



BANCO CENTRAL
REPÚBLICA DOMINICANA

Management of a cyber resilience and wholesale payment security agenda

Ángel González Tejada

Director of Payment Systems Department

Regional Payments Week 2019

Willemstad, Curacao, 20 November 2019

Why cybersecurity?

CYBERCRIME WILL BE MORE PROFITABLE THAN ILLEGAL DRUGS

By 2021, it is estimated that cybercrime will take \$6 quintillion from the global pocket. It is currently costing almost \$4 trillion in damages, however, the number is steadily increasing as criminals become more wiser.

54% OF COMPANY VIOLATIONS ARE DUE TO EMPLOYEES

Employees without knowing it, allow hacking to occur by opening an phishing email or following an insecure link. The second aspect is when the employee performs the attack by himself.

THE ORGANIZATION NEEDS AN AVERAGE OF 191 DAYS TO DETECT AN ATTACK
AN ATTACK OCCURS EVERY 39 SECONDS IN THE USA

Dominican Republic in an International Context

National Cybersecurity Strategy in Latin America

Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE) of the OAS

Panama



Chile



Guatemala



Mexico



Colombia



Costa Rica



Jamaica

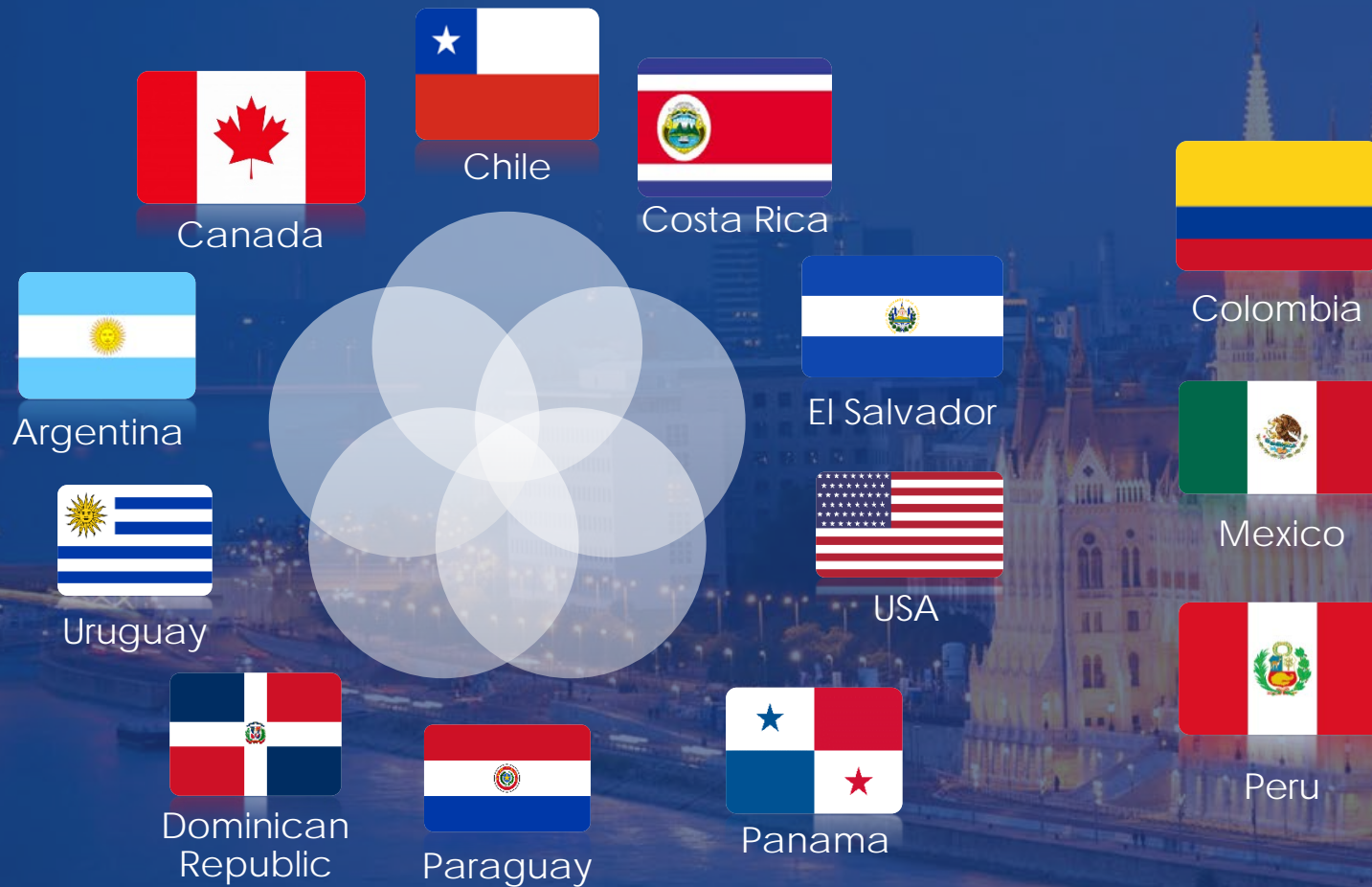


Dominican Republic



<http://www.oas.org/juridico/spanish/cybersp.htm>

Convention on Cybercrime (Budapest Convention)



- Standardization of criminal regulations for cybercrime;
- Strengthening procedural powers in the prerogatives of persecution;
- Establishment an international cooperation regime.

National context

MONETARY AND FINANCIAL LAW (2002)



It focuses on cybersecurity as part of operational risk.

PERSONAL DATA PROTECTION LAW (2013)



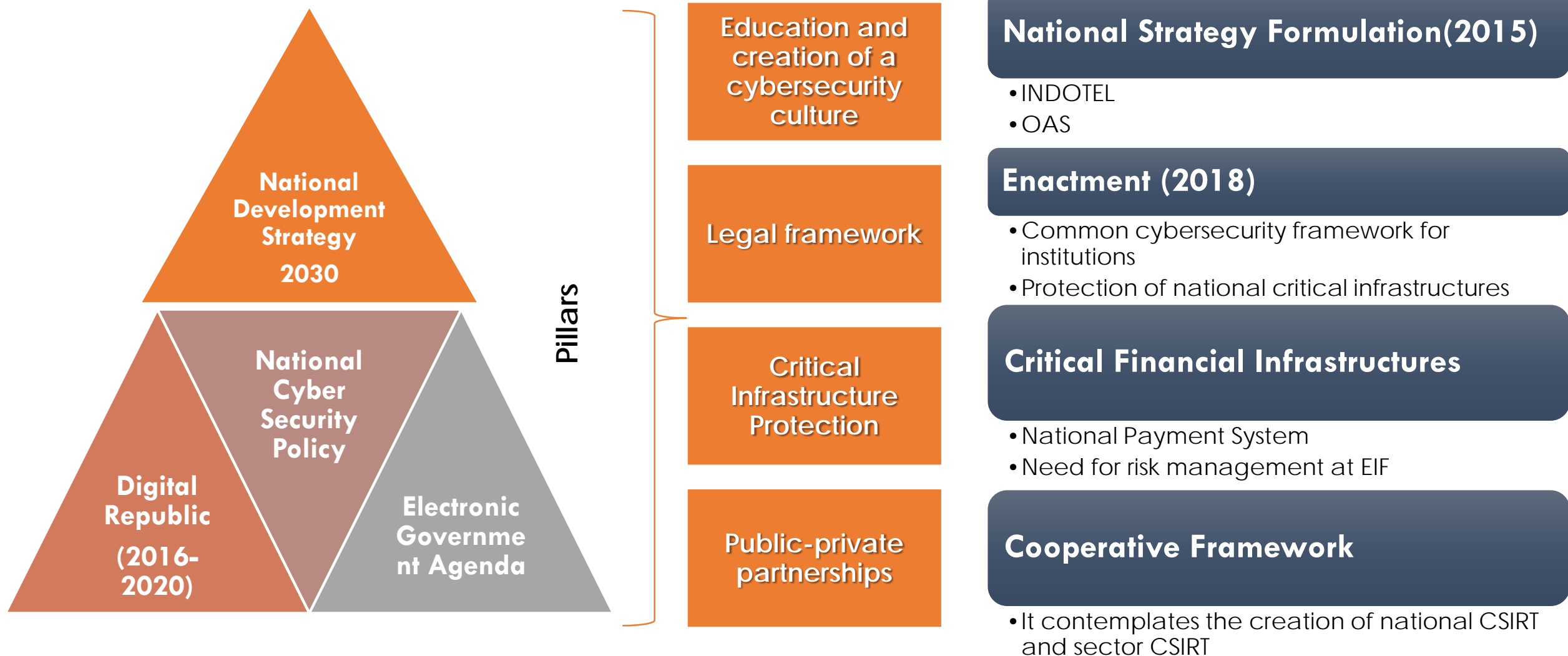
Vision focused on users and the protection of their information.

HIGH TECHNOLOGY CRIMES AND CRIMES LAW (2007)



It focuses on the criminal prosecution of cybercrime.

National Policy Development



Regulation of Cyber Security and Information for the Financial System

BANCO CENTRAL
REPÚBLICA DOMINICANA



- Prepared by the Central Bank.
- Approved by the Monetary Board in November 2018.
- Main mechanism to promote capacity development in the financial system of cyber risk mitigation and its impact on the technological infrastructures of its entities.
- Entry into force in November 2019.



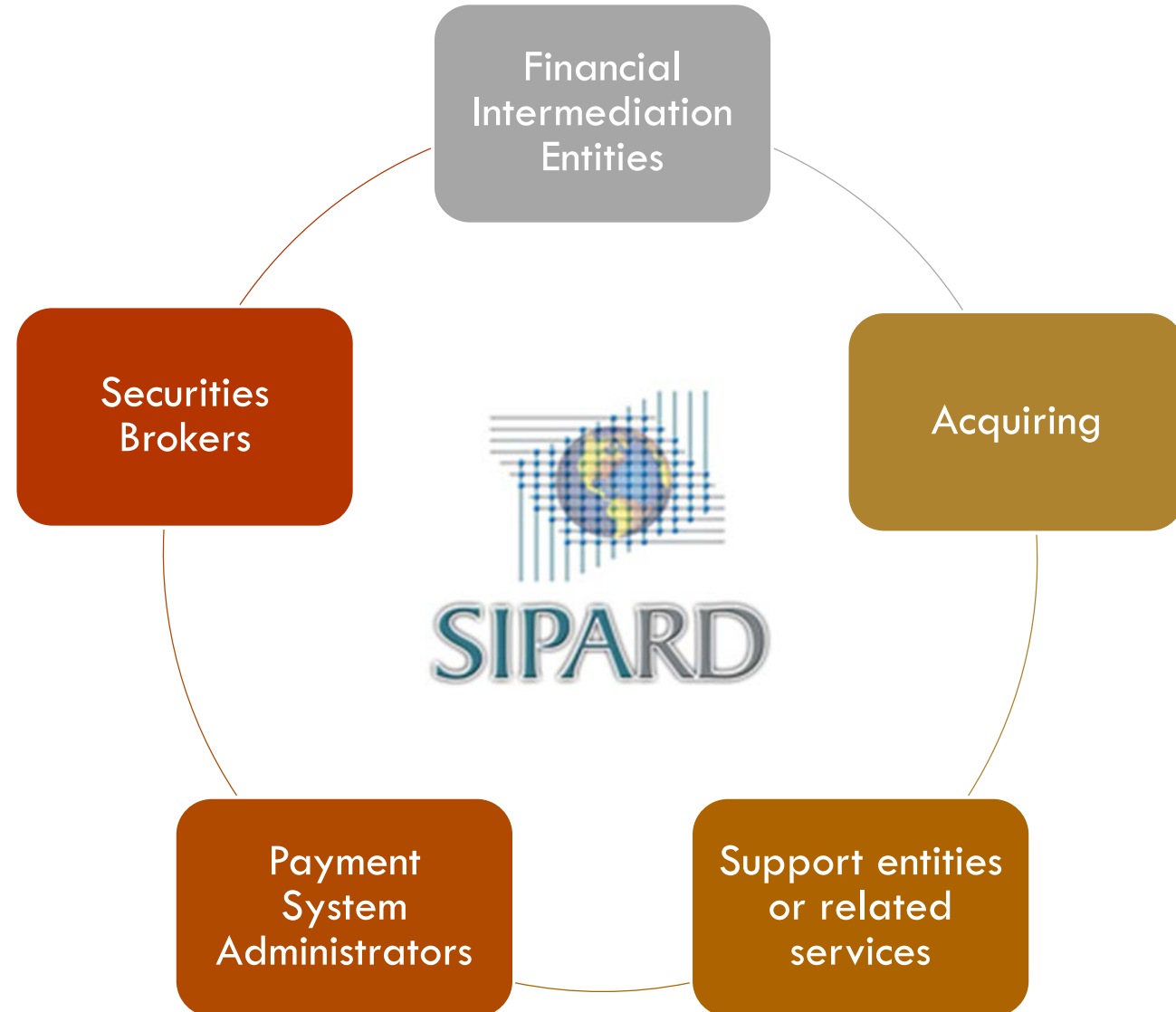
Purpose and scope of the Regulation

BANCO CENTRAL
REPÚBLICA DOMINICANA



Purpose

- Establish the general principles and guidelines for regulators to ensure integrity, availability and confidentiality of the information and the optimal functioning of their Information Systems and the Technological Infrastructure.



Highlights

BANCO CENTRAL
REPÚBLICA DOMINICANA



CYBER SECURITY PROGRAM



- Information security governance
- Risk assessment to internal suppliers

SECTORAL COORDINATION



- Creation of the Cyber Security Sector Council
- Creation of the Cyber Security Incident Response Team for the Financial Sector

CONSEQUENCES REGIME



- Penalty regime for EIFs
- Precautionary measures based on the interconnection with SIPARD



BANCO CENTRAL
REPÚBLICA DOMINICANA

Cyber Security and Information Program

BANCO CENTRAL
REPÚBLICA DOMINICANA



Technology Risk Management

- Self-assessment of technological risks taking into account risk appetite
- Evaluation of technological risks of interconnected entities



Development of a control framework

- Elaboration an internal cyber security and information policy
- Controls for the active management of information, networks, information systems and technological infrastructures



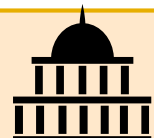
Program monitoring and evaluation

- Internal audits process
- Cyber security and information monitoring



International standards

- Applicable to the regulated that access products and services of international suppliers
- Applicable to outsourced providers of bank card production and identification token services



Compliance reports

- Financial Intermediation Entities (Superintendency of Banks)
- Administrators and Participants SIPARD, Support Entities and Related Services (Central Bank)

Sectoral Coordination

BANCO CENTRAL
REPÚBLICA DOMINICANA



Sector Council for the Response to Cyber Security Incidents of the Financial Sector

From the Monetary and Financial Administration

- Governor of the Central Bank, who chairs the Council
- Superintendent of Banks
- Comptroller of the Central Bank
- Assistant Manager of Systems and Technological Innovation of the Central Bank

Private Financial Sector Guilds

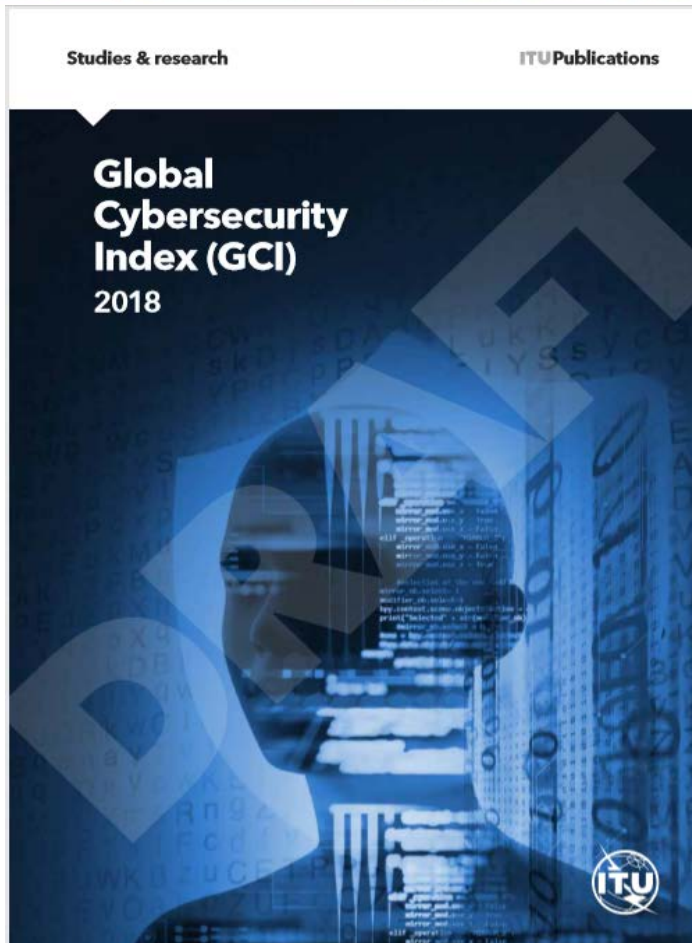
- President of the Association of Commercial Banks of the Dominican Republic (ABA)
- President of the Security Committee of the League of Savings and Loans Associations Dominican (LIDAAPI)
- President of the Technology Committee of the Association of Savings and Credit Banks and Credit Corporations

Cyber Security Incident Response Team (CSIRT)

- Under the administrative dependency of the BCRD and functional of the Sectorial Council
- Defines immediate actions for prevention, detection, containment, eradication and recovery against Cyber Security Incidents that affect the regulated



Global Cybersecurity Index 2018



https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

Indicators by pillars

Legal

- Cybercrime legislation
- Cybersecurity regulation
- Containment/curbing of spam legislation



Technical Measures

- CERT/CIRT/CSIRT
- Standards Implementation Framework
- Standardization Body
- Technical mechanisms and capabilities deployed to address Spam
- Use of cloud for cybersecurity purpose
- Child Online Protection mechanisms



Organizational Measures

- National Cybersecurity Strategy
- Responsible Agency
- Cybersecurity Metrics



Capacity Building Measures

- Public awareness campaigns
- Framework for the certification and accreditation of cybersecurity professionals
- Professional training courses in cybersecurity
- Educational programs or academic curricular in cybersecurity
- Cybersecurity R&D programs
- Incentive mechanisms



Cooperation Measures




- Bilateral agreements
- Multilateral agreements
- Participation in international fora/associations
- Public-Private Partnerships
- Inter-agency/intra-agency partnerships
- Best Practices



Country engagement level

High			Medium			Low		
United Kingdom	Qatar	New Zealand	Uzbekistan	Kuwait	Cote d'Ivoire	Gabon	Afghanistan	Mali
United States Of America	Georgia	Switzerland	Moldova	Bahrain	Iceland	State of Palestine	Barbados	Timor-Leste
France	Finland	Ireland	Ukraine	Belarus	Botswana	Senegal	Myanmar	San Marino
Lithuania	Turkey	Israel	Azerbaijan	Brazil	Chile	Sudan	Saint Vincent and the Grenadines	Marshall Islands
Estonia	Denmark	Kazakhstan	Cyprus	Czech Republic	Ghana	Gambia	Congo	Somalia
Singapore	Germany	Indonesia	South Africa	Romania	Zambia	Ethiopia	Cambodia	South Sudan
Spain	Egypt	Portugal	Nigeria	Colombia	Cameroon	Malawi	Mozambique	Saint kitts and Nevis
Malaysia	Croatia	Monaco	Philippines	Jordan	<u>Dominican Republic</u>	Iraq	Bahamas	Sao Tome and principe
Norway	Italy	Kenya	Serbia	Liechtenstein	Morocco	Tajikistan	Grenada	Djibouti
Canada	Russian Federation	Latvia	Tanzania	Tunisia	Argentina	Algeria	Bolivia	Solomon Islands
Australia	China	Slovakia	United Arab Emirates	Greece	Pakistan	Nepal	Sierra Leone	Tuvalu
Luxembourg	Austria	Bulgaria	Iran	Bangladesh	Jamaica	Seychelles	Eswatini	Guinea-Bissau
Netherlands	Poland	India	Montenegro	Armenia	Peru	Kyrgyzstan	Guyana	Cabo Verde
Saudi Arabia	Belgium	Slovenia	Albania	Benin	Burkina Faso	Guatemala	Papua New Guinea	Lesotho
Japan	Hungary	Rwanda	Mexico	Cuba	Panama	Antigua and Barbuda	Nicaragua	Haiti
Mauritius	Sweden	Viet Nam	Brunei Darussalam	Malta	Samoa	Costa Rica	Belize	Honduras
Republic Of Korea	The former Yugoslav Republic of	Uruguay	Uganda	Sri Lanka	Ecuador	Tonga	Namibia	Micronesia
Oman	Macedonia		Paraguay	Mongolia	Venezuela	Liberia	El Salvador	Central African Republic
	Thailand					Libya	Andorra	Equatorial Guinea
						Bosnia and Herzegovina	Turkmenistan	Kiribati
						Madagascar	Suriname	Vatican
						Lao	Mauritania	Eritrea
						Fiji	Nauru	Democratic people's Republic of
						Guinea	Chad	Korea
						Trinidad and Tobago	Vanuatu	Dominica
						Lebanon	Angola	Yemen
						Zimbabwe	Saint lucia	Comoros
						Bhutan	Niger	Democratic Republic of the
							Burundi	Congo
							Togo	Maldives

Member States are classified according to their level of commitment: high, medium, and low.

1.  Countries that demonstrate high commitment in all five pillars of the index.
2.  Countries that have developed complex commitments and engage in cybersecurity programmes and initiatives.
3.  Countries that have started to initiate commitments in cybersecurity.

Year	Score	Regional Rank	Global Rank
2018	0.430	10	92
2017	0.162	22	121

Regional Ranking of the Global Cybersecurity Index 2018

Member State	Score	Regional Rank	Global Rank	Member State	Score	Regional Rank	Global Rank	Member State	Score	Regional Rank	Global Rank
United States of America*	0.926	1	2	Peru	0.401	12	95	Bolivia (Plurinational State of)	0.139	24	135
Canada*	0.892	2	9	Panama	0.369	13	97	Guyana	0.132	25	138
Uruguay	0.681	3	51	Ecuador	0.367	14	98	Nicaragua	0.129	26	140
Mexico	0.629	4	63	Venezuela	0.354	15	99	Belize	0.129	26	140
Paraguay	0.603	5	66	Guatemala	0.251	16	112	El Salvador*	0.124	27	142
Brazil	0.577	6	70	Antigua and Barbuda	0.247	17	113	Suriname	0.110	28	144
Colombia	0.565	7	73	Costa Rica*	0.221	18	115	Saint Lucia	0.096	29	149
Cuba	0.481	8	81	Trinidad and Tobago	0.188	19	123	Saint Kitts and Nevis	0.065	30	157
Chile	0.470	9	83	Barbados	0.173	20	127	Haiti	0.046	31	164
Dominican Republic	0.430	10	92	Saint Vincent and the Grenadines	0.169	21	129	Honduras	0.044	32	165
Jamaica	0.407	11	94	Bahamas	0.147	22	133	Dominica	0.019	33	172
Argentina	0.407	11	94	Grenada	0.143	23	134				

Year	Score	Regional Rank	Global Rank
2018	0.430	10	92
2017	0.162	22	121



Greater understanding of cyber risk

Regulated entities are expected to pay more attention to such threats.

Increasing efficiency in supervisory efforts

The regulation will allow greater monitoring and control of the regulated entities of the Financial System.

Commissioning of the CSIRT

It is planned that the Sector Information Security Incident Response Team operates with contributions from regulated financial intermediation entities.

Risk mitigation in regulated entities

This regulation will allow the establishment a framework for prevention and detection of threats of this nature.



BANCO CENTRAL
REPÚBLICA DOMINICANA

THANK YOU

     BancoCentralRD | bancentral.gov.do