2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

Desafíos de la Seguridad Cibernética para Atender los Requerimientos Regulatorios y Evitar Sanciones

Camilo Correa Jaramillo

ASOCIACION BANCARIA DE PANAMA
ABP

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Agenda

- Introducción
- Ciberseguridad en la Actualidad
- Regulaciones
- Desafíos de la Ciberseguridad en el Cumplimiento Regulatorio
- Estrategias para Abordar los Desafíos
- Preparación para el Futuro
- Conclusiones y Recomendaciones Finales
- Preguntas y Respuestas

Introducción

Porqué las regulaciones son necesarias ?

Indica que durante los allanamientos realizados por la operación Gavilán en el Distrito Nacional, Santo Domingo, Independencia y San Pedro de Macorís contra los integrantes de la «red que *borraban fichas*», se ocuparon evidencias de los delitos imputados, como dispositivos **electrónicos, prueba de transferencias bancarias, armas de fuego, vehículos, dinero en efectivo, cédulas y copias de cédulas**.

¿A quiénes beneficiaban los imputados en operación Gavilán?

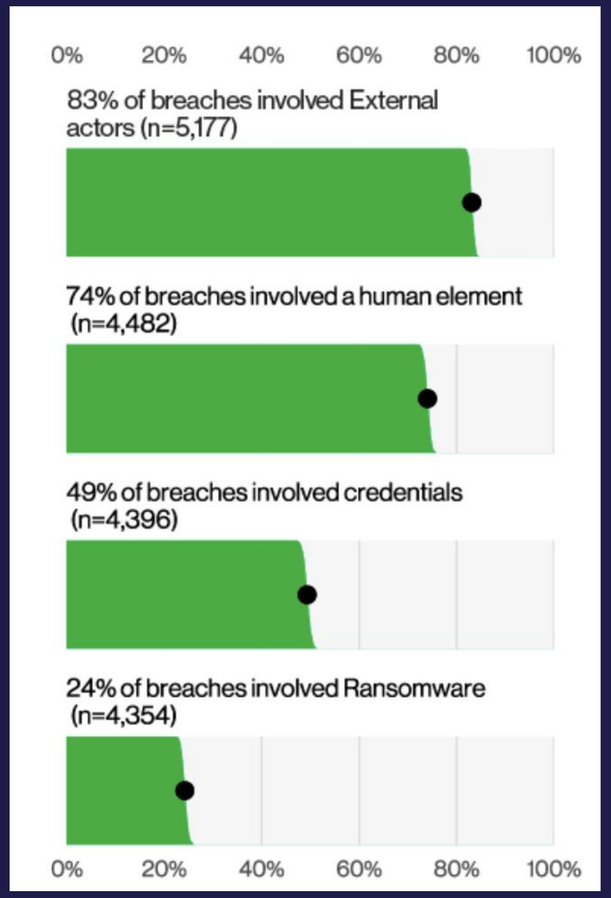
En el borrado de antecedentes penales ejecutado por esta red criminal **han sido beneficiados sicarios, narcotraficantes, violadores sexuales, imputados de violencia de género, por adulteración de alcohol, por secuestro,** llegando esta estructura al extremo de que *personas recluidas cumpliendo condena de hasta de 30 años figuren sin antecedentes penales en los registros oficiales.*

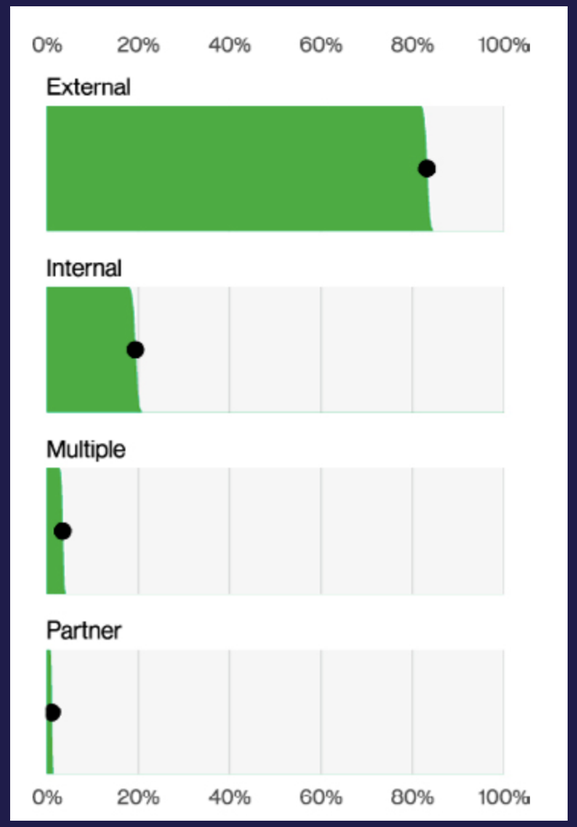
La staba
co ros de
la

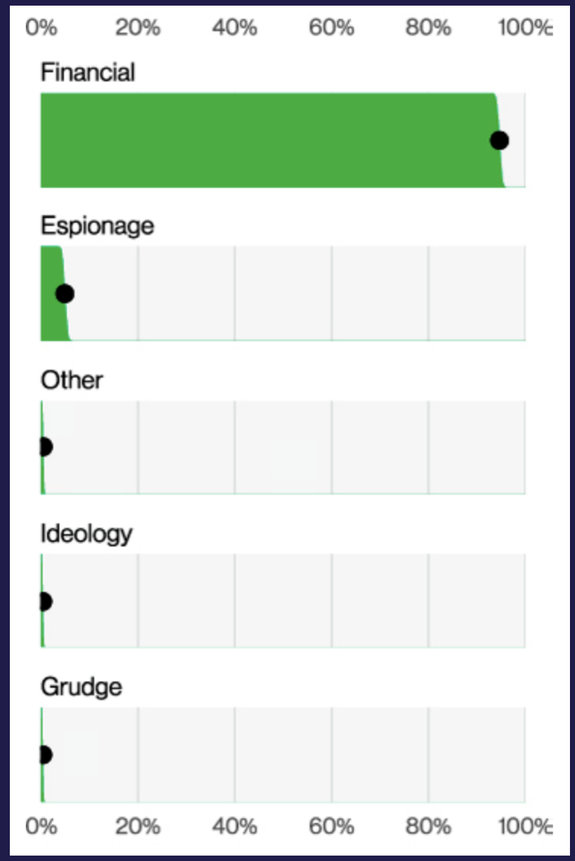
AES
atinoamericano
uridad Bancaria

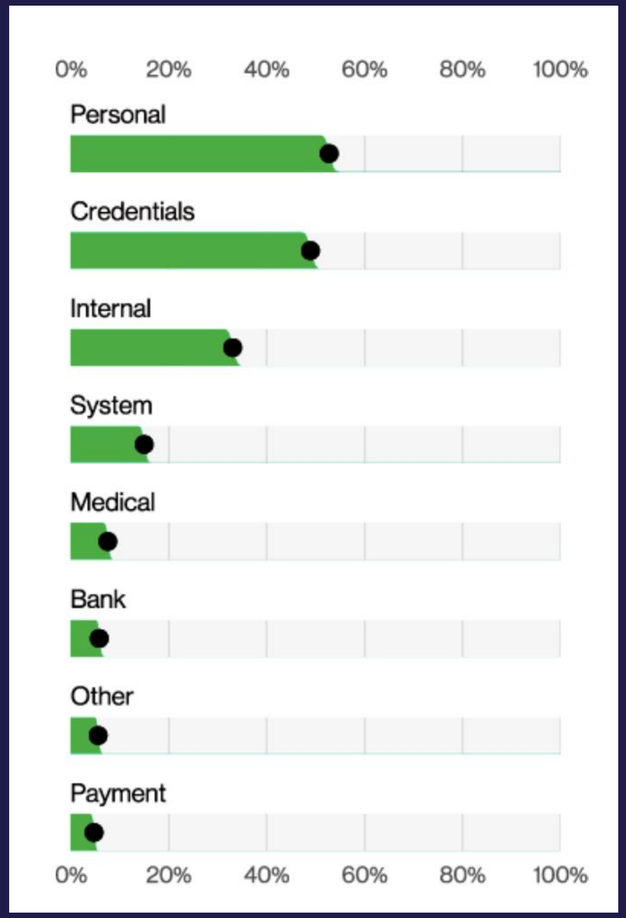
Fuente: https://puntacanainside.net/asi-eliminaban-las-fichas-operacion-gavilan/

Ciberseguridad en la Actualidad







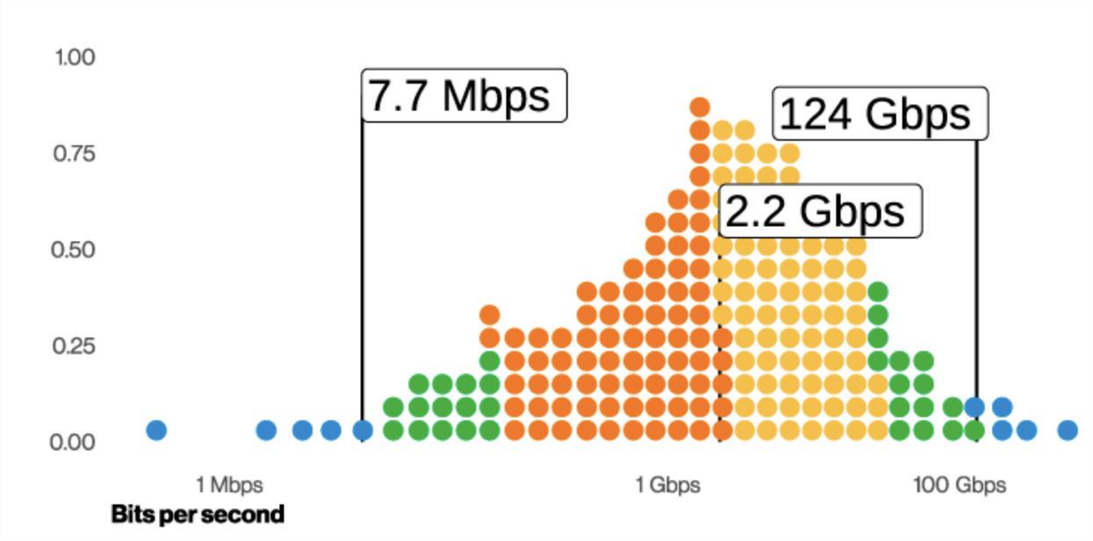


Fuente: https://www.verizon.com/business/resources/T1e7/reports/2023-data-breach-investigations-report-dbir.pdf

2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

Ciberseguridad en la Actualidad

Denial of Service



Privilege Misuse

Frequency	406 incidents, 288 with confirmed data disclosure
Threat actors	Internal (99%), Multiple (7%), External (6%), Partner (2%) (breaches)
Actor motives	Financial (89%), Grudge (13%), Espionage (5%), Convenience (3%), Fun (3%), Ideology (2%) (breaches)
Data compromised	Personal (73%), Medical (34%), Other (18%), Bank (12%), Payment (12%) (incidents)

Fuente: https://www.verizon.com/business/resources/T1e7/reports/2023-data-breach-investigations-report-dbir.pdf

Ciberseguridad en la Actualidad

Incidents

Asset	Accommodation (72)	Administrative (56)	Construction (23)	Education (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Mining + Utilities (21+22)	Other Services (81)	Professional (54)	Public Administration (92)	Real Estate (53)	Retail (44-45)	Transportation (48-49)
Embedded							1									
Kiosk/Term						6		1	1	1	1				11	1
Media	3		1	5	2	24	45	10	5			9	44	1	1	2
Network		1		1	1	15	6	37	9	3	5	6	9	2	2	2
Person	18	5	14	72	18	97	62	133	77	9	33	129	104	15	93	25
Server	239	34	71	434	420	1,750	397	1,968	1,501	126	113	1,301	961	65	361	202
User Dev	14	4	10	62	10	53	50	76	45	7	15	101	2,076	10	71	17

Fuente: https://www.verizon.com/business/resources/T1e7/reports/2023-data-breach-investigations-report-dbir.pdf

Ciberseguridad en la Actualidad

Breaches

Asset	Accommodation (72)	Administrative (56)	Construction (23)	Education (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Mining + Utilities (21+22)	Other Services (81)	Professional (54)	Public Administration (92)	Real Estate (53)	Retail (44-45)	Transportation (48-49)
Embedded							1									
Kiosk/Term						6		1	1	1	1				11	1
Media	3		1	5	2	23	40	10	5			7	9	1		2
Network				1	1	4	2	1	1		1	1	1			
Person	11	5	13	51	15	71	50	86	68	2	28	85	81	10	47	16
Server	58	28	56	190	88	421	344	303	217	38	85	372	256	46	166	78
User Dev	9	4	8	33	8	32	38	48	38	3	15	55	177	4	37	12

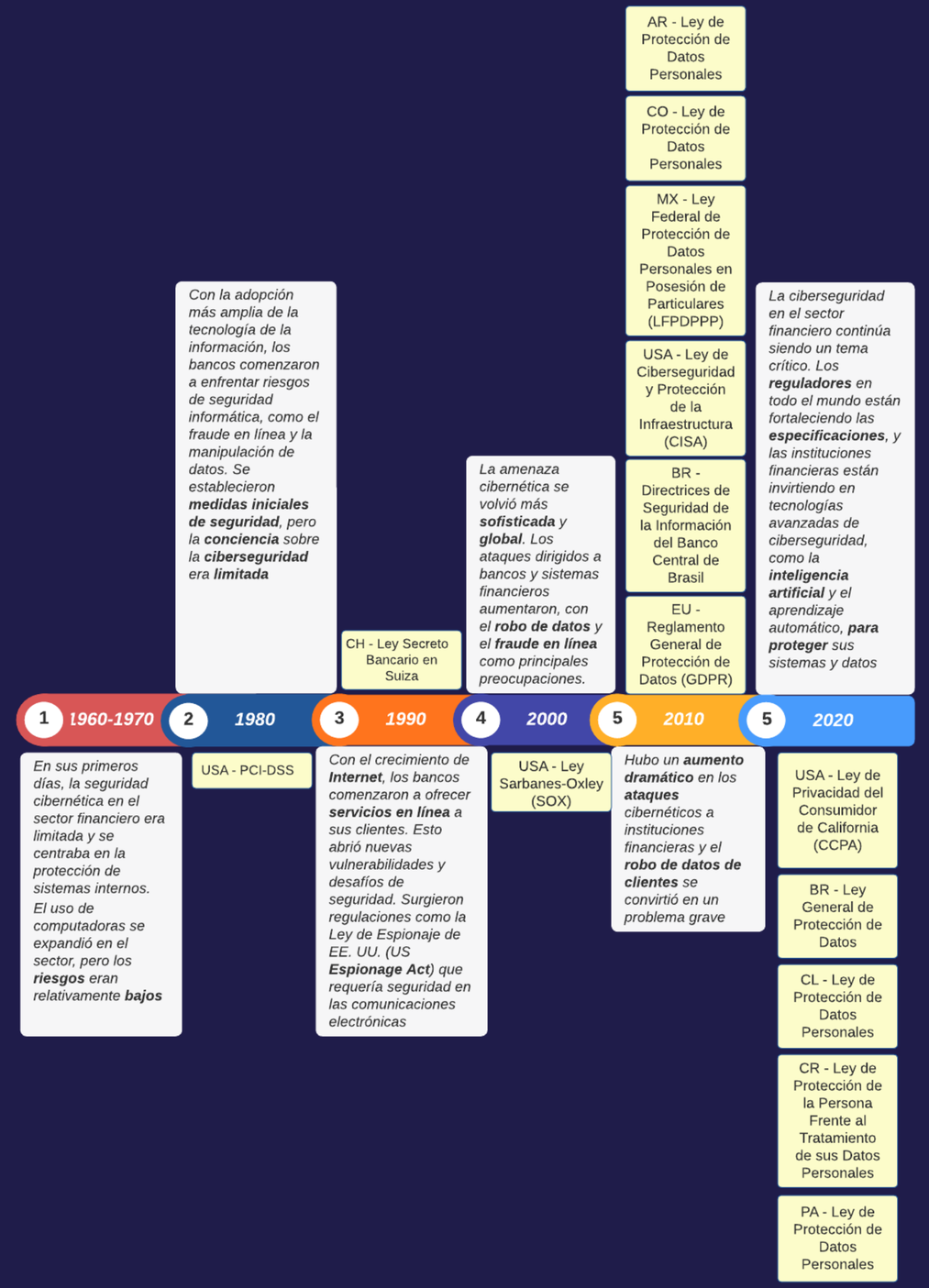
Fuente: https://www.verizon.com/business/resources/T1e7/reports/2023-data-breach-investigations-report-dbir.pdf

Ciberseguridad en la Actualidad

Region	Frequency	Top patterns	Threat actors	Actor motives	Data compromised
APAC	699 incidents, 164 with confirmed data disclosure	Social Engineering, System Intrusion and Basic Web Application Attacks represent 93% of breaches	External (92%), Internal (9%), Partner (2%), Multiple (2%) (breaches)	Financial (61%), Espionage (39%), Convenience (2%), Grudge (2%), Secondary (1%) (breaches)	Internal (56%), Secrets (42%), Other (33%), Credentials (29%) (breaches)
EMEA	2,557 incidents, 637 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 97% of breaches	External (98%), Internal (2%), Multiple (1%) (breaches)	Financial (91%), Espionage (8%), Ideology (1%), Fun (1%) (breaches)	Credentials (53%), Internal (37%), System (35%), Other (15%) (breaches)
LAC	535 incidents, 65 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 94% of breaches	External (95%), Internal (5%), Partner (2%), Multiple (2%) (breaches)	Financial (93%), Espionage (11%), Ideology (2%) (breaches)	System (55%), Internal (32%), Classified (23%), Credentials (23%), Other (19%) (breaches)
NA	9,036 incidents, 1,924 with confirmed data disclosure	System Intrusion, Basic Web Application Attacks and Social Engineering represent 85% of breaches	External (94%), Internal (12%), Multiple (9%), Partner (2%) (breaches)	Financial (99%), Espionage (1%), Grudge (1%) (breaches)	Credentials (67%), Internal (50%), Personal (38%), Other (24%) (breaches)

Fuente: https://www.verizon.com/business/resources/T1e7/reports/2023-data-breach-investigations-report-dbir.pdf

Regulaciones



Regulaciones

País	Nombre de la Regulación	Objetivo/Alcance	Fecha de Promulgación	Tipo de Sanción	Sanción Monetaria (si aplica)
Colombia	Ley 1581 de 2012	Normas generales para la protección de datos	2012	Administrativa	Hasta 2.000 salarios mínimos mensuales legales vigentes (SMLMV)
Perú	Ley N° 29733	Regula la protección de datos personales	2011	Administrativa	Varía según la gravedad
República Dominicana	Ley 172-13	Protección de Datos de Carácter Personal	2013	Administrativa	Varía según la gravedad
Argentina	Ley 141-1999	Protección de datos personales	2000	Administrativa y Penal	Hasta 100.000 pesos argentinos
Chile	Ley N° 19.628	Protección de datos personales	1999	Administrativa	Varía según el caso
Panamá	Ley N° 81	Protección de datos personales	2019	Administrativa	De 1,000 a 10,000 dólares
USA	California Consumer Privacy Act (CCPA)	Protección de datos de los residentes de California	2020	Civil	Hasta $7,500 por violación intencional

Desafíos

- Evolución de las Normativas
- Complejidad Legal y Normativa
- Falta de Conciencia Regulatoria
- Gestión de Datos Sensibles
- Necesidad de Informes y Auditorías
- Amenazas de Ciberseguridad en Constante Evolución
- Requisitos de Notificación de Brechas
- Costos de Cumplimiento
- Escasez de Talento en Ciberseguridad
- Globalización de Operaciones

Estrategias

Evolución de las Normativas	Software de gestión de cumplimiento que rastree y actualice automáticamente las regulaciones pertinentes y te notifique sobre los cambios
Complejidad Legal y Normativa	Asesores legales con experiencia en regulaciones relevantes, herramientas de gestión de cumplimiento
Falta de Conciencia Regulatoria	Soluciones de e-learning o software de formación para proporcionar a los empleados capacitación en línea sobre las regulaciones vigentes
Gestión de Datos Sensibles	Software de detección, cifrado de datos y gestión de acceso. Políticas de retención de datos y destrucción segura de información confidencial.
Necesidad de Informes y Auditorías	Automatizar el proceso de generación de informes y auditorías
Amenazas de Ciberseguridad en Constante Evolución	Implementar soluciones de detección de amenazas avanzadas respaldadas por inteligencia artificial y aprendizaje automático
Requisitos de Notificación de Brechas	Implementar mecanismos de detección y análisis forense adecuados
Costos de Cumplimiento	Concientizar y sensibilizar en prevención de riesgos. Diligencia debida
Escasez de Talento en Ciberseguridad	Automatización
Globalización de Operaciones	Uso de herramientas que permitan el cumplimiento de las diferentes regulaciones

Preparación para el Futuro

Conformed to Federal Register version

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 229, 232, 239, 240, and 249

[Release Nos. 33-11216; 34-97989; File No. S7-09-22]

RIN 3235-AM89

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

AGENCY: Securities and Exchange Commission.

Introducing the NIST Cybersecurity Framework 2.0 Reference Tool!

August 15, 2023

Nuevas normativas de ciberseguridad: la PSD3 y diferencias respecto a regulaciones anteriores

Publicado el 06/10/2023 por Fernando Fuentes en Seguridad Compartir:

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written justification as to why each is necessary.	**6.4.3.a** Examine policies and procedures to verify that processes are defined for managing all payment page scripts that are loaded and executed in the consumer's browser, in accordance with all elements specified in this requirement. **6.4.3.b** Interview responsible personnel and examine inventory records and system configurations to verify that all payment page scripts that are loaded and executed in the consumer's browser are managed in accordance with all elements specified in this requirement.	Scripts loaded and executed in the payment page can have their functionality altered without the entity's knowledge and can also have the functionality to load additional external scripts (for example, advertising and tracking, tag management systems). Such seemingly harmless scripts can be used by potential attackers to upload malicious scripts that can read and exfiltrate cardholder data from the consumer browser. Ensuring that the functionality of all such scripts is understood to be necessary for the operation of the payment page minimizes the number of scripts that could be tampered with. Ensuring that scripts have been explicitly authorized reduces the probability of unnecessary scripts being added to the payment page without appropriate management approval. Using techniques to prevent tampering with the script will minimize the probability of the script being modified to carry out unauthorized behavior, such as skimming the cardholder data from the payment page.
Customized Approach Objective		**Good Practice**
Unauthorized code cannot be present in the payment page as it is rendered in the consumer's browser.		Scripts may be authorized by manual or automated (e.g., workflow) processes. Where the payment page will be loaded into an inline frame (IFRAME), restricting the location that the payment page can be loaded from, using the parent page's Content Security Policy (CSP) can help prevent unauthorized content being substituted for the payment page.
Applicability Notes		*(continued on next page)*
This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

https://csrc.nist.gov/News/2023/just-released-nist-csf-2-0-reference-tool https://www.arsys.es/blog/psd3

Fuente: https://www.sec.gov/files/rules/final/2023/33-11216.pdf

Fuente: https://www.imperva.com/blog/about-complying-with-pci-6-4-3/pci-dss-tackles-client-side-attacks-everything-you-need-know-

Preparación para el Futuro

Gartner

El 10% de las organizaciones utilizará con éxito la privacidad como una ventaja competitiva. Las empresas están empezando a reconocer que un programa de privacidad puede permitirles utilizar los datos de manera más amplia, diferenciándose de la competencia y generando confianza con los clientes, socios, inversores y reguladores. Gartner recomienda que los líderes de seguridad apliquen un **estándar de privacidad integral de acuerdo con la Ley General de Protección de Datos Personales** (LGPD) para destacarse en un mercado cada vez más competitivo y crecer sin obstáculos.

Para 2026, el 70% de las juntas directivas incluirán un miembro con experiencia en ciberseguridad: para que los líderes de esta industria sean reconocidos como socios comerciales, deben reconocer el apetito por el riesgo de la junta directiva y la empresa. Esto significa no sólo mostrar cómo el programa de ciberseguridad evita que sucedan cosas malas, sino también **cómo mejora la capacidad de la empresa para asumir riesgos de manera efectiva**. Gartner recomienda que los CISO anticipen el cambio para promover y apoyar la seguridad cibernética a través del Consejo y establecer una relación más estrecha para mejorar la confianza y el apoyo.

https://es.cointelegraph.com/news/top-cybersecurity-predictions-for-2023-2024-according-to-gartner

Conclusiones

- La Ciberseguridad es una Prioridad Estratégica
- Evolución de las Regulaciones
- Complejidad y Desafíos Legales
- Tecnología y Automatización
- Gestión de Datos y Privacidad
- Respuesta a Incidentes y Notificación de Brechas
- Aprendizaje Continuo y Adaptación
- Diligencia Debida

Gracias!

CELAES 2023
Congreso Latinoamericano
de Seguridad Bancaria