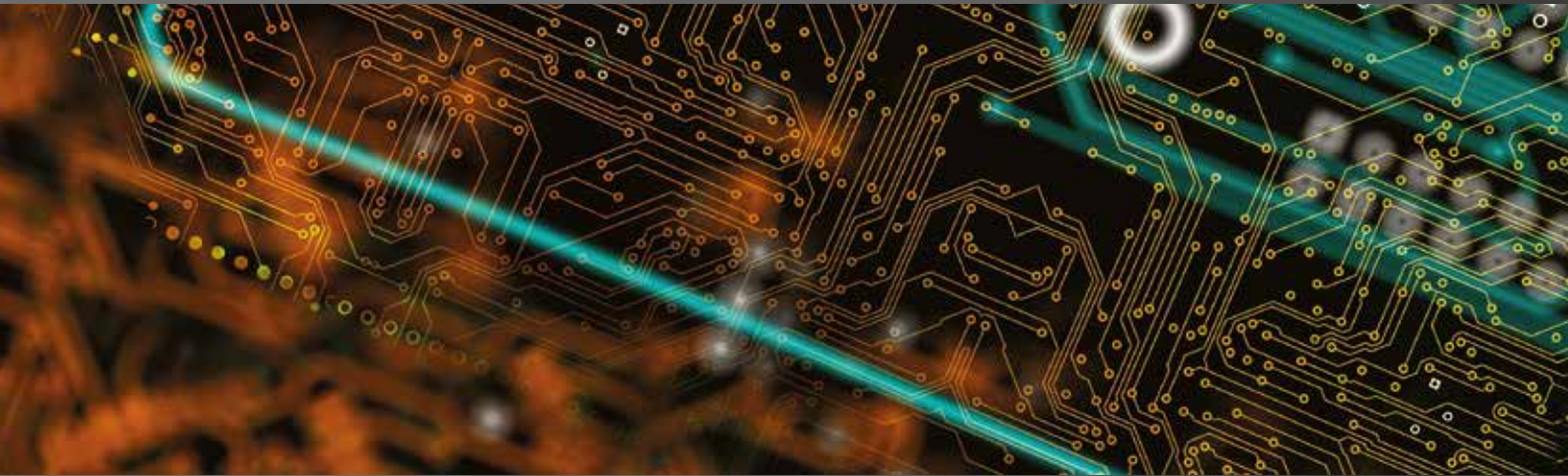


# International **Comparative** Legal Guides



## Cybersecurity **2021**

A practical cross-border insight into cybersecurity law

**Fourth Edition**

### Featuring contributions from:

Alburhan  
Allen & Overy LLP  
Ankura Consulting Group  
Creel, García-Cuellar, Aiza y Enríquez  
Drew & Napier LLC  
Eversheds Sutherland (Germany) LLP  
Hamdan AlShamsi Lawyers & Legal Consultants  
Ince  
Iwata Godo  
Kellerhals Carrard

King & Wood Mallesons  
Kluge Advokatfirma AS  
Lee & Ko  
Lee and Li, Attorneys-at-Law  
Leśniewski Borkiewicz & Partners (LB&P)  
Maples Group  
McMillan LLP  
Mori Hamada & Matsumoto  
Nikolinakos & Partners Law Firm  
Nyman Gibson Miralis

Pearl Cohen Zedek Latzer Baratz  
R&T Asia (Thailand) Limited  
Ropes & Gray LLP  
Rothwell Figg  
Rubino Avvocati  
Schönherr Rechtsanwälte GmbH  
Simion & Baci  
Sirius Legal  
Stehlin & Associés  
TIME DANOWSKY Advokatbyrå AB

**ICLG.com**

## Expert Chapters

- 1** **Get Stuffed! Are You Prepared for a Credential-Stuffing Attack?**  
Nigel Parker & Nathan Charnock, Allen & Overy LLP
- 5** **Current and Emerging Cybersecurity Threats and Risks**  
Robert Olsen, Daron M. Hartvigsen & Brandon Catalan, Ankura Consulting Group
- 10** **Phantom Responsibility: How Data Security and Privacy Lapses Lead to Personal Liability for Officers and Directors**  
Christopher Ott, Rothwell Figg
- 20** **Mitigating Cyber-Risk – A Boardroom Priority**  
Rory Macfarlane, Ince
- 24** **Why AI is the Future of Cybersecurity**  
Akira Matsuda & Hiroki Fujita, Iwata Godo

## Q&A Chapters

- 28** **Australia**  
Nyman Gibson Miralis: Dennis Miralis, Phillip Gibson & Jasmina Ceic
- 35** **Austria**  
Schönherr Rechtsanwälte GmbH: Christoph Haid, Veronika Wolfbauer & Michael Lindtner
- 42** **Belgium**  
Sirius Legal: Roeland Lembrechts & Bart Van den Brande
- 49** **Canada**  
McMillan LLP: Lyndsay A. Wasser & Kristen Pennington
- 58** **China**  
King & Wood Mallesons: Susan Ning & Han Wu
- 67** **England & Wales**  
Allen & Overy LLP: Nigel Parker & Nathan Charnock
- 75** **France**  
Stehlin & Associés: Frédéric Lecomte
- 82** **Germany**  
Eversheds Sutherland (Germany) LLP: Dr. Alexander Niethammer, Constantin Herfurth, Dr. David Rieks & Stefan Saerbeck
- 89** **Greece**  
Nikolinakos & Partners Law Firm: Dr. Nikos Th. Nikolinakos & Dina Th. Kouvelou
- 98** **Ireland**  
Maples Group: Claire Morrissey & Kevin Harnett
- 105** **Israel**  
Pearl Cohen Zedek Latzer Baratz: Haim Ravia & Dotan Hammer
- 112** **Italy**  
Rubino Avvocati: Alessandro Rubino & Gaetano Citro
- 120** **Japan**  
Mori Hamada & Matsumoto: Hiromi Hayashi, Masaki Yukawa & Daisuke Tsuta
- 129** **Korea**  
Lee & Ko: Hwan Kyoung Ko & Kyung Min Son
- 136** **Mexico**  
Creel, García-Cuellar, Aiza y Enríquez: Begoña Cancino
- 142** **Norway**  
Kluge Advokatfirma AS: Stian Hultin Oddbjørnsen, Ove André Vanebo, Iver Jordheim Brække & Mari Klungsøyr Kristiansen
- 149** **Poland**  
Leśniewski Borkiewicz & Partners (LB&P): Mateusz Borkiewicz, Grzegorz Leśniewski & Jacek Cieśliński
- 158** **Romania**  
Simion & Baci: Ana-Maria Baci, Cosmina Maria Simion, Andrei Cosma & Andrei Nicolae Dumbravă
- 166** **Saudi Arabia**  
Alburhan: Saeed Algarni, Mohammed Ashbah & Muhanned Alqaity
- 172** **Singapore**  
Drew & Napier LLC: Lim Chong Kin, David N. Alfred & Albert Pichlmaier
- 182** **Sweden**  
TIME DANOWSKY Advokatbyrå AB: Jonas Forzelius & Esa Kymäläinen
- 189** **Switzerland**  
Kellerhals Carrard: Dr. Oliver M. Brupbacher, Dr. Nicolas Mosimann & Marlen Schultze
- 199** **Taiwan**  
Lee and Li, Attorneys-at-Law: Ken-Ying Tseng
- 206** **Thailand**  
R&T Asia (Thailand) Limited: Supawat Srirungruang & Saroj Jongsaritwang
- 214** **United Arab Emirates**  
Hamdan AlShamsi Lawyers & Legal Consultants: Hamdan Al Shamsi & Helen Tung
- 220** **USA**  
Ropes & Gray LLP: Edward R. McNicholas & Kevin J. Angle

# Mexico

Creel, García-Cuellar, Aiza y Enríquez



Begoña Cancino

## 1 Cybercrime

**1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:**

### Hacking (i.e. unauthorised access)

The Federal Criminal Code provides for two different criminal types when it comes to unauthorised access: simple; and aggravated. The aggravation criteria depend on the purported intention to cause damages by obtaining a specific result with the unauthorised access, especially when it entails the violation of intellectual property rights. Unauthorised access is then a federal crime under articles 211 *bis* 1 to 211 *bis* 7 of the Federal Criminal Code, but also article 426, which is contained in a chapter devoted exclusively to copyrights and provides that performing any act with the purpose of breaking an encrypted satellite signal or carrying programs without the proper authorisation, would be penalised with imprisonment from six months to four years, as well as a fine. Development and distribution of equipment intended to receive an encrypted signal and services intended to receive or assisting others in receiving an encrypted signal, will be also penalised as described in this paragraph.

Also, the Federal Criminal Code provides that a person who, with or without authorisation, modifies, destroys or causes loss of information contained in credit institutions' systems or computer equipment protected by a security mechanism shall be penalised with imprisonment of up to six months to four years, as well as a fine. Moreover, an unauthorised person who knows or copies information from credit institutions' computer systems or equipment protected by a security mechanism shall be subject to imprisonment of three months to two years, as well as a fine.

### Denial-of-service attacks

The Federal Criminal Code does not provide any definition, or similar definition, for this criminal offence. However, article 427 *quater*, it includes penalties of imprisonment from six months to six years and a fine to those who provide services to the public aimed primarily at circumventing an effective technological protection measure of any work of authorship (including, of course, software).

### Phishing

The Federal Criminal Code does not provide any definition for phishing; however, such criminal offence could be considered fraud. According to article 386 of the Federal Criminal

Code, a person commits fraud when he/she handles information through deceit, takes advantage of errors or misleads a person with the intent of obtaining a financial gain. In such case, the responsible party shall be subject to imprisonment of three days to 12 years, as well as a fine.

### Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

The Federal Criminal Code does not provide any definition for this criminal offence; however, this type of behaviour may fall under the scope of hacking. The aforementioned penalties are applicable in this case. If the criminal offence is committed against the state, the relevant authority shall be subject to imprisonment of one year to four years, as well as a fine.

### Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

The Federal Criminal Code contains a specific criminal offence in this regard, providing that those who manufacture, import, distribute, rent or in any way market devices, products or components intended to circumvent an effective technological measure, would be subject to imprisonment from six months to six years and a fine.

### Possession or use of hardware, software or other tools used to commit cybercrime

The Federal Criminal Code provides that those who, knowingly, without authorisation and for profit, suppress or alter, by themselves or through another, any information on rights management, will be imposed with six months' to six years imprisonment and a fine. The same penalty will be imposed on any person who, for profit: distributes, or imports for distribution, information on rights management, knowing that it has been suppressed or altered without authorisation; or distributes, imports for distribution, transmits, communicates or makes available to the public, copies of works, performances, performances or phonograms, knowing that the information on rights management has been suppressed or altered without authorisation.

### Identity theft or identity fraud (e.g. in connection with access devices)

The Credit Institutions Law provides that a person who produces, manufactures, reproduces, copies, prints, sells, trades or alters any credit card, debit card or, in general, any other payment instrument, including electronic devices, issued by credit institutions, without authorisation of the holder, shall be given a prison sentence of three to nine years, by the relevant authority, as well as a fine.

**Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)**

As mentioned, identity theft or identity fraud are penalised under the Credit Institutions Law, if such activities are committed by any counsellor, official, employee or service provider of any credit institution there would be grounds for alleging breach of confidence and the penalties would increase.

In addition, under the Mexican Industrial Property Law, the theft of trade secrets – by electronic means or not – by current or former employees constitutes a crime and triggers imprisonment and fines to the responsible parties.

**Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)**

The Federal Criminal Code does not provide any definition for this criminal offence; however, this type of behaviour may fall under the scope of hacking. The aforementioned penalties are applicable in this case. If the criminal offence is committed against the state, the relevant authority shall impose a prison sentence of one year to four years, as well as a fine.

**Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data**

In addition, activities such as espionage, conspiracy, crimes against means of communication, tapping of communications, acts of corruption, extortion and money laundering could be considered threats to the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

The Federal Criminal Code includes a complete chapter devoted to crimes in connection with copyrights, where the unauthorised production, reproduction, introduction in the country, storage, transportation, distribution, commercialisation or other uses for commercial speculation purposes will be sanctioned with imprisonment and fines.

**1.2 Do any of the above-mentioned offences have extraterritorial application?**

In principle, all of the above-mentioned offences are applicable only within Mexican territory; however, there might be cases of serious criminal offences in which the Mexican authorities may collaborate with other authorities in other jurisdictions.

**1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves “ethical hacking”, with no intent to cause damage or make a financial gain)?**

The Federal Criminal Code does not provide for any exception such as “ethical hacking”; however, it should be noted that most of the crimes referred therein will be considered as such if the activity has been carried out for profit or with the aim to cause damage.

The Federal Law against Organized Crime provides that in the investigation of a crime which is assumed on good grounds that a member of organised crime is involved, it is possible to tap private communications by means of electronic systems and subject to a judicial order. The same occurs with the General Law to Prevent and Sanction Kidnapping Crimes, and when the Mexican government must request a judicial warrant to intercept

private communications for national security purposes and accordingly, the Federal Telecommunications and Broadcasting Law in its articles 189 and 190 allows competent authorities to control and tap private communications and provide support to those official requests.

**2 Cybersecurity Laws**

**2.1 Applicable Law:** Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Please see the following Applicable Laws:

- the Mexican Constitution;
- the Federal Telecommunications and Broadcasting Law (FTBL);
- the Federal Law on the Protection of Personal Data held by Private Parties (the Data Protection Law), its regulations, recommendations, guidelines and similar regulations on data protection;
- the Federal Law on Transparency and Access to Public Information;
- the General Law on Transparency and Access to Public Information;
- General Standards as specified under the Mexican Official Standard regarding the requirements that shall be observed when keeping data messages;
- the Law on Negotiable Instruments and Credit Operations;
- the Mexican Federal Tax Code;
- the Credit Institutions Law;
- the Sole Circular for Banks;
- the Industrial Property Law;
- the Mexican Copyright Law;
- the Federal Labour Law;
- the Federal Criminal Code;
- the Law of the National Security Guard;
- the National Strategy of Cybersecurity 2017; and
- the White Paper on National Defense of the Mexican State.

**2.2 Critical or essential infrastructure and services:** Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

There is an industry-specific risk in certain sectors: financial; telecommunications; and health, not only in the private sector, but also at the governmental level. The National Security Guard Act, in November 8, 2019, which allows Mexican authorities to rule judicial decisions to intervene private communications for National Security purposes, anticipated the replacement of the Center of Investigation and National Security by the newly created National Intelligence Center, a Mexican intelligence agency controlled by the Ministry of Security and Civilian Protection, the main purpose of which is to preserve the State's integrity, stability and endurance. This was a radical structural change in the Mexican government as the former intelligence agency used to be under the control of the Ministry of Interior, the purpose being the reinvention of the image of the agency as an authority focused on security instead of conducting



“authorised” espionage. During 2019, the National Intelligence Center hosted an official meeting where representatives of the National Bureau of Investigation and the Department of Justice agreed with the Mexican Government on a programme to coordinate efforts to reinforce the exchange of information concerning cybersecurity, including best practices to cope with activities that pose a risk for Mexico and the USA (i.e. financial, telecommunications and health, not only in the private sector, but also at the governmental level).

**2.3 Security measures: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.**

According to Mexican law (specifically, the Mexican Privacy Law), organisations are compelled to implement corrective, preventive and improvement measures to make security measures adequate to avoid a breach. Organisations should be able to differentiate between material and non-material harm under Mexican laws by conducting a risk analysis. Material harm should be prioritised over non-material harm and will always depend on the business, scope, context and processing of the data compromised in the incident. Industry-specific risk identification of material and non-material harm is thus crucial for all companies facing a cybersecurity incident. Certain sectors, such as healthcare and banking, should provide companies with the required latitude to adapt their own internal policies. Compromising the security of databases, sites, programs or equipment (and this may include failure to implement required security measures) constitutes an administrative infringement of the Mexican Privacy Law, which could be sanctioned with fines of up to Mex\$25.6 million, a fine that may be doubled if sensitive data is compromised.

**2.4 Reporting to authorities: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.**

From those incidents involving personal data, the Mexican Data Privacy Law does not contain any obligation to the National Institute of Transparency, Access to Information and Protection of Personal Data (“INAI”) about potential or actual incidents, including cyber threat or cyber-attacks. If the incident compromised personal data of identifiable individuals, then the business (understood as a data controller) must evaluate the breach through a risk assessment, implement the corrective, preventive and improvement actions to reinforce security measures, and determine if the event may result in prejudice to the property or non-pecuniary rights of the data subjects; if so, it should notify the affected parties. Under the Mexican Privacy Law (Federal Law on the Personal Data held by Private Parties), security breaches occurring at any stage of processing personal data

must be reported immediately by the data controller to the data owner, so that the latter can take appropriate action to defend its rights. There is no official format to notify breaches; however, the Mexican Privacy Law and its regulations provide that the notification must include, at least, the nature of the breach, the personal data compromised, corrective actions implemented immediately by the data controller, recommendations concerning measures for the data owner to protect its interests after the breach and the means available for the data owner to obtain more information on the breach.

On the other hand and pursuant to article 106 of the Securities Market Law and its general provisions, listed entities are compelled to report to the National Banking and Securities Commission (“CNBV”) all relevant events that may affect the value of its assets, including those involving incidents that impact a large amount of personal information, regardless of the cause of such events and including, of course, breaches of contracts, negligence or violation of other statutes such as the Mexican Privacy Law.

**2.5 Reporting to affected individuals or third parties: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.**

Rules for reporting threats of breaches that may involve the unauthorised use of personal data are contained in the Mexican Data Privacy Law and Regulations. These Regulations provide that the data controller must inform only the data subject, not the federal regulator or other authority. As per the timeline, the regulations only provide that this notification should be conducted immediately, and after assessing whether the breach significantly affects the property or non-pecuniary rights of the data subjects upon having conducted an exhaustive review of the magnitude of the breach, so that the prejudiced data subjects may act appropriately.

There is no official format to notify breaches related to data privacy matters; however, the Mexican Privacy Law and its regulations provide that the notification must include, at least, the nature of the breach, the personal data compromised, corrective actions implemented immediately by the data controller, recommendations concerning measures for the data owner to protect its interests after the breach and the means available for the data owner to obtain more information on the breach. Failure to comply with reporting obligations constitutes an administrative infringement to the Mexican Data Privacy Law and may trigger fines that increase in cases of repeated infringements.

**2.6 Responsible authority(ies): Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.**

The Applicable Laws empower the following authorities to investigate an Incident: (i) the General Attorney Office; (ii) Public Prosecutors; (iii) the National Banking and Securities Commission (“CNBV”); (iv) the INAI; and (v) the Federal Telecommunications Institute (“IFT”). Public Prosecutors in Mexico are in charge of investigating cyber activities and to resolve them, a cyber police has been created to follow up on crimes or unlawful activities committed through the internet. Complaints directed to the cyber police can be submitted via its website, by phone or through a Twitter or email account; in

addition, the Federal Police has created a scientific division called the National Centre For Cyber-Incidents Response, specialising in providing assistance to the victims or claimants of cyber threats and cyber-attacks. In the case of data protection, the INAI may conduct investigations to follow up personal data matters. Regarding telecommunications, the IFT is in charge of this sector.

### 2.7 Penalties: What are the penalties for not complying with the above-mentioned requirements?

There is no single framework for non-compliance with notice requirements and penalties in Mexico; they will depend heavily on the relevant law and regulator, for example:

- Failure to comply with reporting obligations constitutes an administrative infringement of the Mexican Data Privacy Law and may trigger fines that increase in case of repeated infringements.
- Failure to comply with reporting obligations of relevant events under the Securities Market Law may trigger the imposition of injunctive measures or the temporary suspension of the registry of securities' issuer.

### 2.8 Enforcement: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

As of April 2020, the INAI has sanctioned many companies in cases involving violation of Data Privacy Law, most of them involving cybersecurity issues, to the extent that such authority has imposed fines for up to US\$21 million in the last nine years. Entities devoted to financial services have been fined with almost US\$12 million, followed by entities related to the communication industry, which fines amount US\$2.5 million.

According to INAI and figures obtained from the official source of the National Commission for the Protection and Defence of Users of Financial Services, Mexico takes the eight place in identity theft worldwide; 67% of those reported cases are due to the loss of documents, 63% for robbery, and 53% for information taken directly from credit accounts. During the third quarter of 2017, cyber fraud grew by 102% compared with the same period in 2016, representing a proportion from 13% to 51% per year. In 2018, 49,843 claims were filed upon identity theft and only 54% were decided in favour of the claimant. In addition, Mexico takes the second place in Latin America with the greatest number of cyber-attacks to mobile devices.

## 3 Preventing Attacks

### 3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

**Beacons** (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

Generally, yes.

**Honeypots** (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

Generally, yes.

**Sinkholes** (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

Generally, yes.

### 3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Generally, yes, if organisations inform in advance that they will take these measures and obtain the proper consent from employees.

### 3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Generally, no, other than the restrictions already provided in the Industrial Property Law and the Copyright Law.

## 4 Specific Sectors

### 4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, according to the Mexican Data Privacy Law, data controllers have to implement technical, physical and administrative measures in order to protect personal data from damage, loss, alteration, destruction, unauthorised use, access or processing.

The Federal Criminal Code and the Law on Negotiable Instruments and Credit Operations also include penalties to prevent criminal offences or violation of cybersecurity measures.

### 4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Yes. Such requirements are found under the Law on Negotiable Instruments and Credit Operations, the Credit Institutions Law, the Securities Market Act and the Federal Criminal Code, among other official regulations and guidelines.

## 5 Corporate Governance

### 5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

There is not a single framework, nor penalties for non-compliance with: prevention; mitigation; response to incidents amounting to a breach of directors' or officers' duties in Mexico. This will depend heavily on the relevant law.

**5.2** Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There is no single framework providing for requirements to designate a CISO or equivalent; establishing incident response plans, conducting risk assessments and performing vulnerability tests will depend heavily on the Applicable Law and industry. When personal data is involved, the appointment of a data privacy officer would then be required, as well as the implementation of other measures to avoid risks (including cyber risks).

**5.3** Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Requirements will depend heavily on the relevant law and especially whether the risk constitutes a relevant incident. Please refer to questions 2.4 and 2.6 above.

## 6 Litigation

**6.1** Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

According to Article 32 of the Federal Criminal Code, organisations and companies are civilly liable for the damages caused to third parties by crimes committed by their partners, managers and directors. The state is similarly liable for the crimes committed by its public officials.

The Federal Civil Code provides a standard of civil liability established in Article 1910, which provides that a party that illegally causes harm to another person shall be obliged to repair the damage, unless he/she proves that the damage was produced as a consequence of the victim's guilt or negligence.

**6.2** Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

This is not applicable.

**6.3** Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

This is not applicable.

## 7 Insurance

**7.1** Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Generally, yes.

**7.2** Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Generally, no.

## 8 Investigatory and Police Powers

**8.1** Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Applicable Laws empower the following authorities to investigate an Incident: (i) the General Attorney Office; (ii) public Prosecutors; (iii) the INAI; and (iv) the IFT.

Public Prosecutors in Mexico are in charge of investigating and resolving cyber activities; a cyber police service has been created to follow up on crimes or unlawful activities committed through the Internet. Complaints directed to the cyber police can be submitted via its website, by phone, or through a Twitter or email account; in addition, the Federal Police have created a scientific division called the National Centre For Cyber-Incidents Response, specialised in providing assistance to the victims or claimants of cyber threats and cyber-attacks.

In the case of data protection, the INAI may conduct investigations to follow up personal data matters. The IFT is in charge of the telecommunications sector.

**8.2** Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

This is not applicable in Mexican law.



**Begoña Cancino** is a partner in the Mexico City office. Her practice focuses on Intellectual Property, Data Privacy, Regulatory and Administrative Litigation. From the standard IP front, Ms. Cancino counsels clients from all kinds of industries with the protection and enforcement of their IP rights in Mexico, also assisting with the transfer of IP portfolios within the context of complex corporate transactions involving all sorts of IP rights (such as trademarks, copyrights and appellations of origin). Ms. Cancino also provides assistance with her legal advice on regulatory and advertising, assessing our clients to comply with all applicable provisions with COFEPRIS and PROFECO. She has represented clients in all sort of administrative litigation proceedings, in general, concerning advertising, health, environmental and, of course, IP matters, before administrative authorities and federal judicial courts. Pursuant to the data privacy aspects of her practice, Ms. Cancino has counselled clients from multiple industries in the drafting and implementation of internal policies, privacy notices and specific legal concerns, not only regarding client daily operations, but also within the context of cross-border transactions and internal investigations for compliance.

**Creel, García-Cuellar, Aiza y Enríquez**  
Torre Virreyes Pedregal no. 24, piso 24 col.  
Molino del Rey, Ciudad de México 11040  
Mexico

Tel: +52 55 4748 0600  
Email: [begona.cancino@creel.mx](mailto:begona.cancino@creel.mx)  
URL: [www.creel.mx](http://www.creel.mx)

With over 80 years of history, Creel, García-Cuellar, Aiza y Enríquez is a leading full-service corporate law firm with an unwavering commitment to excellence. We have an established reputation for delivering creative, specialised and responsive legal advice on the most complex and innovative matters in Mexico for the most sophisticated and demanding clients. Our practice is based on the philosophy that a client is best served by legal advice designed to anticipate and avoid problems, rather than respond to them. Our goal is to be the law firm of choice for clients with the most demanding transactions and projects, and, in such endeavour, become a strategic service provider to them, by offering the type of legal advice that gives clients certainty and peace of mind. We view our role as one of adding value to our clients and providing them with certainty and peace of mind. As such we strive to become their strategic service provider.

[www.creel.mx](http://www.creel.mx)

**C R E E L** GARCÍA-CUÉLLAR  
AIZA Y ENRÍQUEZ



# ICLG.com

## Other titles in the ICLG series

Alternative Investment Funds  
Anti-Money Laundering  
Aviation Finance & Leasing  
Aviation Law  
Business Crime  
Cartels & Leniency  
Class & Group Actions  
Competition Litigation  
Construction & Engineering Law  
Consumer Protection  
Copyright  
Corporate Governance  
Corporate Immigration  
Corporate Investigations  
Corporate Tax  
Data Protection  
Derivatives  
Designs  
Digital Business

Digital Health  
Drug & Medical Device Litigation  
Employment & Labour Law  
Enforcement of Foreign Judgments  
Environment & Climate Change Law  
Environmental, Social & Governance Law  
Family Law  
Fintech  
Foreign Direct Investment Regimes  
Franchise  
Gambling  
Insurance & Reinsurance  
International Arbitration  
Investor-State Arbitration  
Lending & Secured Finance  
Litigation & Dispute Resolution  
Merger Control  
Mergers & Acquisitions  
Mining Law

Oil & Gas Regulation  
Outsourcing  
Patents  
Pharmaceutical Advertising  
Private Client  
Private Equity  
Product Liability  
Project Finance  
Public Investment Funds  
Public Procurement  
Real Estate  
Renewable Energy  
Restructuring & Insolvency  
Sanctions  
Securitisation  
Shipping Law  
Telecoms, Media & Internet  
Trade Marks  
Vertical Agreements and Dominant Firms