La ciberseguridad y el rol del Directorio en Latinoamérica y el Caribe

Comtelca, Septiembre 11, 2020

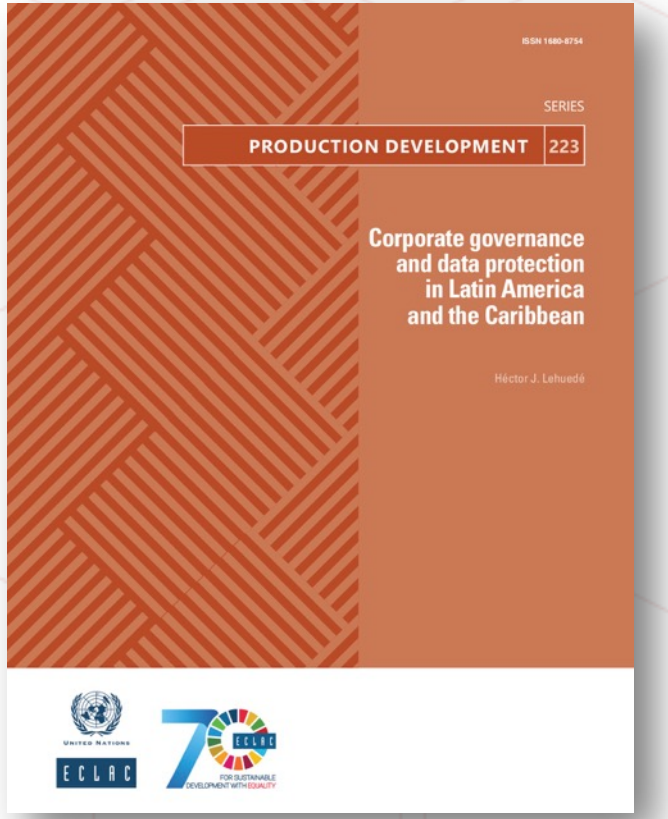
Héctor J. Lehuedé
hlehuede@razorconsulting.cl

La ciberseguridad y el rol del Directorio

- Mejorar la ciberseguridad es un desafío que involucra a todos los actores relevantes en un esfuerzo colectivo e idealmente bien coordinado para mantenernos a salvo de las amenazas.
- El aumento de los flujos digitales provocados por la pandemia y las nuevas formas en que trabajamos y aprendemos han hecho que este desafío sea aún más crucial.
- Las empresas juegan un papel importante en él y es vital que las consideraciones de ciberseguridad estén integradas en su estrategia y sean abordadas adecuadamente por sus directorios (juntas directivas).
- Dos de las tres áreas / comunidades principales dentro de lo que tendemos a entender como parte de la ciberseguridad tienen expectativas concretas para las empresas y sus directorios:
  - Ciberseguridad
  - Cibercrimen
  - Ciberdefensa

La ciberseguridad y el rol del Directorio

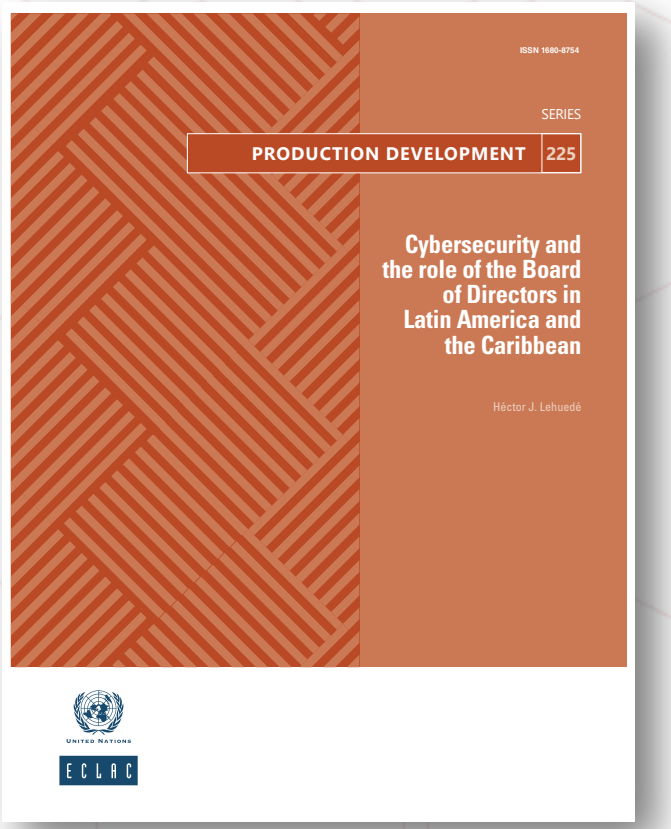
- Ciberseguridad, entendida como la prevención de ciberataques y la construcción de seguridad en la forma en que se protegen los sistemas TIC y datos.
- Aquí se espera que las empresas y sus directorios protejan los datos y los activos digitales del robo y el fraude, si no por su propio interés, para proteger los datos personales de sus clientes, consumidores y otras partes interesadas.
- La atención se centra principalmente en posibles daños, multas, responsabilidad corporativa y daño reputacional.
- El enfoque es más legal, sancionatorio.
- Materia fue cubierta en paper de CEPAL 2019



Corporate Governance and Data Protection
in Latin America and the Caribbean
June 2019 - ECLAC Production Development

La ciberseguridad y el rol del Directorio

- La ciberseguridad como ciberdefensa, que se ocupa de la preparación para defender los intereses nacionales o atacar a los enemigos en el ciberespacio, involucrando tanto iniciativas militares como civiles.
- Aquí, entre las últimas, este grupo está particularmente interesado en proteger la continuidad de la infraestructura y los servicios críticos, donde los ciberataques podrían causar daños considerables.
- El enfoque no está tanto en la responsabilidad o las multas, como en que las organizaciones velen por la continuidad de los servicios que prestan.
- El enfoque es técnico, operacional.
- Materia se trata en este nuevo paper de CEPAL



Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean
September 2020 - ECLAC Production Development

La ciberseguridad y el rol del Directorio

- Estas expectativas sobre el papel de los directorios y el gobierno corporativo en la lucha contra los riesgos cibernéticos se están traduciendo en leyes, regulaciones y políticas.
- Dentro de la región, pudimos encontrar mucha regulación y orientación para el primer grupo, principalmente sobre protección de datos.
- No tanto para el segundo grupo sobre infraestructura crítica y servicios esenciales.
- Aunque es la mejor práctica de aquellas jurisdicciones que son reconocidas como líderes en ciberseguridad y una recomendación incluida en casi cualquier informe sobre el tema, tanto de expertos técnicos como organizaciones internacionales.

La ciberseguridad y el rol del Directorio

Key cybersecurity rules related to data protection (selected jurisdictions)	Argentina	Bolivia	Brazil	Chile*	Colombia	Costa Rica	Dominican Republic	Guatemala *	Mexico	Panama	Paraguay	Peru	Uruguay	Venezuela
Data protection authority														
Restriction on international transfers to other jurisdictions														
Restrictions on transfers to data processors														
Sanctions														
Mandatory notification of breaches to authority and/or data subjects					A									U
Mandatory DPOs	E											E		
Mandatory DPIAs					R									
Accountability														

Notes: (*): These jurisdictions have bills of law currently in Congress that include some of these measures; E: exceptionally; R: recommended; A: notification to the authority only; U: it is unclear who should be notified. Source: Author's elaboration.

La ciberseguridad y el rol del Directorio

Rank	Country	Protection of personal data	Personal data protection legislation	Personal data protection authority
		Protection of personal data		
1.	Greece	4	1	3
3.	Estonia	4	1	3
5.	Spain	4	1	3
8.	France	4	1	3
15.	United States	4	1	3
39.	Chile	1	1	0
41.	Canada	4	1	3
38.	Paraguay	1	1	0
48.	Costa Rica	4	1	3
57.	Argentina	4	1	3
55.	Panama	4	1	3
58.	Uruguay	4	1	3
61.	Brazil	1	1	0
60.	Colombia	4	1	3
67.	Dominican Republic	1	1	0
70.	Peru	4	1	3
75.	Mexico	4	1	3
78.	Ecuador	0	0	0
85.	Venezuela	0	0	0
94.	Guatemala	0	0	0
95.	Bolivia	0	0	0
96.	Jamaica	0	0	0
103.	Bahamas	4	1	3
105.	Nicaragua	4	1	3
108.	Trinidad and Tobago	1	1	0
113.	Suriname	0	0	0
111.	El Salvador	0	0	0
121.	Barbados	1	1	0
125.	Grenada	0	0	0
128.	Cuba	0	0	0
136.	Antigua and Barbuda	4	1	3
137.	Haiti	0	0	0
143.	Saint Kitts and Nevis	1	1	0
141.	Honduras	0	0	0
147.	Saint Vincent and the Grenadines	0	0	0
146.	Saint Lucia	4	1	3
149.	Guyana	0	0	0
152.	Belize	0	0	0
153.	Dominica	0	0	0

NCSI Data Protection

Rank	Country	Protection of personal data	Personal data protection legislation	Personal data protection authority
		Protection of personal data		
1.	Greece	4	1	3
3.	Estonia	4	1	3
5.	Spain	4	1	3
8.	France	4	1	3
15.	United States	4	1	3
41.	Canada	4	1	3
48.	Costa Rica	4	1	3
55.	Panama	4	1	3
60.	Colombia	4	1	3
67.	Dominican Republic	1	1	0
75.	Mexico	4	1	3
94.	Guatemala	0	0	0
105.	Nicaragua	4	1	3
111.	El Salvador	0	0	0
141.	Honduras	0	0	0

La ciberseguridad y el rol del Directorio

Rank	Country	Cyber security policy development		Cyber threat analysis and information	Cyber incidents response		Cyber crisis management
		Cyber security policy development	Cyber security strategy	Cyber threat analysis and information	Cyber incidents response	Cyber incidents response unit	Cyber crisis management
1.	Greece	7	1	4	6	3	4
3.	Estonia	6	1	5	6	3	5
5.	Spain	6	1	5	4	3	3
8.	France	6	1	4	4	3	3
15.	United States	7	1	5	3	3	4
39.	Chile	7	1	2	3	3	1
41.	Canada	1	1	4	5	3	2
38.	Paraguay	7	1	2	5	3	1
48.	Costa Rica	6	1	0	5	3	1
57.	Argentina	6	1	1	3	3	1
55.	Panama	1	1	0	3	3	1
58.	Uruguay	0	0	1	5	3	1
61.	Brazil	4	1	4	3	3	1
60.	Colombia	2	1	2	3	3	1
67.	Dominican Republic	7	1	0	5	3	1
70.	Peru	0	0	0	3	3	1
75.	Mexico	3	1	0	3	3	1
78.	Ecuador	0	0	0	5	3	1
85.	Venezuela	3	0	1	3	3	1
94.	Guatemala	1	1	0	0	0	1
95.	Bolivia	0	0	1	3	3	0
96.	Jamaica	2	0	0	3	3	0
103.	Bahamas	0	1	0	0	0	0
105.	Nicaragua	0	0	0	0	0	1
108.	Trinidad and Tobago	1	1	0	3	3	1
113.	Suriname	0	0	0	3	3	0
111.	El Salvador	0	0	0	0	0	1
121.	Barbados	0	1	1	0	0	0
125.	Grenada	0	0	0	0	0	0
128.	Cuba	0	0	0	3	3	0
136.	Antigua and Barbuda	0	0	0	0	0	0
137.	Haiti	0	0	0	0	0	0
143.	Saint Kitts and Nevis	0	0	0	0	0	0
141.	Honduras	0	0	0	0	0	1
147.	Saint Vincent and the Grenadines	0	0	1	0	0	0
146.	Saint Lucia	0	0	0	0	0	0
149.	Guyana	0	0	0	3	3	0
152.	Belize	0	0	0	0	0	0
153.	Dominica	0	0	0	0	0	0

NCSI General Cybersecurity

Rank	Country	Cyber security policy development		Cyber threat analysis and information	Cyber incidents response		Cyber crisis management
		Cyber security policy development	Cyber security strategy	Cyber threat analysis and information	Cyber incidents response	Cyber incidents response unit	Cyber crisis management
1.	Greece	7	1	4	6	3	4
3.	Estonia	6	1	5	6	3	5
5.	Spain	6	1	5	4	3	3
8.	France	6	1	4	4	3	3
15.	United States	7	1	5	3	3	4
41.	Canada	1	1	4	5	3	2
48.	Costa Rica	6	1	0	5	3	1
55.	Panama	1	1	0	3	3	1
60.	Colombia	2	1	2	3	3	1
67.	Dominican Republic	7	1	0	5	3	1
75.	Mexico	3	1	0	3	3	1
94.	Guatemala	1	1	0	0	0	1
105.	Nicaragua	0	0	0	0	0	1
111.	El Salvador	0	0	0	0	0	1
141.	Honduras	0	0	0	0	0	1

La ciberseguridad y el rol del Directorio

Rank	Country	Protection of digital services		Protection of essential services			
		Protection of digital services	Cyber security responsibility for digital service providers	Protection of essential services	Operators of essential services are identified	Cyber security requirements for operators of essential services	Regular monitoring of security measures
1.	Greece	5	1	6	1	1	1
3.	Estonia	5	1	6	1	1	1
5.	Spain	4	1	5	1	1	0
8.	France	4	1	5	1	1	0
15.	United States	1	0	6	1	1	1
39.	Chile	1	0	1	1	0	0
41.	Canada	1	0	2	1	1	1
38.	Paraguay	1	0	3	0	0	0
48.	Costa Rica	0	0	0	0	0	0
57.	Argentina	1	0	0	0	0	0
55.	Panama	3	0	0	0	0	0
58.	Uruguay	1	0	3	0	0	0
61.	Brazil	0	0	1	1	0	0
60.	Colombia	0	0	1	1	0	0
67.	Dominican Republic	0	0	0	0	0	0
70.	Peru	0	0	0	0	0	0
75.	Mexico	0	0	0	0	0	0
78.	Ecuador	1	0	0	0	0	0
85.	Venezuela	0	0	0	0	0	0
94.	Guatemala	0	0	0	0	0	0
95.	Bolivia	0	0	0	0	0	0
96.	Jamaica	0	0	0	0	0	0
103.	Bahamas	0	0	1	1	0	0
105.	Nicaragua	0	0	0	0	0	0
108.	Trinidad and Tobago	0	0	1	1	0	0
113.	Suriname	0	0	0	0	0	0
111.	El Salvador	0	0	0	0	0	0
121.	Barbados	0	0	1	1	0	0
125.	Grenada	0	0	1	1	0	0
128.	Cuba	5	1	0	0	0	0
136.	Antigua and Barbuda	0	0	1	1	0	0
137.	Haiti	0	0	0	0	0	0
143.	Saint Kitts and Nevis	0	0	0	0	0	0
141.	Honduras	0	0	0	0	0	0
147.	Saint Vincent and the Grenadines	0	0	0	0	0	0
146.	Saint Lucia	0	0	0	0	0	0
149.	Guyana	0	0	0	0	0	0
152.	Belize	0	0	0	0	0	0
153.	Dominica	0	0	1	1	0	0

NCSI Protection of Critical Services

Rank	Country	Protection of digital services		Protection of essential services			
		Protection of digital services	Cyber security responsibility for digital service providers	Protection of essential services	Operators of essential services are identified	Cyber security requirements for operators of essential services	Regular monitoring of security measures
1.	Greece	5	1	6	1	1	1
3.	Estonia	5	1	6	1	1	1
5.	Spain	4	1	5	1	1	0
8.	France	4	1	5	1	1	0
15.	United States	1	0	6	1	1	1
41.	Canada	1	0	2	1	1	1
48.	Costa Rica	0	0	0	0	0	0
55.	Panama	3	0	0	0	0	0
60.	Colombia	0	0	1	1	0	0
67.	Dominican Republic	0	0	0	0	0	0
75.	Mexico	0	0	0	0	0	0
94.	Guatemala	0	0	0	0	0	0
105.	Nicaragua	0	0	0	0	0	0
111.	El Salvador	0	0	0	0	0	0
141.	Honduras	0	0	0	0	0	0

La ciberseguridad y el rol del Directorio

- Ya en 2004, la Asamblea General de la OEA aprobó una Estrategia Interamericana Integral para Combatir Amenazas a la Seguridad Cibernética, impulsando la adopción de Estrategias Nacionales de Seguridad Cibernética que pudieran gestionar riesgos sobre infraestructura crítica.
- Los ciberataques a la infraestructura crítica fueron calificados como el quinto mayor riesgo a nivel mundial en 2020 por el WEF.
- Sin embargo, las pocas regulaciones que pudimos encontrar en la región, muchas de ellas actualmente en proceso, están presentes solo para una fracción de las empresas que manejan infraestructura crítica, poseen activos o prestan servicios que deben ser resguardados como parte de una estrategia nacional de ciberseguridad.

La ciberseguridad y el rol del Directorio

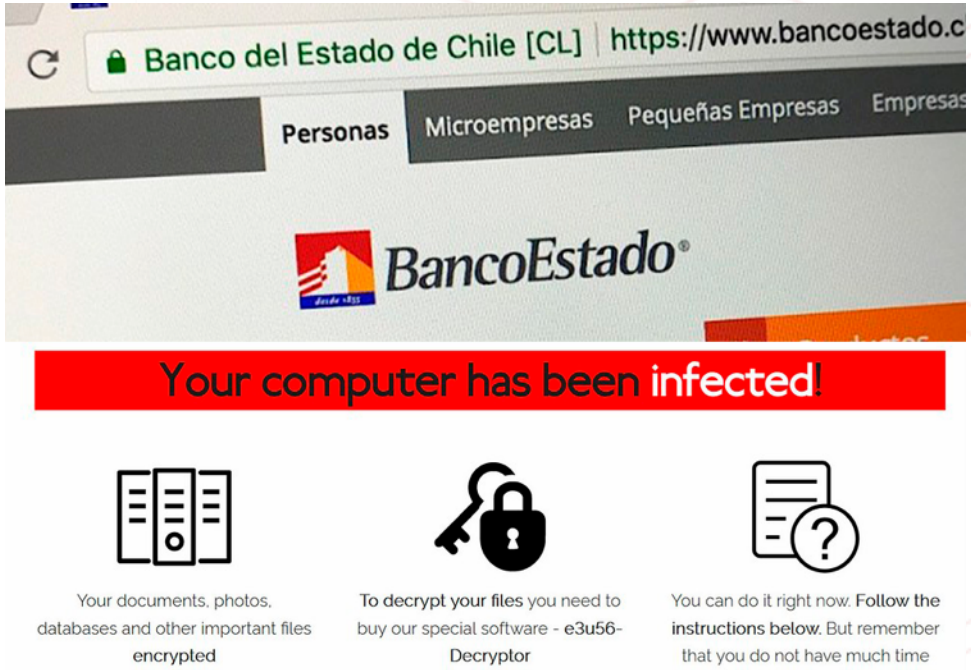
- La mayoría de los países no han identificado con precisión las infraestructuras que deben considerarse críticas, las entidades que las controlan, los estándares de ciberseguridad que necesitan implementar para protegerlos y las reglas de monitoreo y responsabilidad que asegurarán que esos estándares se implementen.
- Existen buenos ejemplos a seguir (se incluyen en el reporte algunos casos de estudio) y hay buenas prácticas y estándares de ciberseguridad (en el reporte se describen) que pueden exigirse a las empresas y sus directorios, para asegurarse que contribuyan a reducir estos riesgos.
- Cuando ellas administran activos críticos y servicios esenciales, que en el pasado hubiese manejado el Estado directamente, es importante asegurarse que existan los incentivos para que hagan las inversiones en seguridad y continuidad que garanticen una adecuada provisión de los bienes públicos de que la ciudadanía depende, y que la ciberseguridad pase a formar parte de su estrategia de negocio. Buen gobierno corporativo y ciberseguridad van de la mano.

La ciberseguridad y el rol del Directorio

El viernes **4 de septiembre de 2020**, a través de un documento de Office que fue abierto por un empleado del banco, hackers instalaron el *ransomware* Sodinokibi en 13 mil computadores y robaron información del banco.

Los empleados que llegaron el sábado en la manana a trabajabar en el turno del fin de semana descubrieron que no tenían acceso a sus archivos.

El **jueves 10** el banco había logrado abrir solo 80% sus sucursales, que habían permanecido cerradas desde el sábado.



BancoEstado es una empresa **100% estatal**, no sometida a las normas de buen gobierno ni supervisión del Sistema de Empresas Públicas de Chile y que tiene un directorio de 7 miembros en que 6 son nombrados directamente por el Presidente de la República, de acuerdo a sus estatutos de 1977 (reformados la última vez en 1989):

https://www.corporativo.bancoestado.cl/sites/default/files/default-source/ley-orgánica-del-banco-del-estado-de-chile-(d-l-2-079-de-1977).pdf#page=2

La ciberseguridad y el rol del Directorio en Latinoamérica y el Caribe

Comtelca, Septiembre 11, 2020

Héctor J. Lehuedé
hlehuede@razorconsulting.cl