ejemplo, políticas, planes, procedimientos, roles definidos, capacitación y comunicaciones) para preparar, detectar y responder rápidamente ante un ataque.

18 Probar la eficacia y resiliencia de los activos empresariales mediante la identificación y explotación de debilidades en los controles (por ejemplo, personas, procesos y tecnología), y simulando los objetivos y acciones de un atacante.

Control 1: Inventario y Control de Activos Empresariales

Gestionar activamente (inventariar, rastrear y corregir) todos los activos empresariales (dispositivos de usuario final, incluidos los portátiles y móviles; dispositivos de red; dispositivos no computacionales/Internet de las Cosas (IoT); y servidores) conectados a la infraestructura, ya sea de forma física, virtual, remota, o en entornos en la nube, para conocer con precisión la totalidad de activos que deben ser monitoreados y protegidos dentro de la empresa. Esto también apoyará la identificación de activos no autorizados y no gestionados para su eliminación o corrección.

1.1 Establecer y mantener un inventario preciso, detallado y actualizado de todos los activos empresariales con el potencial de almacenar o procesar datos, incluyendo: dispositivos de usuario final (incluidos los portátiles y móviles), dispositivos de red, dispositivos no computacionales/IoT y servidores. Para los dispositivos móviles de usuario final, herramientas tipo MDM pueden apoyar este proceso, cuando sea apropiado. Este inventario incluye activos conectados a la infraestructura de manera física, virtual, remota y aquellos en entornos en la nube. Adicionalmente, incluye activos que se conectan regularmente a la infraestructura de red de la empresa, incluso si no están bajo control de la organización. Los pasos incluyen:

- Asegurar que el inventario registre la dirección de red (si es estática), dirección de hardware, nombre de la máquina, propietario del activo de datos, departamento correspondiente a cada activo, y si el activo ha sido aprobado para conectarse a la red.
- Revisar y actualizar el inventario de todos los activos empresariales de forma semestral, o con mayor frecuencia.

1.2 Asegurar que exista un proceso para abordar los activos no autorizados semanalmente. La empresa puede optar por eliminar el activo de la red, denegar su conexión remota a la red, o ponerlo en cuarentena. Los pasos incluyen:

- Después de crear una lista de activos aprobados, detectar los dispositivos no autorizados.
- Verificar si el activo no autorizado debe ser autorizado y actualizar el formulario de inventario de activos.
- En caso contrario, aplicar la política de: eliminar el activo de la red, denegar su conexión remota a la red o ponerlo en cuarentena.
- Abordar los activos no autorizados semanalmente.

1.3 Utilizar una herramienta de descubrimiento activo para identificar activos conectados a la red empresarial. Configurar la herramienta de descubrimiento activo para que se ejecute diariamente, o con mayor frecuencia. Los pasos incluyen:

- Crear una lista de herramientas de descubrimiento activo de la empresa.
- Ejecutar, al menos diariamente, la(s) herramienta(s) de descubrimiento activo.

- Agregar los activos autorizados a la lista de inventario de activos aprobados y actualizar según corresponda

1.4 Utilizar el registro DHCP en todos los servidores DHCP o herramientas de gestión de direcciones del Protocolo de Internet (IP) para actualizar el inventario de activos de la empresa. Revisar y utilizar los registros para actualizar el inventario de activos de la empresa semanalmente, o con mayor frecuencia. Los pasos incluyen:

- Utilizar el inventario de activos empresariales para crear una lista de servidores DHCP y CMDB.
- Para cada servidor DHCP, asegurar que el registro DHCP esté habilitado.
- Para cada servidor CMDB, asegurar que se utilicen los registros DHCP para actualizar las direcciones IP.
- Agregar los activos autorizados a la lista de inventario de activos aprobados y actualizar según corresponda

1.5 Utilizar una herramienta de descubrimiento pasivo para identificar activos conectados a la red empresarial. Revisar y utilizar los escaneos para actualizar el inventario de activos de la empresa al menos semanalmente, o con mayor frecuencia. Los pasos incluyen:

- Crear una lista de herramientas de descubrimiento pasivo de activos en uso por la organización. Para cada una, incluir la ubicación de la información de configuración de la herramienta y qué redes cubre.
- Para cada herramienta de descubrimiento pasivo de activos, asegurar que esté configurada correctamente.
- Asegurar que cada red en la empresa esté cubierta por una herramienta de descubrimiento pasivo de activos.
- Agregar los activos autorizados a la lista de inventario de activos aprobados y actualizar según corresponda.

Control 2: Inventario y Control de Activos de Software

Gestionar activamente (inventariar, rastrear y corregir) todo el software (sistemas operativos y aplicaciones) en la red para que solo el software autorizado esté instalado y pueda ejecutarse, y para que el software no autorizado y no gestionado sea detectado y se impida su instalación o ejecución.

2.1 Establecer y mantener un inventario detallado de todo el software licenciado instalado en los activos de la empresa. El inventario de software debe documentar el título, editor, fecha de instalación/uso inicial y propósito comercial de cada entrada; cuando sea apropiado, incluir el Localizador Uniforme de Recursos (URL), tienda(s) de aplicaciones, versión(es), mecanismo de implementación, fecha de desactivación y número de licencias. Revisar y actualizar el inventario de software semestralmente o con mayor frecuencia. Los pasos incluyen:

- Asegurar que el inventario de software documente el título, editor, fecha de instalación/uso inicial y propósito comercial de cada entrada; cuando sea apropiado, incluir el Localizador Uniforme de Recursos (URL), tienda(s) de aplicaciones, versión(es), mecanismo de implementación y fecha de desactivación.

2.2 Revisar y actualizar el inventario de software semestralmente o con mayor frecuencia. Asegurar que solo el software actualmente soportado esté designado como autorizado en el inventario de software para los activos de la empresa. Si un software no tiene soporte pero es necesario para el cumplimiento de la misión de la empresa, documentar una excepción que detalle los controles de mitigación y la aceptación del riesgo residual. Para cualquier software sin soporte y sin documentación de excepción, designarlo como no autorizado. Revisar la lista de software para verificar su soporte al menos mensualmente o con mayor frecuencia. Los pasos incluyen:

- Usar el inventario de activos de software y determinar si el software está "soportado" o "no soportado".
- Si el software está "no soportado", entonces documentar una excepción o designarlo como no autorizado y eliminarlo, según la política.

2.3 Abordar el software no autorizado. Asegurar que el software no autorizado sea eliminado de los activos empresariales o reciba una excepción documentada. Revisar mensualmente o con mayor frecuencia. Los pasos incluyen:

- Utilizando los inventarios de activos de la empresa y de software autorizado, la empresa debe definir un periodo para escanear los activos empresariales en busca de software.
- Cualquier software detectado que no esté en el inventario de software autorizado debe abordarse conforme a la política.
- Si es necesario, actualizar el inventario de software.
- Esto debe hacerse mensualmente o con mayor frecuencia.

2.4 Utilizar herramientas automatizadas de inventario de software, cuando sea posible, en toda la empresa para automatizar el descubrimiento y documentación del software instalado. Los pasos incluyen:

- Usar el inventario de activos de la empresa para identificar y enumerar los activos capaces de ejecutar herramientas automatizadas de inventario de software.

- Si un activo no puede soportar una herramienta de inventario de software, esto debe ser documentado.

2.5 Usar controles técnicos, como listas de permitidos (allowlisting) de aplicaciones, para asegurar que solo el software autorizado pueda ejecutarse o accederse. Reevaluar semestralmente o con mayor frecuencia. Los pasos incluyen:

- Identificar y enumerar los activos capaces de soportar software de listas de permitidos (algunos activos pueden no permitir la instalación de software de terceros o tener entornos restringidos que impidan el uso de software de listas de permitidos).
- Identificar todo el software de listas de permitidos autorizado dentro de la empresa.
- Identificar y documentar las configuraciones del software de listas de permitidos.
- Asegurar que el software de listas de permitidos esté configurado correctamente.
- Documentar los activos sin software de listas de permitidos.
- Reevaluar semestralmente o con mayor frecuencia.

2.6 Usar controles técnicos para asegurar que solo bibliotecas de software autorizadas, como archivos .dll, .ocx y .so específicos, estén permitidas para cargarse en un proceso del sistema. Bloquear la carga de bibliotecas no autorizadas en un proceso del sistema. Reevaluar semestralmente o con mayor frecuencia. Los pasos incluyen:

- Crear una lista de bibliotecas de software autorizadas.
- Identificar y enumerar el software de listas de permitidos correctamente configurado para permitir la carga de procesos de bibliotecas autorizadas.
- Identificar y enumerar el software de listas de permitidos configurado incorrectamente que permite la carga de procesos de bibliotecas no autorizadas.
- Actualizar las configuraciones según corresponda.
- Reevaluar semestralmente o con mayor frecuencia.

2.7 Usar controles técnicos, como firmas digitales y control de versiones, para asegurar que solo scripts autorizados, como archivos .ps1 y .py específicos, estén permitidos para ejecutarse. Bloquear la ejecución de scripts no autorizados. Reevaluar semestralmente o con mayor frecuencia. Los pasos incluyen:

- Crear una lista de scripts autorizados.
- Identificar y enumerar todo el software autorizado en la empresa capaz de ejecutar scripts, incluyendo software de listas de permitidos, aplicaciones cliente de correo electrónico y aplicaciones cliente web.
- Identificar las configuraciones aprobadas para todo el software identificado en el paso anterior.
- Asegurar que el software esté configurado correctamente para permitir la ejecución de scripts autorizados y firmados.
- Actualizar las configuraciones según corresponda.
- Reevaluar semestralmente o con mayor frecuencia.

Control 3: Protección de Datos

Desarrollar procesos y controles técnicos para identificar, clasificar, manejar de forma segura, retener y desechar los datos.

3.1 Establecer y mantener un proceso documentado de gestión de datos. En dicho proceso, abordar la sensibilidad de los datos, el propietario de los datos, el manejo de los datos, los límites de retención y los requisitos de eliminación, en función de los estándares de sensibilidad y retención de la empresa. Revisar y actualizar la documentación anualmente o cuando se produzcan cambios significativos en la empresa que puedan afectar esta salvaguarda. Los pasos incluyen:

- Crear un proceso para abordar la sensibilidad de los datos, el propietario de los datos, el manejo de los datos, los límites de retención y los requisitos de eliminación, en función de los estándares de sensibilidad y retención de la empresa.
- Revisar y actualizar la documentación anualmente o cuando se produzcan cambios significativos en la empresa que puedan afectar esta salvaguarda.

3.2 Establecer y mantener un inventario de datos basado en el proceso de gestión de datos de la empresa. Inventariar los datos sensibles, como mínimo. Revisar y actualizar el inventario anualmente, como mínimo, con prioridad en los datos sensibles. Los pasos incluyen:

- Enumerar e identificar los datos sensibles.
- Mapear los datos sensibles al esquema de datos de la organización y al activo empresarial donde se encuentran.
- Revisar y actualizar el inventario anualmente, como mínimo, con prioridad en los datos sensibles.

3.3 Configurar listas de control de acceso a datos en función de la necesidad de conocimiento del usuario. Aplicar listas de control de acceso a datos, también conocidas como permisos de acceso, a sistemas de archivos locales y remotos, bases de datos y aplicaciones. Los pasos incluyen:

- Utilizar el proceso documentado de gestión de datos como guía para mapear qué cuentas de usuario tienen acceso a los datos sensibles.
- Para cada activo empresarial que almacene datos sensibles, aplicar listas de control de acceso a datos, también conocidas como permisos de acceso, a sistemas de archivos locales y remotos, bases de datos y aplicaciones.

3.4 Retener los datos conforme al proceso documentado de gestión de datos de la empresa. La retención de datos debe incluir tanto plazos mínimos como máximos.

- Identificar y enumerar los tipos de datos sensibles con tasas de retención mínimas y máximas definidas.
- Identificar y enumerar los elementos del inventario que cumplen con los plazos de retención.
- Identificar y enumerar los elementos del inventario que no cumplen con los plazos de retención.
- Tomar medidas para cumplir con los requisitos de retención de datos.

3.5 Eliminar de forma segura los datos según lo establecido en el proceso documentado de gestión de datos de la empresa. Asegurar que el proceso y el método de eliminación sean proporcionales a la sensibilidad de los datos. Los pasos incluyen:

- Identificar y enumerar cada tipo de dato sensible con un método y proceso de eliminación definidos por el proceso de gestión de datos.
- Asegurar que todos los datos sensibles cumplan con los requisitos de eliminación.

3.6 Cifrar los datos en los dispositivos de usuario final que contengan datos sensibles. Los ejemplos de implementación pueden incluir Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

- Utilizar el inventario de activos de la empresa para identificar y enumerar los dispositivos de usuario final con datos sensibles.
- Identificar y enumerar los dispositivos de usuario final que tienen software de cifrado instalado.
- Identificar y enumerar los dispositivos de usuario final sin software de cifrado. Documentar las excepciones según sea necesario. De lo contrario, hacer que los dispositivos de usuario final cumplan con la política de datos.
- Para los dispositivos de usuario final que tienen software de cifrado, asegurar que dicho software esté configurado correctamente.

3.7 Establecer y mantener un esquema general de clasificación de datos para la empresa. Las organizaciones pueden usar etiquetas como "Sensible", "Confidencial" y "Público", y clasificar sus datos de acuerdo con estas etiquetas. Los pasos incluyen:

- Crear una clasificación de datos y aplicarla a los tipos de datos sensibles.
- Revisar y actualizar el esquema de clasificación anualmente o cuando se produzcan cambios significativos en la empresa que puedan afectar esta salvaguarda.

3.8 Documentar los flujos de datos. La documentación de flujos de datos incluye los flujos de datos de proveedores de servicios y debe basarse en el proceso de gestión de datos de la empresa. Revisar y actualizar la documentación anualmente o cuando se produzcan cambios significativos en la empresa que puedan afectar esta salvaguarda. Los pasos incluyen:

- Crear documentación que describa el flujo de datos propiedad de la empresa. La documentación debe incluir, como mínimo, los flujos de datos hacia empresas externas.
- Revisar y actualizar el esquema de clasificación anualmente o cuando se produzcan cambios significativos en la empresa que puedan afectar esta salvaguarda.

3.9 Cifrar los datos en medios removibles. Los pasos incluyen:

- Utilizar el inventario de activos de la empresa para identificar y enumerar los activos autorizados para soportar medios removibles.
- Utilizar el inventario de software autorizado para identificar el software de cifrado en los activos mencionados.
- Identificar y enumerar los activos sin software de cifrado instalado.
- Instalar software de cifrado donde sea posible en los activos identificados anteriormente. Documentar las excepciones.
- Asegurar que todos los activos identificados tengan software de cifrado configurado correctamente.

3.10 Cifrar los datos sensibles en tránsito. Los ejemplos de implementación pueden incluir Transport Layer Security (TLS) y Open Secure Shell (OpenSSH). Los pasos incluyen:

- Utilizando el inventario de datos sensibles, identificar los medios y componentes para cifrar los datos en tránsito.
- Asegurar que el software esté configurado correctamente y habilitar el cifrado seleccionado.

3.11 Cifrar los datos sensibles en reposo en servidores, aplicaciones y bases de datos. El cifrado a nivel de almacenamiento, también conocido como cifrado del lado del servidor, cumple con el requisito mínimo de esta salvaguarda. Métodos adicionales de cifrado pueden incluir el cifrado a nivel de aplicación, también conocido como cifrado del lado del cliente, donde el acceso al dispositivo(s) de almacenamiento de datos no permite el acceso a los datos en texto plano. Los pasos incluyen:

- Utilizar el inventario de software autorizado para identificar y enumerar todas las herramientas de cifrado que requieran sistemas de autenticación secundaria.
- Utilizar el inventario de activos de la empresa y el inventario de datos sensibles para identificar y enumerar todos los activos empresariales que almacenan datos sensibles.
- Asegurar que todos los activos con datos sensibles estén configurados correctamente para cifrar los datos en reposo.

3.12 Las organizaciones deben segmentar el procesamiento y almacenamiento de datos según la sensibilidad de los datos. No procesar datos sensibles en activos empresariales destinados a datos de menor sensibilidad. El nivel general de sensibilidad de un activo debe ser el nivel de sensibilidad más alto de los datos que almacena/procesa/transmite. Si un sistema contiene información sensible, ese activo debe ser tratado en consecuencia y debe estar adecuadamente separado de redes o segmentos de red que no necesiten acceder a ese tipo de información sensible. Los pasos incluyen:

- Utilizar el inventario de datos sensibles para identificar los activos que almacenan, procesan o transmiten datos sensibles.
- Utilizando los datos del paso anterior, identificar todas las redes/VLAN conectadas a los activos que almacenan, procesan o transmiten datos sensibles.
- Identificar y enumerar cualquier instancia de activos correctamente separados de redes menos sensibles.
- Identificar y enumerar cualquier instancia de activos incorrectamente separados de redes menos sensibles.
- Tomar medidas para asegurar la separación adecuada de los datos sensibles en los activos.

3.13 Implementar una herramienta automatizada, como una herramienta de Prevención de Pérdida de Datos (DLP) basada en host, para identificar todos los datos almacenados, procesados o transmitidos a través de los activos empresariales, incluidos aquellos ubicados en sitio o en un proveedor de servicios remoto, y actualizar el inventario de datos sensibles de la empresa. Los pasos incluyen:

- Utilizar el inventario de software autorizado para identificar y enumerar todo el software de prevención de pérdida de datos.
- Asegurar que cada activo empresarial que almacene, procese o transmita datos sensibles tenga software de prevención de pérdida de datos instalado.
- Asegurar que el software de prevención de pérdida de datos esté configurado correctamente.

3.14 Registrar el acceso a los datos sensibles, incluyendo la modificación y eliminación. Los pasos incluyen:

- Utilizar el inventario de software autorizado para identificar el software de registro autorizado.
- Asegurar que los activos empresariales que almacenan, procesan o transmiten datos sensibles tengan software de registro instalado.
- Asegurar que el software de registro esté configurado correctamente.

Control 4: Configuración Segura de los Activos Empresariales y el Software

Establecer y mantener la configuración segura de los activos empresariales (dispositivos de usuario final, incluidos los portátiles y móviles; dispositivos de red; dispositivos no computacionales/IoT; y servidores) y del software (sistemas operativos y aplicaciones).

4.1 Establecer y mantener un proceso documentado de configuración segura para los activos empresariales (dispositivos de usuario final, incluidos los portátiles y móviles, dispositivos no computacionales/IoT y servidores) y el software (sistemas operativos y aplicaciones). Los pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los dispositivos de usuario final, incluidos los portátiles y móviles, los dispositivos no computacionales/IoT y los servidores.
- Utilizar el inventario de software autorizado para identificar y enumerar el software instalado en los activos.
- Verificar si existe un estándar de configuración que pueda aplicarse al software instalado. Un estándar de configuración puede incluir lineamientos base reconocidos por la industria, como los puntos de referencia de CIS, las Guías de Implementación Técnica de Seguridad (STIG) de DISA, o las configuraciones base del gobierno de los Estados Unidos (USGCB).
- Aplicar los estándares de configuración cuando corresponda.
- Revisar y actualizar la documentación anualmente o cuando ocurran cambios significativos en la empresa que puedan afectar esta Salvaguarda.

4.2 Establecer y mantener un proceso de configuración segura para los dispositivos de red. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos de infraestructura de red.
- Utilizar el inventario de software autorizado para identificar y enumerar el software instalado en dichos activos de infraestructura de red.
- Verificar si existe un estándar de configuración que pueda aplicarse al software instalado. Un estándar de configuración puede incluir líneas base estándar de la industria como los benchmarks del CIS, las guías DISA STIGs o las líneas base de configuración del gobierno de EE. UU. (USGCB).
- Aplicar estándares de configuración cuando corresponda.
- Revisar y actualizar la documentación anualmente, o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

4.3 Configurar el bloqueo automático de sesión en los activos empresariales tras un período definido de inactividad. Para sistemas operativos de propósito general, el período no debe exceder 15 minutos. Para dispositivos móviles de usuario final, el período no debe exceder 2 minutos. Pasos incluyen:

- Identificar y enumerar los activos que soportan el bloqueo automático por inactividad.
- Para activos de computación general, asegurar que el bloqueo automático esté configurado correctamente (15 minutos o menos).
- Para activos móviles, asegurar que el bloqueo automático esté configurado correctamente (2 minutos o menos).

4.4 Implementar y gestionar un firewall en los servidores, cuando sea compatible. Ejemplos de implementación incluyen un firewall virtual, un firewall del sistema operativo o un agente firewall de terceros. Pasos incluyen:

- Identificar y enumerar los servidores capaces de alojar un firewall.
- Identificar y enumerar las aplicaciones capaces de alojar un firewall.
- Asegurar que los firewalls estén configurados correctamente utilizando estándares de configuración.

4.5 Implementar y gestionar un firewall basado en host o una herramienta de filtrado de puertos en los dispositivos de usuario final, con una regla predeterminada de denegación que bloquee todo el tráfico, excepto aquellos servicios y puertos explícitamente permitidos. Pasos incluyen:

- Identificar y enumerar los dispositivos de usuario final capaces de alojar un firewall o una regla de denegación.
- Utilizar estándares de configuración para asegurar que los firewalls o reglas de denegación estén correctamente configurados en los dispositivos de usuario final.

4.6 Gestionar de forma segura los activos y el software empresariales. Ejemplos de implementación incluyen la gestión de configuraciones mediante infraestructura como código (IaC) controlada por versiones y el acceso a interfaces administrativas mediante protocolos de red seguros como Secure Shell (SSH) y HTTPS. No utilizar protocolos de gestión inseguros como Telnet y HTTP, a menos que sea operacionalmente esencial. Pasos incluyen:

- Identificar y enumerar los activos con software de gestión autorizado instalado.
- Utilizar estándares de configuración para asegurar que el software de gestión esté configurado correctamente.

4.7 Gestionar las cuentas predeterminadas en los activos y el software de la empresa, como root, administrador y otras cuentas preconfiguradas del proveedor. Ejemplos de implementación pueden incluir la desactivación de cuentas predeterminadas o hacerlas inutilizables. Pasos incluyen:

- Identificar y enumerar el software operativo autorizado, las aplicaciones y el software de terceros que contengan cuentas predeterminadas en los activos empresariales.
- Enumerar las cuentas predeterminadas.
- Verificar si las cuentas predeterminadas pueden ser desactivadas y desactivarlas si es posible.
- Si una cuenta no puede ser desactivada, asegurarse de cambiar las contraseñas predeterminadas conforme a la política de contraseñas única de la empresa.
- Documentar las cuentas predeterminadas con contraseñas cambiadas.

4.8 Desinstalar o desactivar servicios innecesarios en los activos y software empresariales, como un servicio de compartición de archivos no utilizado, módulo de aplicación web o función de servicio. Pasos incluyen:

- Identificar y enumerar los servicios autorizados.
- Identificar y enumerar todos los servicios en los activos empresariales.
- Identificar y enumerar los servicios autorizados en los activos.
- Identificar y enumerar los servicios no autorizados en los activos.
- Atender los servicios no autorizados en los activos conforme a la política.
- Verificar las configuraciones de los servicios autorizados para asegurarse de que estén correctamente configurados.

4.9 Configurar servidores DNS confiables en la infraestructura de red. Ejemplos de implementación incluyen la configuración de dispositivos de red para utilizar servidores DNS controlados por la empresa y/o servidores DNS externos reputados. Pasos incluyen:

- Identificar y enumerar los servidores DNS autorizados.
- Identificar y enumerar los activos configurados con servidores DNS autorizados.
- Verificar la configuración de los servidores DNS identificados en los activos para asegurar que estén configurados con los servidores DNS autorizados.

4.10 Aplicar bloqueo automático del dispositivo tras un umbral predeterminado de intentos fallidos de autenticación local en dispositivos portátiles de usuario final, cuando sea compatible. Para laptops, no permitir más de 20 intentos fallidos de autenticación; para tabletas y smartphones, no más de 10 intentos fallidos. Ejemplos de implementación incluyen Microsoft InTune Device Lock y Apple Configuration Profile maxFailedAttempts. Pasos incluyen:

- Identificar y enumerar todos los dispositivos portátiles.
- Verificar la configuración de intentos fallidos de autenticación para todos los dispositivos portátiles.
  - Asegurar que la autenticación fallida en laptops esté correctamente configurada a 20 intentos o menos.
  - Asegurar que la autenticación fallida en dispositivos móviles esté correctamente configurada a 10 intentos o menos

4.11 Eliminar remotamente los datos empresariales de los dispositivos portátiles de usuario final propiedad de la empresa cuando se considere apropiado, como en caso de dispositivos perdidos o robados, o cuando un individuo ya no brinde soporte a la empresa. Pasos incluyen:

- Identificar y enumerar los dispositivos portátiles de usuario final que soportan eliminación remota.
- Asegurar la configuración adecuada para la eliminación remota en los dispositivos portátiles capaces de soportarla

4.12 Asegurar el uso de espacios de trabajo empresariales separados en los dispositivos móviles de usuario final, cuando sea compatible. Ejemplos de implementación incluyen el uso de un perfil de configuración de Apple o un perfil de trabajo de Android para separar las aplicaciones y datos empresariales de las aplicaciones y datos personales. Pasos incluyen:

- Identificar y enumerar el software de gestión de dispositivos móviles autorizado.
- Identificar dispositivos móviles capaces de soportar software de gestión de dispositivos móviles.
- Asegurar la configuración adecuada de los dispositivos móviles con el software de gestión de dispositivos móviles.

Control 5: Gestión de Cuentas

Utilizar procesos y herramientas para asignar y gestionar la autorización de credenciales para cuentas de usuario, incluyendo cuentas de administrador, así como cuentas de servicio, para los activos y el software de la empresa.

5.1 Establecer y mantener un inventario de todas las cuentas gestionadas en la empresa. El inventario debe incluir, como mínimo, cuentas de usuario, de administrador y de servicio. El inventario, como mínimo, debe contener el nombre de la persona, nombre de usuario, fechas de inicio/finalización y departamento. Validar que todas las cuentas activas estén autorizadas, en un cronograma recurrente al menos trimestral, o con mayor frecuencia. Los pasos incluyen:

- Crear un inventario de cuentas y documentar los siguientes elementos: nombre de la persona, nombre de usuario, fechas de inicio/finalización y departamento.
- Validar que todas las cuentas activas estén autorizadas, en un cronograma recurrente al menos trimestral, o con mayor frecuencia.
- Validar que todas las cuentas inactivas estén deshabilitadas o eliminadas, en un cronograma recurrente al menos trimestral, o con mayor frecuencia.

5.2 Utilizar contraseñas únicas para todos los activos de la empresa. La mejor práctica incluye, como mínimo, una contraseña de 8 caracteres para cuentas que utilizan MFA y una contraseña de 14 caracteres para cuentas que no utilizan MFA.

5.3 Eliminar o deshabilitar cualquier cuenta inactiva después de un período de 45 días de inactividad, donde sea compatible.

5.4 Restringir los privilegios de administrador a cuentas dedicadas de administrador en los activos de la empresa. Realizar actividades informáticas generales, como navegación por internet, correo electrónico y uso de suites de productividad, desde la cuenta principal del usuario, sin privilegios elevados.

5.5 y mantener un inventario de cuentas de servicio. El inventario, como mínimo, debe contener el propietario del departamento, fecha de revisión y propósito. Los pasos incluyen:

- Utilizando el inventario de cuentas, asegurarse de que los siguientes elementos estén presentes: propietario del departamento, fecha de revisión y propósito.
- Validar que todas las cuentas activas estén autorizadas, en un cronograma recurrente al menos trimestral, o con mayor frecuencia.

5.6 Centralizar la gestión de cuentas a través de un directorio o servicio de identidad. Los pasos incluyen:

- Identificar y enumerar los puntos de autenticación centralizados.
- Para cada punto de autenticación centralizado identificado, determinar si es necesario o puede ser consolidado.
- Cuando sea apropiado, consolidar los puntos de autenticación centralizados.

Control 6: Gestión del Control de Acceso

Utilizar procesos y herramientas para crear, asignar, gestionar y revocar credenciales de acceso y privilegios para cuentas de usuario, administrador y servicio para los activos y software de la empresa.

6.1 Establecer y seguir un proceso documentado, preferentemente automatizado, para otorgar acceso a los activos de la empresa al momento de la contratación o cambio de rol de un usuario.

6.2 Establecer y seguir un proceso, preferentemente automatizado, para revocar el acceso a los activos de la empresa, mediante la desactivación inmediata de cuentas al momento de la terminación, revocación de derechos o cambio de rol de un usuario. La desactivación de cuentas, en lugar de su eliminación, puede ser necesaria para preservar los registros de auditoría.

6.3 Requerir que todas las aplicaciones empresariales o de terceros expuestas externamente implementen MFA, cuando sea compatible. La implementación de MFA a través de un servicio de directorio o proveedor de inicio de sesión único (SSO) es una implementación satisfactoria de esta salvaguarda. Los pasos incluyen:

- Identificar y enumerar las aplicaciones expuestas externamente y de terceros.
- Identificar y enumerar todas las cuentas de usuario asociadas con las aplicaciones.
- Asegurar que las cuentas de usuario estén configuradas correctamente para utilizar MFA.

6.4 Requerir MFA para el acceso remoto a la red. Los pasos incluyen:

- Identificar y enumerar todos los activos remotos autorizados.
- Asegurar que todos los activos remotos autorizados estén configurados correctamente para requerir MFA.

6.5 Requerir MFA para todas las cuentas de acceso administrativo, cuando sea compatible, en todos los activos de la empresa, ya sea gestionados localmente o a través de un proveedor de servicios. Los pasos incluyen:

- Identificar y enumerar todas las cuentas administrativas.
- Asegurar que todas las cuentas administrativas estén configuradas correctamente para requerir MFA.

6.6 Establecer y mantener un inventario de los sistemas de autenticación y autorización de la empresa, incluidos aquellos alojados localmente o en un proveedor de servicios remoto. Revisar y actualizar el inventario, como mínimo, anualmente o con mayor frecuencia.

6.7 Centralizar el control de acceso para todos los activos de la empresa a través de un servicio de directorio o proveedor SSO, cuando sea compatible. Los pasos incluyen:

- Identificar todos los servicios de directorio y SSO.
- Identificar y enumerar los activos que soportan servicios de directorio y SSO.
- Asegurar que cada activo esté cubierto por al menos un servicio de directorio o SSO.

6.8 Definir y mantener el control de acceso basado en roles, mediante la determinación y documentación de los derechos de acceso necesarios para cada rol dentro de la empresa para llevar a cabo exitosamente sus funciones asignadas. Realizar revisiones del control de acceso de los activos de la empresa para validar que todos los privilegios estén autorizados, en un cronograma recurrente al menos anual, o con mayor frecuencia.

Control 7: Gestión Continua de Vulnerabilidades

Desarrollar un plan para evaluar y rastrear continuamente las vulnerabilidades en todos los activos de la empresa dentro de la infraestructura empresarial, con el fin de remediarlas y minimizar la ventana de oportunidad para los atacantes. Monitorear fuentes públicas y privadas de la industria para obtener nueva información sobre amenazas y vulnerabilidades.

7.1 Establecer y mantener un proceso documentado de gestión de vulnerabilidades para los activos de la empresa. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

7.2 Establecer y mantener una estrategia de remediación basada en riesgos, documentada en un proceso de remediación, con revisiones mensuales o más frecuentes.

7.3 Realizar actualizaciones del sistema operativo en los activos de la empresa mediante la gestión automatizada de parches mensualmente, o con mayor frecuencia. Los pasos incluyen:

- Identificar los sistemas operativos autorizados dentro de la empresa.
- Identificar el sistema operativo que actualmente se ejecuta en cada activo.
- Para cada activo:
  - Identificar y enumerar los sistemas operativos que están actualizados.
  - Identificar y enumerar los sistemas operativos que no están actualizados.
- Para cada sistema operativo desactualizado identificado, determinar si existe una excepción documentada. Tomar las medidas correctivas que correspondan.
- Identificar el software autorizado de gestión automatizada de parches.

- Identificar y enumerar los sistemas operativos cubiertos por al menos un software de gestión automatizada de parches.
- Identificar y enumerar los sistemas operativos que no están cubiertos por al menos un software de gestión automatizada de parches. Tomar las medidas correctivas que correspondan.
- Asegurar que el software de gestión automatizada de parches esté configurado para ejecutarse cada 30 días o menos.

7.4 Realizar actualizaciones de aplicaciones en los activos de la empresa mediante la gestión automatizada de parches mensualmente, o con mayor frecuencia. Los pasos incluyen:

- Identificar las aplicaciones autorizadas dentro de la empresa.
- Identificar las aplicaciones que actualmente se ejecutan en cada activo.
- Para cada activo:
  - Identificar y enumerar las aplicaciones que están actualizadas.
  - Identificar y enumerar las aplicaciones que no están actualizadas.
- Para cada aplicación desactualizada identificada, determinar si existe una excepción documentada. Tomar las medidas correctivas que correspondan.
- Identificar y enumerar las aplicaciones cubiertas por al menos un software de gestión automatizada de parches.
- Identificar y enumerar los sistemas operativos no cubiertos por al menos un software de gestión automatizada de parches. Tomar las medidas correctivas que correspondan.
- Asegurar que el software de gestión automatizada de parches esté configurado para ejecutarse cada 30 días o menos.

7.5 Realizar escaneos automatizados de vulnerabilidades en los activos internos de la empresa de forma trimestral o con mayor frecuencia. Realizar escaneos autenticados y no autenticados. Los pasos incluyen:

- Identificar y enumerar el software de escaneo de vulnerabilidades.
- Identificar y enumerar el software de escaneo de vulnerabilidades autenticado.
- Utilizar el inventario de activos empresariales para identificar y enumerar todos los activos internos.
- Identificar y enumerar los activos internos cubiertos por al menos un software de escaneo de vulnerabilidades.
- Identificar y enumerar los activos internos que no están cubiertos por al menos un software de escaneo de vulnerabilidades. Tomar las medidas correctivas que correspondan.

- Asegurar que el software de escaneo de vulnerabilidades esté configurado para escanear cada 3 meses o menos.
- Identificar y enumerar los activos internos cubiertos por al menos un escáner de vulnerabilidades autenticado.
- Identificar y enumerar los activos internos que no están cubiertos por al menos un escáner de vulnerabilidades autenticado. Tomar las medidas correctivas que correspondan.
- Asegurar que el software de escaneo de vulnerabilidades autenticado esté configurado para escanear cada 3 meses o menos.

7.6 Realizar escaneos automatizados de vulnerabilidades en los activos empresariales expuestos externamente. Realizar escaneos mensualmente o con mayor frecuencia. Los pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar todos los activos externos.
- Identificar y enumerar los activos externos cubiertos por al menos un software de escaneo de vulnerabilidades.
- Identificar y enumerar los activos externos que no están cubiertos por al menos un software de escaneo de vulnerabilidades. Tomar las medidas correctivas que correspondan.
- Asegurar que los escáneres de vulnerabilidades estén correctamente configurados para escanear cada 30 días o menos.

7.7 Remediar las vulnerabilidades detectadas en el software mediante procesos y herramientas de forma mensual o con mayor frecuencia, conforme al proceso de remediación.

Control 8: Gestión de Registros de Auditoría

Recopilar, alertar, revisar y conservar los registros de auditoría de eventos que podrían ayudar a detectar, entender o recuperarse de un ataque.

8.1 Establecer y mantener un proceso documentado de gestión de registros de auditoría que defina los requisitos de registro de la empresa. Como mínimo, abordar la recopilación, revisión y retención de registros de auditoría para los activos de la empresa. Revisar y actualizar la documentación anualmente o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

8.2 Recopilar registros de auditoría. Asegurar que el registro, según el proceso de gestión de registros de auditoría de la empresa, se haya habilitado en todos los activos empresariales. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos capaces de soportar registro.
- Asegurar que los activos estén configurados adecuadamente para registrar eventos conforme al proceso.

8.3 Asegurar que los destinos de registro mantengan un almacenamiento adecuado para cumplir con el proceso de gestión de registros de auditoría de la empresa.

8.4 Estandarizar la sincronización horaria. Configurar al menos dos fuentes de tiempo sincronizadas en los activos empresariales, cuando sea compatible. Pasos incluyen:

- Identificar y enumerar los activos capaces de soportar sincronización horaria.
- Asegurar que los activos estén configurados usando al menos dos fuentes de tiempo aprobadas.

8.5 Configurar el registro detallado de auditoría para los activos empresariales que contienen datos sensibles. Incluir fuente del evento, fecha, nombre de usuario, marca de tiempo, direcciones de origen, direcciones de destino y otros elementos útiles que puedan ayudar en una investigación forense.

8.6 Recopilar registros de auditoría de consultas DNS en los activos empresariales, donde sea apropiado y compatible. Pasos incluyen:

- Identificar y enumerar los servidores DNS internos.
- Asegurar que los servidores DNS estén configurados adecuadamente para recopilar registros.

8.7 Recopilar registros de auditoría de solicitudes de URL en los activos empresariales, donde sea apropiado y compatible. Pasos incluyen:

- Identificar y enumerar los activos que soportan registro de URLs.
- Asegurar que los activos estén configurados adecuadamente para el registro.

8.8 Recopilar registros de auditoría de línea de comandos. Ejemplos de implementación incluyen la recopilación de registros de auditoría de PowerShell®, BASH™ y terminales administrativas remotas. Pasos incluyen:

- Utilizar el inventario de activos para identificar y enumerar los activos que soportan auditoría de comandos por línea de comandos.

- Asegurar que los activos estén configurados correctamente.

8.9 Centralizar, en la medida de lo posible, la recopilación y retención de registros de auditoría en todos los activos empresariales de acuerdo con el proceso documentado de gestión de registros de auditoría. Ejemplos de implementación incluyen aprovechar una herramienta SIEM para centralizar múltiples fuentes de registros. Pasos incluyen:

- Utilizar el inventario de software para identificar y enumerar el software agregador de registros.
- Asegurar que los activos estén cubiertos por al menos un software agregador.

8.10 Conservar los registros de auditoría en todos los activos empresariales por un mínimo de 90 días.

- Asegurar que el software agregador esté configurado para retener registros por 90 días o más.

8.11 Realizar revisiones de los registros de auditoría para detectar anomalías o eventos anormales que puedan indicar una amenaza potencial. Realizar revisiones semanalmente o con mayor frecuencia.

8.12 Recopilar registros de proveedores de servicios, donde sea compatible. Ejemplos de implementación incluyen la recopilación de eventos de autenticación y autorización, eventos de creación y eliminación de datos, y eventos de gestión de usuarios.

- Para cada servicio incluido en el inventario de proveedores de servicios, identificar y enumerar los proveedores que soportan el registro.

Control 9: **Protección de Correo Electrónico y Navegadores Web**

Mejorar las protecciones y detecciones de amenazas provenientes de vectores de correo electrónico y web, ya que estos representan oportunidades para que los atacantes manipulen el comportamiento humano mediante interacción directa.

9.1 Asegurar que solo navegadores y clientes de correo electrónico completamente soportados estén autorizados para ejecutarse en la empresa, utilizando únicamente la versión más reciente de navegadores y clientes de correo electrónico proporcionados por el proveedor. Pasos incluyen:

- Utilizar el inventario de software autorizado para identificar y enumerar el software de navegador web y cliente de correo electrónico.
- Asegurar que el software etiquetado como “soportado” cuente con soporte actual del proveedor de software.

9.2 Utilizar servicios de filtrado DNS en todos los dispositivos de usuario final, incluyendo activos remotos y locales, para bloquear el acceso a dominios maliciosos conocidos. Pasos incluyen:

- Utilizar el inventario de activos de la empresa para identificar y enumerar los activos que soportan filtrado DNS.
- Utilizar el inventario de software autorizado para identificar y enumerar los servicios de filtrado DNS autorizados.
- Asegurar que el software esté configurado adecuadamente en los activos.

9.3 Aplicar y actualizar filtros de URL basados en red para limitar que un activo de la empresa se conecte a sitios web potencialmente maliciosos o no aprobados. Ejemplos de implementación incluyen filtrado por categorías, filtrado basado en reputación o mediante listas de bloqueo. Aplicar filtros para todos los activos de la empresa. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos capaces de soportar filtros de URL basados en red.
- Utilizar el inventario de software autorizado para identificar navegadores/clientes web autorizados.
- Asegurar que el software esté configurado correctamente.

9.4 Restringir, ya sea mediante la desinstalación o desactivación, cualquier complemento, extensión o aplicación adicional de navegador o cliente de correo electrónico que no esté autorizado o sea innecesario. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos sujetos a restricciones de complementos de navegador/correo electrónico.
- Utilizar el inventario de software para identificar los complementos de navegador y correo electrónico autorizados.
- Asegurar que solo los complementos de navegador autorizados estén instalados o habilitados.
- Asegurar que solo los complementos de correo electrónico autorizados estén instalados o habilitados.

9.5 Para reducir la probabilidad de correos electrónicos falsificados o modificados provenientes de dominios válidos, implementar políticas y verificación DMARC, comenzando por implementar los estándares SPF (Sender Policy Framework) y DKIM (DomainKeys Identified Mail).

9.6 Bloquear tipos de archivo innecesarios que intenten ingresar a través de la pasarela de correo electrónico de la empresa. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos configurados como pasarelas de correo electrónico.
- Asegurar que las pasarelas de correo electrónico estén configuradas correctamente para bloquear archivos adjuntos innecesarios.

9.7 Desplegar y mantener protecciones antimalware en los servidores de correo electrónico, como escaneo de archivos adjuntos y/o sandboxing. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar todos los servidores de correo electrónico dentro de la empresa.
- Para cada servidor de correo, asegurar que las protecciones antimalware nativas o externas estén configuradas adecuadamente.

Control 10: Defensa contra Malware

Prevenir o controlar la instalación, propagación y ejecución de aplicaciones, código o scripts maliciosos en los activos empresariales.

10.1 Desplegar y mantener software antimalware en todos los activos empresariales. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos capaces de soportar software antimalware.
- Utilizar el inventario de software autorizado para identificar el software antimalware autorizado.
- Identificar y enumerar los activos con al menos un software antimalware autorizado instalado.
- Identificar y enumerar los activos con solo software antimalware no autorizado instalado y tomar las medidas correctivas que correspondan.
- Identificar y enumerar los activos sin ningún software antimalware instalado y tomar las medidas correctivas que correspondan.
- Asegurar que el software antimalware esté configurado correctamente.

10.2 Configurar actualizaciones automáticas para los archivos de firmas antimalware en todos los activos empresariales. Paso incluye:

- Asegurar que el software antimalware esté configurado correctamente para realizar actualizaciones automáticas.

10.3 Desactivar la funcionalidad de ejecución automática (autorun y autoplay) para medios removibles. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos empresariales capaces de ejecutar funciones de autorun, autoplay y auto-execute.
- Asegurar que las configuraciones de cada activo identificado desactiven las funciones de autorun, autoplay y auto-execute.

10.4 Configurar el software antimalware para escanear automáticamente los medios removibles.

10.5 Habilitar funciones de anti-explotación en los activos y software de la empresa, cuando sea posible, como Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), o Apple® System Integrity Protection (SIP) y Gatekeeper™.

10.6 Gestionar centralizadamente el software antimalware. Paso incluye:

- Asegurar que cada software antimalware autorizado sea gestionado de manera centralizada.

10.7 Utilizar software antimalware basado en comportamiento. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos capaces de soportar software antimalware basado en comportamiento.
- Utilizar el inventario de software autorizado para identificar el software antimalware basado en comportamiento autorizado.
- Asegurar que los activos cuenten con al menos un software antimalware basado en comportamiento autorizado instalado.
- Asegurar que el software antimalware basado en comportamiento esté configurado correctamente.

Control 11: **Recuperación de Datos**

Establecer y mantener prácticas de recuperación de datos suficientes para restaurar los activos empresariales dentro del alcance a un estado previo al incidente y de confianza.

11.1 Establecer y mantener un proceso documentado de recuperación de datos. En dicho proceso, abordar el alcance de las actividades de recuperación de datos, la priorización de la recuperación y la seguridad de los datos respaldados. Revisar y actualizar la documentación anualmente o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

11.2 Realizar respaldos automatizados de los activos empresariales dentro del alcance. Ejecutar respaldos semanalmente, o con mayor frecuencia, según la sensibilidad de los datos. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos que estén dentro del alcance para respaldos automatizados.
- Utilizar el inventario de software autorizado para identificar el software de respaldo autorizado para cada activo identificado anteriormente.
- Asegurar que los activos estén cubiertos por al menos un software de respaldo autorizado.
- Asegurar que el software de respaldo esté configurado correctamente.

11.3 Proteger los datos de recuperación con controles equivalentes a los de los datos originales. Referenciar cifrado o separación de datos, según los requisitos. Paso incluye:

- Para cada activo con software de respaldo instalado, asegurar que el cifrado esté configurado para los respaldos.

11.4 Establecer y mantener una instancia aislada de los datos de recuperación. Ejemplos de implementación incluyen el control de versiones de los destinos de respaldo mediante sistemas o servicios fuera de línea, en la nube o fuera del sitio. Paso incluye:

- Asegurar que los respaldos estén configurados correctamente para enviarse a una instancia aislada.

11.5 Probar la recuperación de respaldos trimestralmente, o con mayor frecuencia, para una muestra de los activos empresariales dentro del alcance.

Control 12: **Gestión de la Infraestructura de Red**

Establecer, implementar y gestionar activamente (rastrear, informar, corregir) los dispositivos de red para evitar que los atacantes exploten servicios de red y puntos de acceso vulnerables.

12.1 Asegurar que la infraestructura de red se mantenga actualizada. Ejemplos de implementación incluyen ejecutar la versión estable más reciente del software y/o utilizar ofertas actuales de red como servicio (NaaS). Revisar las versiones del software mensualmente, o con mayor frecuencia, para verificar que tengan soporte.

12.2 Establecer y mantener una arquitectura de red segura. Una arquitectura de red segura debe abordar, como mínimo, la segmentación, el privilegio mínimo y la disponibilidad. Ejemplos de implementación pueden incluir documentación, políticas y componentes de diseño.

12.3 Gestionar de forma segura la infraestructura de red. Ejemplos de implementación incluyen la infraestructura como código controlada por versiones, y el uso de protocolos de red seguros como SSH y HTTPS. Pasos incluyen:

- Para los activos de infraestructura de red, asegurar que estén configurados para usar sesiones cifradas.
- Para cada segmento de red, identificar y enumerar los segmentos de red que utilizan infraestructura como código para todo el segmento o parcialmente.
- Asegurar que los segmentos de red estén cubiertos por infraestructura como código controlada por versiones.

12.4 Establecer y mantener diagramas de arquitectura y/o otra documentación del sistema de red. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

12.5 Centralizar la Autenticación, Autorización y Auditoría (AAA) de red. Pasos incluyen:

- Utilizar el inventario de software autorizado para identificar y enumerar todos los servicios AAA dentro de la empresa.
- Para cada punto AAA centralizado, determinar si es necesario o si puede ser consolidado.
- Asegurar que cada activo de infraestructura de red esté cubierto por al menos un sistema AAA.

12.6 Adoptar protocolos seguros de gestión de red (por ejemplo, 802.1X) y protocolos de comunicación seguros (por ejemplo, Wi-Fi Protected Access 2 (WPA2) Enterprise o alternativas más seguras). Pasos incluyen:

- Para cada segmento de red, identificar los protocolos de comunicación.
- Asegurar que solo se utilicen protocolos de comunicación autorizados.
- Asegurar que los protocolos de comunicación estén configurados correctamente.
- Para cada segmento de red, identificar los protocolos de gestión de red.
- Asegurar que solo se utilicen protocolos de gestión de red autorizados.
- Asegurar que los protocolos de gestión de red estén configurados correctamente.

12.7 Requerir que los usuarios se autentiquen en servicios de autenticación y VPN administrados por la empresa antes de acceder a los recursos empresariales desde dispositivos de usuario final. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos empresariales remotos.

- Utilizar el inventario de activos empresariales y de software para identificar y enumerar todos los dispositivos y software VPN.
- Asegurar que los dispositivos y software VPN estén configurados correctamente para requerir autenticación antes de otorgar acceso.
- Asegurar que los activos adecuados estén cubiertos por una VPN.
- Asegurar que los servicios AAA estén configurados correctamente para requerir autenticación antes de otorgar acceso.
- Asegurar que los activos adecuados estén cubiertos por un servicio AAA.

12.8 Establecer y mantener recursos de cómputo dedicados, ya sea físicamente o lógicamente separados, para todas las tareas administrativas o tareas que requieran acceso administrativo. Los recursos de cómputo deben estar segmentados de la red principal de la empresa y no deben tener acceso a Internet. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos utilizados para fines administrativos.
- Para cada activo identificado anteriormente, asegurarse de que estén configurados para no tener acceso a Internet.

Control 13: Monitoreo y Defensa de la Red

Operar procesos y herramientas para establecer y mantener un monitoreo integral de la red y una defensa contra amenazas de seguridad en toda la infraestructura de red de la empresa y su base de usuarios.

13.1 Centralizar las alertas de eventos de seguridad en todos los activos empresariales para la correlación y análisis de registros. La mejor práctica requiere el uso de una herramienta SIEM, que incluya alertas de correlación de eventos definidas por el proveedor. Una plataforma de análisis de registros configurada con alertas de correlación relevantes para la seguridad también satisface esta salvaguarda. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos que generan registros de eventos de seguridad.
- Para cada activo identificado, asegurar que los registros se centralicen en la ubicación de la herramienta de correlación o análisis de registros.

13.2 Desplegar una solución de detección de intrusiones basada en host en los activos empresariales, donde sea apropiado y/o compatible. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos capaces de soportar sistemas de detección de intrusiones basados en host.
- Utilizar el inventario de software autorizado para identificar el software de detección de intrusiones basado en host autorizado.
- Para cada activo identificado, asegurar que esté cubierto por al menos un software de detección de intrusiones basado en host autorizado.

13.3 Desplegar una solución de detección de intrusiones de red en los activos empresariales, donde sea apropiado. Ejemplos de implementación incluyen el uso de un Sistema de Detección de Intrusiones en la Red (NIDS) o un servicio equivalente del proveedor de servicios en la nube (CSP). Pasos incluyen:

- Utilizar los activos identificados que forman parte de la infraestructura de red para identificar las soluciones de detección de intrusiones de red para la empresa.
- Utilizar la documentación de arquitectura de red empresarial para identificar y enumerar los límites de red.
- Para cada límite de red identificado, asegurar que esté cubierto por al menos una solución de detección de intrusiones de red.

13.4 Realizar filtrado de tráfico entre segmentos de red, donde sea apropiado. Pasos incluyen:

- Identificar y enumerar los segmentos de red que requieren comunicación con otros segmentos de red.
- Para cada segmento de red identificado, identificar los activos de infraestructura de red responsables del filtrado de tráfico, asegurarse de que cada segmento esté configurado correctamente para filtrar el tráfico.

13.5 Gestionar el control de acceso para los activos que se conectan remotamente a los recursos empresariales. Determinar el nivel de acceso a los recursos empresariales en base a: software antimalware actualizado instalado, cumplimiento con la configuración segura de la empresa y asegurarse de que el sistema operativo y las aplicaciones estén actualizados. Pasos incluyen:

- Utilizar el inventario de sistemas de autenticación y autorización para identificar y enumerar los sistemas de autorización que permiten inicios de sesión remotos.
- Para cada sistema de autorización identificado, asegurar que esté configurado correctamente para todas las políticas.
- Asegurar que cada activo remoto esté cubierto por al menos un sistema de autorización compatible.

13.6 Recopilar registros de flujo de tráfico de red y/o tráfico de red para su revisión y alertas desde los dispositivos de red. Pasos incluyen:

- Utilizar los activos que forman parte de la infraestructura de red para identificar y enumerar los activos en los límites de red.
- Para cada activo de límite de red identificado, asegurar la configuración adecuada para habilitar el registro de tráfico de red o del flujo de tráfico de red.

13.7 Desplegar una solución de prevención de intrusiones basada en host en los activos empresariales, donde sea apropiado y/o compatible. Ejemplos de implementación incluyen el uso de un cliente de Detección y Respuesta en el Endpoint (EDR) o un agente IPS basado en host. Pasos incluyen:

- Utilizar el inventario de activos empresariales para identificar y enumerar los activos capaces de soportar sistemas de prevención de intrusiones basados en host.
- Utilizar el inventario de software autorizado para identificar el software de prevención de intrusiones basado en host autorizado.
- Para cada activo identificado, asegurar que esté cubierto por al menos un software de prevención de intrusiones basado en host autorizado.

13.8 Desplegar una solución de prevención de intrusiones de red, donde sea apropiado. Ejemplos de implementación incluyen el uso de un Sistema de Prevención de Intrusiones en la Red (NIPS) o un servicio CSP equivalente. Pasos incluyen:

- Utilizar los activos que forman parte de la infraestructura de red para identificar las soluciones de prevención de intrusiones de red para la empresa.
- Identificar los límites de red y asegurar que cada límite esté cubierto por al menos una solución de prevención de intrusiones de red.

13.9 Desplegar control de acceso a nivel de puerto. El control de acceso a nivel de puerto utiliza 802.1x, o protocolos de control de acceso de red similares, como certificados, y puede incorporar autenticación de usuario y/o dispositivo. Pasos incluyen:

- Utilizar el inventario de software autorizado para identificar y enumerar los autenticadores 802.1x.
- Para cada autenticador identificado, asegurar que esté configurado correctamente.
- Utilizar servicios AAA dentro de la empresa para identificar servidores de autenticación 802.1x.
- Para cada servidor de autenticación identificado, asegurar que la configuración incluya una conexión con al menos un servidor CMDB.
- Si la empresa no utiliza el diseño de red 802.1x para controlar el acceso a la red, asegurar la configuración adecuada para usar certificados de autenticación de cliente.

13.10 Realizar filtrado a nivel de capa de aplicación. Ejemplos de implementación incluyen un proxy de filtrado, firewall de capa de aplicación o puerta de enlace. Pasos incluyen:

- Utilizar el inventario de software autorizado para identificar el software utilizado para el filtrado a nivel de capa de aplicación.
- Para los activos que son parte de la infraestructura de red, asegurar que todos estén cubiertos por software de filtrado de capa de aplicación.

13.11 Ajustar los umbrales de alerta de eventos de seguridad mensualmente, o con mayor frecuencia.

Control 14: Concientización sobre Seguridad y Capacitación en Habilidades

Establecer y mantener un programa de concientización sobre seguridad para influir en el comportamiento del personal de la empresa, fomentando la conciencia en seguridad y el desarrollo de habilidades adecuadas para reducir los riesgos de ciberseguridad para la organización.

14.1 Establecer y mantener un programa de concientización sobre seguridad. El propósito de este programa es educar al personal de la empresa sobre cómo interactuar de manera segura con los activos y datos de la organización. Realizar la capacitación al momento de la contratación y, como mínimo, de manera anual. Revisar y actualizar el contenido anualmente, o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

14.2 Capacitar a los miembros del personal para reconocer ataques de ingeniería social, como el phishing, compromiso del correo electrónico empresarial (BEC), pretextos y seguimiento sin autorización (tailgating).

14.3 Capacitar a los miembros del personal sobre las mejores prácticas de autenticación. Los temas de ejemplo incluyen MFA (autenticación multifactor), composición de contraseñas y gestión de credenciales.

14.4 Capacitar a los miembros del personal sobre cómo identificar, almacenar, transferir, archivar y destruir adecuadamente datos sensibles. Esto también incluye formación en buenas prácticas de escritorio y pantalla limpia, como bloquear la pantalla al alejarse del activo empresarial, borrar pizarras físicas y virtuales al final de las reuniones, y almacenar datos y activos de forma segura.

14.5 Capacitar a los miembros del personal para que sean conscientes de las causas de exposición involuntaria de datos. Ejemplos de temas incluyen la entrega errónea de datos sensibles, la pérdida de un dispositivo portátil de usuario final o la publicación de datos a audiencias no deseadas.

14.6 Capacitar a los miembros del personal para que puedan reconocer un posible incidente y sepan cómo reportarlo.

14.7 Capacitar al personal para que entienda cómo verificar y reportar parches de software desactualizados o cualquier falla en los procesos y herramientas automatizadas. Parte de esta capacitación debe incluir la notificación al personal de TI de cualquier falla en los procesos y herramientas automatizadas.

14.8 Capacitar a los miembros del personal sobre los peligros de conectarse a redes inseguras y transmitir datos a través de ellas durante actividades empresariales. Si la empresa tiene trabajadores remotos, la capacitación debe incluir orientación para garantizar que todos los usuarios configuren su infraestructura de red doméstica de manera segura.

14.9 Realizar capacitación en concientización sobre seguridad y habilidades específicas según el rol. Ejemplos de implementación incluyen cursos de administración segura de sistemas para profesionales de TI, capacitación en concientización y prevención de vulnerabilidades del Top 10 de OWASP® para desarrolladores de aplicaciones web, y capacitación avanzada en concientización sobre ingeniería social para roles de alto perfil.

Control 15: Gestión de Proveedores de Servicios

Desarrollar un proceso para evaluar a los proveedores de servicios que manejan datos sensibles o que son responsables de plataformas o procesos críticos de TI de la empresa, a fin de garantizar que dichos proveedores protejan adecuadamente esas plataformas y datos.

15.1 Establecer y mantener un inventario de proveedores de servicios. El inventario debe listar todos los proveedores de servicios conocidos, incluir su(s) clasificación(es) y designar un contacto dentro de la empresa para cada proveedor. Revisar y actualizar el inventario anualmente, o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

15.2 Establecer y mantener una política de gestión de proveedores de servicios. Asegurar que la política aborde la clasificación, el inventario, la evaluación, el monitoreo y el retiro de los proveedores de servicios. Revisar y actualizar la política anualmente, o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

15.3 Clasificar a los proveedores de servicios. La clasificación puede considerar una o más características, como la sensibilidad de los datos, el volumen de datos, los requisitos de disponibilidad, regulaciones aplicables, riesgo inherente y riesgo mitigado. Actualizar y revisar las clasificaciones anualmente, o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

15.4 Asegurar que los contratos con proveedores de servicios incluyan requisitos de seguridad. Ejemplos de requisitos pueden incluir requisitos mínimos de programas de seguridad, notificación y respuesta ante incidentes de seguridad y/o violaciones de datos, requisitos de cifrado de datos y compromisos de eliminación de datos. Estos requisitos de seguridad deben ser coherentes con la política de gestión de proveedores de servicios de la empresa. Revisar los contratos con proveedores de servicios anualmente para asegurar que no falten requisitos de seguridad.

15.5 Evaluar a los proveedores de servicios conforme a la política de gestión de proveedores de servicios de la empresa. El alcance de la evaluación puede variar según la(s) clasificación(es), e incluir la revisión de informes de evaluación estandarizados como el Service Organization Control 2 (SOC 2) y la Atestación de Cumplimiento (AoC) de PCI, cuestionarios personalizados u otros procesos rigurosos apropiados. Reevaluar a los proveedores de servicios al menos anualmente o con nuevos contratos o renovaciones.

15.6 Monitorear a los proveedores de servicios conforme a la política de gestión de proveedores de servicios de la empresa. El monitoreo puede incluir reevaluaciones periódicas del cumplimiento del proveedor, seguimiento de notas de versiones del proveedor y monitoreo de la web oscura.

15.7 Retirar de manera segura a los proveedores de servicios. Ejemplos de consideraciones incluyen la desactivación de cuentas de usuario y de servicio, la finalización de flujos de datos y la eliminación segura de los datos empresariales dentro de los sistemas del proveedor.

Control 16: **Seguridad del Software de Aplicación**

Gestionar el ciclo de vida de seguridad del software desarrollado internamente, alojado o adquirido, para prevenir, detectar y remediar debilidades de seguridad antes de que puedan afectar a la empresa.

16.1 Establecer y mantener un proceso de desarrollo de aplicaciones seguras. En el proceso, abordar elementos como: estándares de diseño seguro de aplicaciones, prácticas de codificación segura, capacitación de desarrolladores, gestión de vulnerabilidades, seguridad del código de terceros y procedimientos de pruebas de seguridad de aplicaciones. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

16.2 Establecer y mantener un proceso para aceptar y abordar reportes de vulnerabilidades de software, incluyendo un medio para que entidades externas puedan reportar. El proceso debe incluir elementos como: una política de manejo de vulnerabilidades que identifique el proceso de reporte, la parte responsable del manejo de los reportes de vulnerabilidades y un proceso para la recepción, asignación, remediación y prueba de remediación. Como parte del proceso, utilizar un sistema de seguimiento de vulnerabilidades que incluya clasificaciones de severidad y métricas para medir los tiempos de identificación, análisis y remediación de vulnerabilidades. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

- Los desarrolladores de aplicaciones de terceros deben considerar esta una política de cara al exterior que ayuda a establecer expectativas para las partes interesadas externas.

16.3 Realizar análisis de causa raíz sobre vulnerabilidades de seguridad. Al revisar vulnerabilidades, el análisis de causa raíz consiste en evaluar los problemas subyacentes que crean vulnerabilidades en el código y permite a los equipos de desarrollo ir más allá de simplemente corregir vulnerabilidades individuales a medida que surgen.

16.4 Establecer y gestionar un inventario actualizado de componentes de terceros usados en el desarrollo, comúnmente conocido como "lista de materiales", así como componentes planificados para uso futuro. Este inventario debe incluir cualquier riesgo que cada componente de terceros pueda representar. Evaluar la lista al menos mensualmente para identificar cualquier cambio o actualización en estos componentes y validar que el componente aún cuenta con soporte.

16.5 Utilizar componentes de software de terceros actualizados y confiables. Cuando sea posible, elegir frameworks y bibliotecas establecidos y comprobados que proporcionen seguridad adecuada. Adquirir estos componentes de fuentes confiables o evaluar el software en busca de vulnerabilidades antes de su uso.

16.6 Establecer y mantener un sistema de clasificación de severidad y un proceso para vulnerabilidades de aplicaciones que facilite priorizar el orden en que se corrigen las vulnerabilidades descubiertas. Este proceso incluye establecer un nivel mínimo de aceptabilidad de seguridad para liberar código o aplicaciones. Las clasificaciones de severidad aportan una forma sistemática de clasificar vulnerabilidades que mejora la gestión de riesgos y ayuda a garantizar que los errores más graves se solucionen primero. Revisar y actualizar el sistema y el proceso.

16.7 Utilizar plantillas de configuración reforzada estándar recomendadas por la industria para los componentes de la infraestructura de aplicaciones. Esto incluye servidores subyacentes, bases de datos y servidores web, y aplica a contenedores en la nube, componentes de Plataforma como Servicio (PaaS) y componentes de Software como Servicio (SaaS). No permitir que el software desarrollado internamente debilite la configuración reforzada.

16.8 Mantener entornos separados para sistemas de producción y no producción.

16.9 Asegurar que todo el personal de desarrollo de software reciba capacitación en escritura de código seguro para su entorno de desarrollo específico y responsabilidades. La capacitación puede incluir principios generales de seguridad y prácticas estándar de seguridad en aplicaciones. Realizar la capacitación al menos anualmente y diseñarla de manera que promueva la seguridad dentro del equipo de desarrollo, y construya una cultura de seguridad entre los desarrolladores.

16.10 Aplicar principios de diseño seguro en las arquitecturas de aplicaciones. Los principios de diseño seguro incluyen el concepto de privilegio mínimo y la aplicación de mediación para validar cada operación que realiza el usuario, promoviendo el concepto de "nunca confiar en la entrada del usuario". Ejemplos incluyen asegurar que se realice y documente una verificación de errores explícita para toda entrada, incluyendo tamaño, tipo de datos y rangos o formatos aceptables. El diseño seguro también implica minimizar la superficie de ataque de la infraestructura de la aplicación, como desactivar puertos y servicios no protegidos, eliminar programas y archivos innecesarios, y renombrar o eliminar cuentas predeterminadas.

16.11 Aprovechar módulos o servicios verificados para los componentes de seguridad de aplicaciones, como gestión de identidad, cifrado, auditoría y registro. Usar funciones de plataforma en funciones de seguridad críticas reducirá la carga de trabajo de los desarrolladores y minimizará la probabilidad de errores de diseño o implementación. Los sistemas operativos modernos proporcionan mecanismos eficaces para identificación, autenticación y autorización, y ponen esos mecanismos a disposición de las aplicaciones. Utilizar únicamente algoritmos de cifrado estandarizados, actualmente aceptados y extensamente revisados. Los sistemas operativos también proporcionan mecanismos para crear y mantener registros de auditoría seguros.

16.12 Aplicar herramientas de análisis estático y dinámico dentro del ciclo de vida de la aplicación para verificar que se sigan prácticas de codificación segura.

16.13 Realizar pruebas de penetración de aplicaciones. Para aplicaciones críticas, las pruebas de penetración autenticadas son más adecuadas para encontrar vulnerabilidades de lógica de negocio que el escaneo de código y las pruebas de seguridad automatizadas. Las pruebas de penetración dependen de la habilidad del evaluador para manipular manualmente una aplicación como usuario autenticado y no autenticado.

16.14 Realizar modelado de amenazas. El modelado de amenazas es el proceso de identificar y abordar fallas de diseño de seguridad en una aplicación antes de que se cree el código. Se lleva a cabo mediante individuos especialmente capacitados que evalúan el diseño de la aplicación y evalúan los riesgos de seguridad para cada punto de entrada y nivel de acceso. El objetivo es mapear la aplicación, la arquitectura y la infraestructura de manera estructurada para entender sus debilidades.

Control 17: Gestión de Respuesta ante Incidentes

Establecer un programa para desarrollar y mantener una capacidad de respuesta ante incidentes (por ejemplo, políticas, planes, procedimientos, roles definidos, capacitación y comunicaciones) con el fin de prepararse, detectar y responder rápidamente a un ataque.

17.1 Designar a una persona clave, y al menos un respaldo, que gestionará el proceso de manejo de incidentes de la empresa. El personal de gestión es responsable de la coordinación y documentación de los esfuerzos de respuesta y recuperación ante incidentes y puede consistir en empleados internos de la empresa, proveedores de servicios o un enfoque híbrido. Si se utiliza un proveedor de servicios, se debe designar al menos a una persona interna de la empresa para supervisar cualquier trabajo de terceros. Revisar anualmente o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

17.2 Establecer y mantener información de contacto para las partes que deben ser informadas de incidentes de seguridad. Los contactos pueden incluir personal interno, proveedores de servicios, autoridades legales, proveedores de seguros cibernéticos, agencias gubernamentales relevantes, socios del Centro de Análisis e Intercambio de Información (ISAC), u otros interesados. Verificar los contactos anualmente para asegurar que la información esté actualizada.

17.3 Establecer y mantener un proceso documentado en la empresa para que el personal reporte incidentes de seguridad. El proceso incluye el tiempo de reporte, el personal al que se debe reportar, el mecanismo de reporte y la información mínima a ser reportada. Asegurar que el proceso esté públicamente disponible para toda la fuerza laboral. Revisar anualmente o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

17.4 Establecer y mantener un proceso documentado de respuesta ante incidentes que aborde roles y responsabilidades, requisitos de cumplimiento y un plan de comunicaciones. Revisar anualmente o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

17.5 Asignar roles y responsabilidades clave para la respuesta ante incidentes, incluyendo personal de las áreas legal, TI, seguridad de la información, instalaciones, relaciones públicas, recursos humanos, equipos de respuesta a incidentes y analistas. Revisar anualmente o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

17.6 Determinar cuáles serán los mecanismos primarios y secundarios que se utilizarán para comunicarse e informar durante un incidente de seguridad. Los mecanismos pueden incluir llamadas telefónicas, correos electrónicos, chat seguro o cartas de notificación. Tener en cuenta que ciertos mecanismos, como el correo electrónico, pueden verse afectados durante un incidente de seguridad. Revisar anualmente o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

17.7 Planificar y realizar ejercicios y escenarios rutinarios de respuesta ante incidentes para el personal clave involucrado en el proceso de respuesta a incidentes, con el fin de prepararse para responder a incidentes del mundo real. Los ejercicios deben probar los canales de comunicación, la toma de decisiones y los flujos de trabajo. Realizar pruebas al menos anualmente.

17.8 Realizar revisiones posteriores al incidente. Las revisiones posteriores a un incidente ayudan a prevenir la recurrencia del mismo mediante la identificación de lecciones aprendidas y acciones de seguimiento.

17.9 Establecer y mantener umbrales para incidentes de seguridad, incluyendo, como mínimo, la diferenciación entre un incidente y un evento. Ejemplos pueden incluir: actividad anormal, vulnerabilidad de seguridad, debilidad de seguridad, violación de datos, incidente de privacidad, etc. Revisar anualmente o cuando ocurran cambios significativos en la empresa que puedan afectar esta salvaguarda.

Control 18: **Pruebas de Penetración**

Probar la efectividad y resiliencia de los activos empresariales mediante la identificación y explotación de debilidades en los controles (personas, procesos y tecnología), y la simulación de los objetivos y acciones de un atacante.

18.1 Establecer y mantener un programa de pruebas de penetración apropiado al tamaño, complejidad, industria y nivel de madurez de la empresa. Las características del programa de pruebas de penetración incluyen el alcance, como red, aplicaciones web, interfaces de programación de aplicaciones (API), servicios alojados y controles físicos de las instalaciones; la frecuencia; limitaciones, como horarios aceptables y tipos de ataques excluidos; información de contacto; remediación, como la forma en que los hallazgos serán canalizados internamente; y requisitos retrospectivos.

18.2 Realizar pruebas de penetración externas periódicas basadas en los requisitos del programa, al menos una vez al año. Las pruebas de penetración externas deben incluir reconocimiento empresarial y del entorno para detectar información explotable. Las pruebas de penetración requieren habilidades y experiencia especializadas, y deben ser llevadas a cabo por una parte calificada. Las pruebas pueden ser de caja blanca o caja negra.

18.3 Remediar los hallazgos de las pruebas de penetración de acuerdo con el proceso documentado de remediación de vulnerabilidades de la empresa. Esto debe incluir la determinación de una línea de tiempo y el nivel de esfuerzo con base en el impacto y la priorización de cada hallazgo identificado.

18.4 Validar las medidas de seguridad después de cada prueba de penetración. Si se considera necesario, modificar las reglas y capacidades para detectar las técnicas utilizadas durante las pruebas.

18.5 Realizar pruebas de penetración internas periódicas basadas en los requisitos del programa, al menos una vez al año. Las pruebas pueden ser de caja blanca o caja negra.

APÉNDICE I

Metodologías para Evaluar la Razonabilidad de la Ciberseguridad

Las dos oportunidades más evidentes para aplicar una prueba de razonabilidad de los controles de ciberseguridad se presentan cuando las empresas (gestores de riesgos) están planificando o evaluando las medidas de protección (controles y salvaguardas) que implementan y operan, y cuando una autoridad legal (jueces) debe determinar si dichos controles y salvaguardas son razonables. Las autoridades legales pueden ser jueces, jurados o árbitros que determinan la responsabilidad después de un incidente de seguridad, o bien reguladores que, durante auditorías o investigaciones, evalúan la conformidad de los programas de ciberseguridad.

Este apéndice describe recursos públicos disponibles que modelan cómo pueden realizarse estas pruebas "ex ante" y "ex post" para determinar la razonabilidad en cada escenario.

Método de Evaluación de Riesgos del Center for Internet Security

El Center for Internet Security publicó un método de evaluación de riesgos (Center for Internet Security Risk Assessment Method, o CIS RAM)[30] en 2018 para ayudar a las organizaciones a determinar si su aplicación de los Controles del CIS demostraría un equilibrio adecuado entre costo y beneficio. CIS RAM se basa en el Análisis de Riesgos basado en el Deber de Cuidado (DoCRA, por sus siglas en inglés).[31]

El proceso de evaluación de riesgos del CIS RAM se asemeja a muchos otros, como las Publicaciones Especiales 800-30[32] del NIST, ISO 27005,[33] y FAIR,[34] en tanto que el Riesgo se calcula en términos de Impacto y Probabilidad (por ejemplo, R = I x P). Otras variaciones incluyen factores adicionales, como el tiempo hasta el evento, vulnerabilidad, atractivo del objetivo y otras características del riesgo.

CIS RAM exige que el análisis de riesgos también siga un conjunto de principios alineados con el deber de cuidado y con definiciones comunes de razonabilidad. Estos principios son:

1. El análisis de riesgos debe considerar los intereses de todas las partes que podrían resultar perjudicadas por el riesgo.
2. Los riesgos deben reducirse a un nivel que no requiera una reparación para ninguna parte.
3. Las salvaguardas no deben ser más onerosas que los riesgos contra los que protegen.

Esto garantiza que cada análisis de riesgos evalúe el potencial de daño que puede afectar los objetivos internos de la empresa (por ejemplo, rentabilidad), su misión (por ejemplo, curar pacientes,

educar estudiantes, proveer alimentos o fabricar productos), y sus obligaciones de prevenir daño a terceros (lo cual podría incluir preservar la privacidad, prevenir el fraude o el daño físico).

CIS RAM instruye a los gestores de riesgos a evaluar tanto el estado actual del riesgo, los riesgos asociados con una salvaguarda recomendada, y sus alternativas.

CIS RAM también exige que una empresa establezca una definición de aceptación de riesgos que sea aceptable para todas las partes previsiblemente afectadas. De este modo, un gestor de riesgos puede determinar si los riesgos eran aceptables o no. CIS RAM incluye el concepto de un "tope de impacto": un impacto máximo evaluado como lo suficientemente bajo como para no requerir mitigación del riesgo.

Desde su publicación, CIS RAM, DoCRA y los principios de DoCRA han sido citados o utilizados por reguladores de EE. UU. como métodos para determinar si los programas de ciberseguridad son razonables. Véase el Apéndice J para casos específicos.

Comentario del Sedona Conference sobre una Prueba de Seguridad Razonable

El Sedona Conference, una organización no partidista y sin fines de lucro que publica documentos y guías sobre tecnología y derecho, publicó un documento en 2021[35] que ofrece un modelo útil para aplicar el análisis de riesgos al evaluar la razonabilidad de medidas de protección. El propósito del documento fue ayudar a los jueces (jueces, reguladores, mediadores y otros) a determinar, después de una violación de datos, si la organización vulnerada empleó medidas razonables de ciberseguridad para proteger los datos. El documento sugiere que la responsabilidad de la empresa puede argumentarse a favor o en contra con base en un proceso de dos pasos:

1. Determinar si la organización aplicó un estándar de cuidado (por ejemplo, ¿siguió los Controles del CIS como parte de su programa de ciberseguridad?)
2. Si no fue así, y la organización sí implementó algunas medidas de protección, determinar si existían una o más acciones protectoras alternativas (controles o salvaguardas) que deberían haberse aplicado en proporción al riesgo potencial, su impacto y probabilidad. Si el demandante o el regulador sugiere una acción protectora cuyo costo añadido habría sido menor que el beneficio añadido (la reducción del riesgo), entonces la inclusión de esa acción protectora—según el documento del Sedona Conference—no habría sido irrazonable.

Diferencias entre estos Enfoques de Evaluación

La prueba de seguridad razonable del Sedona Conference difiere del CIS RAM en dos aspectos importantes.

1. Como prueba retrospectiva, determina si los controles alternativos habrían sido más razonables que el control vulnerado. Los demandantes y jueces tienen la ventaja de la retrospectiva, que los gestores de riesgos no poseen antes del incidente. Un gestor de riesgos puede haber evaluado un control original como razonable en el momento del incidente, sin haber evaluado cada otro control posible con una mejor relación costo-beneficio.

2 CIS RAM incluye el concepto de un tope (cap), mientras que el documento del Sedona Conference no lo hace.

De este modo, la prueba del juez y la del gestor de riesgos son apropiadas para sus respectivos roles. El gestor de riesgos busca controles y salvaguardas que evalúa como razonables, según lo que sabe, lo que prevé y sus intereses empresariales legítimos. El rol del juez es determinar si el daño inaceptable era evitable dentro de las posibilidades de la empresa.

En ambos casos, sin embargo, tanto el gestor de riesgos como el juez reconocen que la seguridad perfecta no es alcanzable. Las medidas de protección no siempre pueden evitar el daño, y las empresas no siempre pueden implementar y operar medidas ideales de protección. En lugar de exigir un estado perfecto e inalcanzable de seguridad, tanto las comunidades legales como las de ciberseguridad han recurrido al análisis de riesgos para al menos determinar si una empresa aplicó medidas de seguridad suficientes, dadas su misión, sus objetivos y sus obligaciones hacia otros.

APÉNDICE J

Acciones de Cumplimiento de los Fiscales Generales Estatales en Demandas por Violaciones de Datos

Al hacer referencia a guías y metodologías existentes como el Estándar de Análisis de Riesgo basado en el Deber de Cuidado (Estándar DoCRA),[36] el Método de Evaluación de Riesgos del Center for Internet Security (CIS RAM),[37] una herramienta basada en los Controles del CIS — los cuales, como se ha discutido a lo largo de esta guía, se están convirtiendo en un estándar de facto global en ciberseguridad— y el "Comentario del Sedona Conference sobre una Prueba de Seguridad Razonable", varios Fiscales Generales Estatales han concluido acciones de cumplimiento contra entidades que sufrieron una violación de datos, exigiendo que dichas entidades demuestren controles de seguridad razonables en adelante.

Estados y casos de ejemplo incluyen:

Año	Caso
2021	**Pensilvania** utiliza DoCRA y CIS RAM para definir salvaguardas razonables en una demanda por violación de datos. *Pensilvania v Earl Enterprises:* https://thesedonaconference.org/sites/default/files/meeting_paper/02-08.pdf
2022	**Pensilvania** utiliza DoCRA, CIS RAM y el documento del Sedona Conference para definir salvaguardas razonables en una demanda por violación de datos. *Pensilvania v Hanna Andersson:* https://thesedonaconference.org/sites/default/files/meeting_paper/02-07.pdf
2022	**Siete estados** utilizan los principios de DoCRA como prueba de seguridad razonable en una demanda por violación de datos. *Pensilvania v Wawa*. Estos estados incluyen Pensilvania, Nueva Jersey, Delaware, Maryland, Washington D.C., Virginia y Florida. https://thesedonaconference.org/sites/default/files/meeting_paper/02-06.pdf
2022	**Dos estados** (Pensilvania y Nueva York) utilizan DoCRA, CIS RAM y el documento del Sedona Conference para definir salvaguardas razonables en una demanda por violación de datos. *Pensilvania v Herff Jones:* https://thesedonaconference.org/sites/default/files/meeting_paper/02-05.pdf

2023	**Dos estados** (Pensilvania y Ohio) utilizan DoCRA, CIS RAM y el documento del Sedona Conference para definir salvaguardas razonables en una demanda por violación de datos. *Pensilvania v DNA Diagnostics Center, Inc.:* https://thesedonaconference.org/sites/default/files/meeting_paper/02-04.pdf

APÉNDICE K

Resumen histórico del mosaico de leyes y directivas federales sobre ciberseguridad

A continuación, se proporciona información adicional sobre las leyes y directivas federales en materia de ciberseguridad incluidas en la línea de tiempo gráfica de la Sección 3 de este documento:

En 2002, la Ley de Modernización de la Seguridad de la Información Federal (FISMA, por sus siglas en inglés) estableció la base para la protección de las redes civiles federales.[38] Con la enmienda de 2014, FISMA exige ahora que "las agencias, al implementar sus programas de seguridad de TI, deben seguir la orientación emitida por la OMB y los estándares promulgados por el NIST."[39] Sin embargo, FISMA no obliga a las agencias a implementar estrategias específicas de ciberseguridad, ni a aplicar estándares determinados o utilizar herramientas concretas.[40]

También en 2002, la Ley Sarbanes-Oxley (SOX)[41] buscó proteger a los inversionistas mediante la mejora de la precisión y confiabilidad de las divulgaciones corporativas realizadas conforme a las leyes de valores de EE. UU. SOX dio lugar a un enfoque más riguroso sobre los controles de tecnología de la información, ya que estos respaldan el procesamiento financiero y, por lo tanto, entran en el ámbito de la evaluación del control interno por parte de la administración. SOX exige que cualquier empresa que cotice en bolsa tenga políticas formales de seguridad de datos, así como que comunique y haga cumplir dichas políticas.

La Ley de Portabilidad y Responsabilidad del Seguro de Salud de 1996 (HIPAA), enmendada por la Ley de Tecnología de la Información de la Salud para la Salud Económica y Clínica de 2009 (HITECH), establece estándares nacionales para que los proveedores de atención médica, los planes de seguro médico, las entidades de compensación de datos médicos y sus socios comerciales cumplan con los requisitos de privacidad y seguridad de los registros médicos en papel y electrónicos.[42] HIPAA lo hace con un alto grado de complejidad, a través de una Norma de Privacidad, una Norma de Seguridad complementaria y salvaguardas específicas —administrativas, físicas y técnicas— que, a su vez, están compuestas por varios estándares, cada uno de los cuales consta de una o más especificaciones de implementación.[43]

En 2018, el Congreso creó la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA),[44] que actúa principalmente como la agencia líder de EE. UU. para proteger las redes civiles federales. CISA también lidera la consulta y coordinación con gobiernos estatales, locales, tribales y territoriales, así como con el sector privado, en temas de infraestructura crítica y ciberseguridad.[45]

En 2022, el Congreso aprobó la Ley de Notificación de Incidentes Cibernéticos para Infraestructura Crítica, que establece nuevos requisitos significativos para que las organizaciones de infraestructura crítica en EE. UU. reporten incidentes cibernéticos y pagos de rescate al Gobierno Federal.[46]

Aunque existen otros estatutos federales que impactan la ciberseguridad de alguna manera, ninguno establece un estándar mínimo específico que se aplique a todas las organizaciones en todos los sectores.

Las regulaciones federales exigen que algunas organizaciones cumplan con ciertos estándares de ciberseguridad, lo que agrega aún más complejidad e inconsistencia en el panorama. Estos incluyen:

- En 1999, la Ley Gramm–Leach–Bliley (GLBA)[47] modificó los requisitos en la industria bancaria y, en noviembre de 2000, conforme a la GLBA, la FTC emitió la Norma de Privacidad de la Información Financiera del Consumidor para abordar los requisitos de protección de "información personal no pública."[48] La Norma de Privacidad exige que los avisos de privacidad proporcionen una descripción precisa de las políticas y prácticas actuales relacionadas con la protección de la confidencialidad y seguridad de dicha información.[49]
- En 2003, entró en vigor la "Norma de Salvaguardas" de la FTC.[50] Según sus enmiendas, la Norma exige que las instituciones financieras bajo jurisdicción de la FTC implementen salvaguardas razonables para mantener segura la información de los clientes y que determinen dichas salvaguardas mediante una evaluación de riesgos.[51] En octubre de 2023, la FTC publicó una nueva enmienda que exige a las instituciones financieras informar a la agencia sobre ciertas violaciones de datos y otros eventos de seguridad.[52] A lo largo de los años, la FTC ha emprendido numerosas acciones legales contra organizaciones que han violado los derechos de privacidad de los consumidores o no han protegido adecuadamente información sensible de los mismos.[53] En apoyo a FISMA, el Departamento de Comercio de EE. UU. publicó en 2006 la Publicación de Normas Federales de Procesamiento de Información (FIPS PUB 200)[54] sobre Requisitos Mínimos de Seguridad para Información y Sistemas de Información Federales. Si bien FISMA ordenó la promulgación de estándares federales para requisitos mínimos de seguridad para información y sistemas de información dentro de categorías específicas definidas en FISMA, no especificó estándares concretos. FIPS 200 "establece los requisitos mínimos de seguridad para la información y los sistemas de información federales."[55]
- En julio de 2023, la Comisión de Bolsa y Valores (SEC) adoptó normas que exigen a las empresas que cotizan en bolsa divulgar todos los incidentes cibernéticos relevantes mediante un formulario estándar de la SEC, a más tardar cuatro días hábiles después de determinar que el incidente es material.[56] La norma también requiere una divulgación anual de todos los procesos de gestión de riesgos cibernéticos.[57]

- Las empresas que venden bienes o servicios al gobierno federal deben cumplir con ciertos estándares mínimos de ciberseguridad establecidos por el Reglamento Federal de Adquisiciones (FAR), el cual exige que los contratistas del gobierno sigan quince requisitos y procedimientos básicos de protección para salvaguardar los sistemas utilizados en la recopilación, procesamiento, mantenimiento, uso, intercambio, difusión o eliminación de Información de Contratos Federales.[58]
- Las empresas que venden bienes o servicios al Departamento de Defensa de EE. UU. (DOD) pueden estar obligadas a cumplir con los estándares mínimos de ciberseguridad establecidos en el Suplemento del Reglamento Federal de Adquisiciones de Defensa (DFARS), si esos productos no están disponibles comercialmente fuera de estantería.[59]
- Como ejemplo final, en 2019, el Consejo de Examinación de Instituciones Financieras Federales (FFIEC) recomendó un enfoque estandarizado para evaluar la preparación en ciberseguridad, sugiriendo los Controles de Seguridad Críticos del CIS como una de cuatro herramientas específicas. El FFIEC establece principios, estándares y formularios de informe uniformes para promover la uniformidad en la supervisión de instituciones financieras.[60]

APÉNDICE L

Lista de Verificación de Políticas de Razonabilidad

Los siguientes elementos comprenden aspectos esenciales de políticas que una organización debe aplicar para cumplir con las directrices de razonabilidad presentadas en esta guía. Una organización debe documentar cuidadosamente los pasos que toma para abordar, implementar y mantener cada uno de estos elementos. Además, estas actividades deben realizarse de manera recurrente para mantener un programa de ciberseguridad actualizado.

1. Comprender la misión, las partes interesadas y las obligaciones de la organización
2. Desarrollar e implementar un programa de ciberseguridad*
3. Identificar recursos: fondos, personal, funciones subcontratadas, herramientas automatizadas
4. Seguir un marco o estándar de ciberseguridad reconocido por la industria
5. Medir la conformidad con el marco y mitigar los hallazgos para asegurar el cumplimiento continuo de su programa
6. Realizar evaluaciones periódicas de riesgos conforme a la metodología definida en el programa de ciberseguridad, y mitigar los hallazgos
7. Realizar evaluaciones independientes periódicas del programa de ciberseguridad y mitigar los hallazgos

Elementos de un Programa de Ciberseguridad

- [ ] Proceso y criterios para identificar y proteger información del mismo tipo abordado en la ley de protección de datos
- [ ] Roles y responsabilidades
- [ ] Políticas internas y requisitos de aplicacións
- [ ] Capacitación regular en ciberseguridad y concientización para el personal
- [ ] Metodología de evaluación de riesgos (incluye daño a la organización y a terceros; establece una base para aceptar o mitigar los hallazgos de riesgos)
- [ ] Proceso y políticas para mantener un estado “seguro” (por ejemplo, actualizaciones de software, eliminación de software innecesario y gestión de cuentas privilegiadas)
- [ ] Proceso de recuperación de datos

El Apéndice H proporciona una lista completa de controles de seguridad y sus acciones subyacentes.

NOTAS FINALES

1 Los lectores notarán que los términos privacidad de datos, seguridad de datos, seguridad de la información y ciberseguridad se utilizan a lo largo del documento. Estos términos están relacionados; de hecho, la existencia de múltiples términos es consecuencia del entorno de comunicaciones digitales, complejo y en evolución. Sin embargo, existen diferencias sutiles entre la mayoría de ellos. Las definiciones se proporcionan en el Apéndice A.

2 Center for Internet Security [CIS]. CIS Critical Security Controls. Recuperado de https://www.cisecurity.org/controls

3 Virginia Consumer Data Protection Act. Va. Code § 59.1-578(A)(3) (énfasis añadido). Recuperado del Código Legal de Virginia: https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

4 Buckbee, M. (2023, 16 de junio). What the H**L Does Reasonable Data Security Really Mean? [Publicación en blog del autor]. Varonis Blog/Privacy & Compliance. Recuperado de https://www.varonis.com/blog/what-the-hl-does-reasonable-data-security-really-mean

5 The Sedona Conference, Commentary on a Reasonable Security Test, 22 SEDONA CONF. J. 345 (2021). Recuperado de https://thesedonaconference.org/sites/default/files/publications/5_Reasonable_Security_Test_0.pdf

6 Center for Internet Security. CIS Risk Assessment Model (CIS RAM) Version 2.1 [Material del curso]. https://learn.cisecurity.org/cis-ram

7 Cyber Incident Reporting for Critical Infrastructure Act. (15 de marzo de 2022). En Consolidated Appropriations Act (Ley Pública 117-103). [Legislación]. Recuperado de https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf

Hoja informativa de CISA: https://www.cisa.gov/sites/default/files/2022-11/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf

8 National Conference of State Legislatures. Security Breach Notification Laws (actualizado 17 de enero de 2022) recuperado de https://www.ncsl.org/technology-and-communication/security-breach-notification-laws

9 National Conference of State Legislatures. (s.f.). Security breach notification laws. Recuperado de: https://www.ncsl.org/technology-and-communication/2022-security-breach-legislation Véase también: Privacy Rights Clearinghouse. (2023). United States data breach notification laws 2023 report. Recuperado de https://privacyrights.org/resources/united-states-data-breach-notification-united-states-2023-report

10 201 Mass. Reg. 17.03. 201 CMR 17.00: Standards for the protection of personal information of residents of the Commonwealth. Recuperado de https://www.mass.gov/regulations/201-CMR-1700-standards-for-the-protection-of-personal-information-of-ma-residents

11 Departamento de Servicios Financieros del Estado de Nueva York. (1 de noviembre de 2023). Segunda enmienda al 23 NYCRR 500. Recuperado de https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf

12 Cybersecurity Bankers Association [CSBA]. (2017). Cybersecurity 101: A resource guide for financial sector executives. Recuperado de https://www.csbs.org/sites/default/files/cybersecurity101_2019_final_with_links.pdf

13 Federal Communication Commission. (2022). Notice of proposed rulemaking [FCC 22-83] (pp. 13–14) (recomienda los CIS Critical Security Controls como uno de los dos estándares). Recuperado de https://docs.fcc.gov/public/attachments/FCC-22-82A1.pdf

14 Deloitte. (2016). Beneath the surface of a cyberattack: A deeper look at business impacts. Recuperado de https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf

15 Departamento de Justicia de California. (2016). California data breach report. Recuperado de https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

16 Nevada Revised Statutes [NRS] § 603A.210. (2019). Recuperado de https://www.leg.state.nv.us/nrs/nrs-603a.html

17 Ohio Revised Code § 1354.01-1354.05 (2018). Recuperado de https://codes.ohio.gov/ohio-revised-code/section-1354.01

18 Id.

19 Ver, por ejemplo, id.

20 National Institute of Standards and Technology [NIST]. (2020, septiembre). Security and privacy controls for information systems and organizations (Publicación Especial 800-53, Revisión 5). Recuperado de https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

21 Payment Card Industry Security Standards Council. (s.f.). PCI Data Security Standard [PCI DSS]. Recuperado de https://www.pcisecuritystandards.org/standards/

22 International Organization for Standardization [ISO]. (2022). ISO/IEC 27005:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Guía para la gestión de riesgos de seguridad de la información (4ª ed.). Recuperado de https://www.iso.org/standard/80585.html

23 Verizon Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

24 Blueprint for Ransomware Defense: An Action Plan for Ransomware Mitigation, Response, and Recovery. Institute for Security and Technology, 2022. https://securityandtechnology.org/ransomwaretaskforce/blueprint-for-ransomware-defense/

25 Center for Internet Security [CIS]. (2021). CIS Community Defense Model v2.0. Recuperado de https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

26 Id.

27 Id.

28 The Cost of Cyber Defense: Implementation Group 1. Center for Internet Security, 2023. https://learn.cisecurity.org/l/799323/2023-08-02/4t3qkj/799323/1694810927NC0iZQGR/CIS_Controls_Cost_of_Cyber_Defense_2023_08.pdf

29 CIS Critical Security Controls Navigator. Center for Internet Security (actualizado regularmente). https://www.cisecurity.org/controls/cis-controls-navigator/

30 Center for Internet Security. (s.f.). CIS Risk Assessment Method (CIS RAM). Recuperado de https://learn.cisecurity.org/cis-ram

31 The DoCRA Council. (2021). Duty of Care Risk Analysis [DoCRA] Standard v 0.6 [Documento]. Recuperado de https://www.docra.org/wp-content/uploads/2021/06/Duty-of-Care-Risk-Analysis-Standard-Draft-20200907.pdf

32 National Institute of Standards and Technology (NIST). (2012). Guide for conducting risk assessments (NIST Publicación Especial 800-30 Rev. 1). Recuperado de https://csrc.nist.gov/pubs/sp/800/30/r1/final

33 International Organization for Standardization (ISO). (2022). ISO/IEC 27005: Seguridad de la información, ciberseguridad y protección de la privacidad – Guía para la gestión de riesgos de seguridad de la información. Recuperado de https://www.iso.org/standard/80585.html

34 Factor Analysis of Information Risk (FAIR). [The FAIR Institute]. Recuperado de https://www.fairinstitute.org/what-is-fair

35 The Sedona Conference, Commentary on a Reasonable Security Test, 22 SEDONA CONF. J. 345 (2021). https://thesedonaconference.org/sites/default/files/publications/5_Reasonable_Security_Test.pdf

36 The DoCRA Council. (2021). Duty of Care Risk Analysis [DoCRA] Standard v 0.6 [Documento]. Recuperado de https://www.docra.org/wp-content/uploads/2021/06/Duty-of-Care-Risk-Analysis-Standard-Draft-20200907.pdf

37 Center for Internet Security. (s.f.). CIS Risk Assessment Method (CIS RAM). Recuperado de https://learn.cisecurity.org/cis-ram

38 Véase Federal Information Security Management Act of 2002. En E-Government Act of 2002, Ley Pública 107-347. Recuperado de https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf

39 Congressional Research Service [CRS]. (29 de septiembre de 2021). Federal cybersecurity: Background and issues for Congress [Informe No. R46926]. Recuperado de https://crsreports.congress.gov/product/pdf/R/R46926. Véase también Federal Information Security Modernization Act of 2014, Ley Pública 113-283. Recuperado de https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

40 Id.

41 Véase Sarbanes-Oxley Act of 2002, Ley Pública No. 107-204. Recuperado de https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf

42 Congressional Research Service [CRS]. (Actualizado el 17 de abril de 2015). HIPAA Privacy, Security, Enforcement, and Breach Notification Standards [Informe No. R43991]. Recuperado de https://crsreports.congress.gov/product/pdf/R/R43991. Véase también Health Insurance Portability and Accountability Act of 1996, Ley Pública No. 104-191. Recuperado de https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf

43 Id.

44 Cybersecurity and Infrastructure Security Agency Act of 2018, Ley Pública No. 115-278. Recuperado de https://www.congress.gov/bill/115th-congress/house-bill/3359/text

45 Id. en la Sección 2202 (e) (1) (I) y (N). Véase también: DHS CISA Cyber Mission Overview: https://www.dhs.gov/news/2022/10/03/cyber-mission-overview

46 Cyber Incident Reporting for Critical Infrastructure Act, Ley Pública No. 117-103 (15 de marzo de 2022). En Consolidated Appropriations Act, 2022 (H.R. 2471, 117º Congreso). Recuperado de https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf

47 Gramm-Leach-Bliley Act (GLBA), Ley Pública 106-102 (1999). Recuperado de https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm

48 Federal Trade Commission. (2000). Privacy of consumer financial information (16 C.F.R. Parte 313). Recuperado de https://www.ftc.gov/legal-library/browse/rules/financial-privacy-rule

49 Federal Trade Commission (FTC). "How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act" [sitio web de la FTC]. Recuperado de https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act

50 Federal Trade Commission. (9 de diciembre de 2021). Standards for safeguarding customer information (16 CFR Parte 314) [Revisión de la regla]. Federal Register, 86(236), 70272-70312. Recuperado de https://www.ftc.gov/system/files/ftc_gov/pdf/p145407_safeguards_rule.pdf

51 Id.

52 Federal Trade Commission. (9 de diciembre de 2021). Standards for safeguarding customer information (16 CFR Parte 314) [Revisión de la regla]. Federal Register, 86(236), 70272-70312. Recuperado de https://www.ftc.gov/system/files/ftc_gov/pdf/p145407_safeguards_rule.pdf

53 Federal Trade Commission (FTC). (s.f.). Privacy and security enforcement [Página temática]. Recuperado de https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement

54 National Institute of Standards and Technology (NIST). (2006). Federal Information Processing Standards (FIPS) Publication 200: Minimum Security Requirements for Federal Information and Information Systems. Recuperado de https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf

55 Id.

56 Securities and Exchange Commission. (26 de julio de 2023). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure [Regla final]. Federal Register, 88(144), 41900-41940. Recuperado de https://www.sec.gov/rules/final/2023/33-11216.pdf

57 Id.

58 Federal Acquisition Regulation (FAR) [Subparte 52.204-21, Salvaguarda básica de sistemas de información de contratistas cubiertos]. Recuperado de https://www.acquisition.gov/far/52.204-21

59 Defense Federal Acquisition Regulation Supplement [DFARS]. (20 de diciembre de 2018). 252.204-7012: Salvaguarda de información cubierta de defensa e informe de incidentes cibernéticos. Recuperado de https://business.defense.gov/Portals/57/Safeguarding%20Covered%20Defense%20Information%20-%20The%20Basics.pdf

60 Federal Financial Institutions Examination Council [FFIEC]. (28 de agosto de 2019). FFIEC encourages standardized approach to assessing cybersecurity preparedness [Comunicado de prensa]. Recuperado de https://www.ffiec.gov/press/pr082819.htm

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

www.cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
CenterforIntSec
TheCISecurity
cisecurity

CIS Center for Internet Security®

CIS Controls®