| | |
|---|---|
| **Assignment 08** | |
| **Name** | **Juan Callejas** |
| **Career field** | **Economics** |
| **Country** | **Guatemala** |
| **ESG Topic** | **Data privacy and cybersecurity** |

Instructions:

1. Guatemala macro indicators[1]
    a. GDP: US$85.99 billion[2]
    b. GDP annual growth rate (2022): 3.5%
    c. GDP per Capita: US$4,388.44[3]
    d. Inflation: 8.32%
    e. Interest rate: 5%
    f. Corporate tax rate: 25%
    g. Personal income tax rate: 7%
    h. Internet access in Guatemala[4]
        i. 62% of the population has access to a cell phone.
        ii. 91% of all internet users in Guatemala access the web through a cell phone.
        iii. 92% of all cell phones in Guatemala are used through pre-paid plans.
        iv. As of 2018, 29% of Guatemala's total population has access to the internet.
            1. 21% of the population has a computer at home.
            2. 17% of the population has access to a home internet service.
2. Data privacy and cybersecurity
    a. ESG issue:
        i. According to the World Economic Forum[5], cybersecurity should be regarded an ESG issue for three main reasons:
            1. It presents a threat to value.
            2. It presents a threat to society.
            3. Insurance can't mitigate the risk indefinitely.
    b. Cybersecurity in Guatemala

---

[1] (n.d.). *Guatemala Indicators*. Trading Economics. Retrieved May 27, 2023, from https://tradingeconomics.com/guatemala/indicators

[2] (n.d.). *Guatemala Indicators*. Trading Economics. Retrieved May 27, 2023, from https://tradingeconomics.com/guatemala/gdp

[3] (n.d.). *Guatemala Indicators*. Trading Economics. Retrieved May 27, 2023, from https://tradingeconomics.com/guatemala/gdp

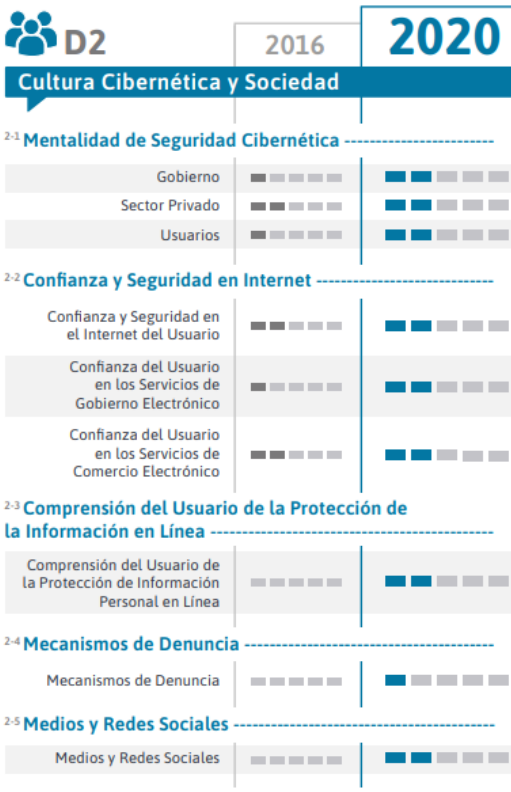
[4] Instituto para la Competitividad Económica (2022, June 6). *¿Cuál es la penetración de internet en Guatemala?* Retrieved May 27, 2023, from https://iceguate.org.gt/cual-es-la-penetracion-del-internet-en-guatemala/

[5] Instituto para la Competitividad Económica (2022, March 1). *Cybersecurity is an environmental, social and governance issue. Here's why*. World Economic Forum. Retrieved May 27, 2023, from https://www.weforum.org/agenda/2022/03/three-reasons-why-cybersecurity-is-a-critical-component-of-esg/?DAG=3&gclid=CjwKCAjw1MajBhAcEiwAagW9MUgEjYRtBTDKGqNsXC1HtMmllhJaiiI2hg-jLRpz-hM4jkwYJJVdJBoC0yIQAvD_BwE

i. Cybersecurity has been a growing concern in Guatemala over the past few years. Many private companies[6] are offering comprehensive cybersecurity solutions for companies, and colleges are offering cybersecurity graduate degrees[7].
ii. Since 2018, the National Cybersecurity Institute was created to raise awareness, train, and develop a stronger cybersecurity culture in the country, and partner with companies, universities, and the government in strengthening our national infrastructure for this. The institute partners with the government's National Science and Technology Secretary to further its efforts as a member of the Intersectoral IT Technical Commission.
iii. Awareness has grown in Guatemala as improvements across the board of key indexes proves over the past years:

[6] (n.d.). *MEJORES EMPRESAS DE CIBERSEGURIDAD EN GUATEMALA*. For Guatemala Lovers. Retrieved May 27, 2023, from https://www.forguatemalalovers.com/es/mejores/empresas-de-ciberseguridad-en-guatemala
[7] Universidad Internaciones and Universidad Galileo offer master's degrees in Cybersecurity


D1
2016
2020
Política y Estrategia de Seguridad Cibernética
1-1 Estrategia Nacional de Seguridad Cibernética
Desarrollo de la Estrategia
Organización
Contenido
1-2 Respuesta a Incidentes
Identificación de Incidentes
Organización
Coordinación
Modo de Operación
1-3 Protección de la Infraestructura Crítica (IC)
Identificación
Organización
Gestión de Riesgos y Respuesta
1-4 Manejo de Crisis
Manejo de Crisis
1-5 Defensa Cibernética
Estrategia
Organización
Coordinación
1-6 Redundancia de Comunicaciones
Redundancia de Comunicaciones


D2
2016
2020
Cultura Cibernética y Sociedad
2-1 Mentalidad de Seguridad Cibernética
Gobierno
Sector Privado
Usuarios
2-2 Confianza y Seguridad en Internet
Confianza y Seguridad en el Internet del Usuario
Confianza del Usuario en los Servicios de Gobierno Electrónico
Confianza del Usuario en los Servicios de Comercio Electrónico
2-3 Comprensión del Usuario de la Protección de la Información en Línea
Comprensión del Usuario de la Protección de Información Personal en Línea
2-4 Mecanismos de Denuncia
Mecanismos de Denuncia
2-5 Medios y Redes Sociales
Medios y Redes Sociales


This shows that a comprehensive approach involving academia, business, communication, culture, and government (legal, judicial, public policy, etc) has been fruitful and although the improvements are small, they continue to grow.

iv. Government response to the issue

1. In Guatemala, the government has been responding to the Cybersecurity issue by opening spaces for the discussion, sponsoring events and different institutions have been slowly adopting important

cybersecurity measures as more services are available online. One such example is RENAP, the National Person Registry[8] which offers its complete service for citizens online, including ID renewal, birth certificate purchasing, etc. An institution that has been highly questioned for the IT practices, however, is the Supreme Elections Tribunal (TSE[9]), which to this day, two weeks away from the national election, is without an IT director[10] and has been highly questioned in its acquisition of its digital platforms[11] for this year's event on June 25th.

2. An interesting effort on behalf of public institutions regarding cybersecurity has been to open training opportunities through:
    a. INTECAP (National Training Institute) course offerings which cost no more than US$25 for a full training program:
        i. CCNA V7: Business networks, security and automatization[12]
        ii. Cybersecurity essentials[13]
        iii. Endpoint security[14]
        iv. Fortinet NSE4 security[15]
        v. Introducción a la ciberseguridad[16]
    b. Also, Guatemala's public university (Universidad de San Carlos de Guatemala), through its School of Engineering, offers a master's program[17] specializing in telecommunication networks and cybersecurity at a very accessible price (US$2,500 for the entire program).
3. In 2021, Guatemala's Technical Secretary for the National Security Council created the National Cybersecurity Committee[18], which would be coordinated by the country's Strategic Intelligence Undersecretary.
    a. The committee would be in office for four years (until 2025) and will be a consulting group to the National Security Council by providing follow up the achievements of the country's National Cybersecurity Strategy.
    b. The committee is integrated by:

---

[8] https://www.renap.gob.gt/
[9] https://tse.org.gt/
[10] https://prensacomunitaria.org/2023/05/tse-sigue-sin-director-de-informatica-a-dos-meses-de-las-elecciones/
[11] https://www.prensalibre.com/guatemala/politica/elecciones-generales-2023-tse-busca-comprar-nuevo-sistema-informatico-para-acelerar-adjudicacion-de-cargos/
[12] https://www.intecap.edu.gt/centros/cti/cursosprogramados/
[13] https://www.intecap.edu.gt/centros/cti/cursosprogramados/
[14] https://www.intecap.edu.gt/centros/cti/cursosprogramados/
[15] https://www.intecap.edu.gt/centros/cti/cursosprogramados/

[16] https://www.intecap.edu.gt/centros/cti/cursosprogramados/

[17] https://postgrado.ingenieria.usac.edu.gt/proyecto-meaning/telecomunicaciones/
[18] Secretaría Técnica del Consejo Nacional de Seguridad (2021, October 29). *COMITÉ NACIONAL DE SEGURIDAD CIBERNÉTICA*. Retrieved June 7, 2023, from https://stcns.gob.gt/comite-nacional-de-seguridad-cibernetica/

i. Strategic Intelligence Undersecretary
ii. Sub-coordinator of the National Security Council's Technical Secretary
iii. Fourth Vice-minister of the interior
iv. IT Commander National Army
v. Vice-minister for the Ministry of Communications, Infrastructure and Housing
vi. Functional Responsible for the Consulting and Planning Commission for the National Security Council
vii. Executive Director for the Presidential Commission on Open and Electronic Government
viii. Telecommunications Superintendent

c. In 2022, the Prevention and Protection against Cybercrime bill was passed by Congress[19] (it can be found here). This bill allows for:
i. The procedural rules for incorporating digital media that allow for the extraction of evidence.
ii. It defines cybercrime as criminal activities of national or transnational scope and reach.
iii. Protects Guatemalans and their personal data from cybercriminals.
iv. Strengthens the social-digital coexistence rules in the country.
v. Updates national legislation for this new digital era
vi. Defines crimes such as cybercrime, IT fraud, etc.
vii. Creates the Center for Institutional Security and Technical Response for IT Incidents
viii. Promotes the execution of actions that prevent attacks on data or IT systems.
ix. Creates alerts for detecting and attacking cybersecurity and cyber defense emergencies.

v. Corporate response to the issue
1. Businesses have been able to attend the issue via a wide variety of options to learn, train and also acquire the capabilities necessary to implement cybersecurity solutions fit for their particular situation.
2. Cybersecurity solutions via hardware and software are readily available "over the counter" at stores like:
a. Office Depot
b. MAX
c. Intelaf

[19] Pérez, C., & Montenegro, H. (2022, August 4). *Congreso aprueba Ley de prevención y protección contra la ciberdelincuencia y esto se sabe de la normativa*. Prensa Libre. Retrieved June 7, 2023, from https://www.prensalibre.com/guatemala/politica/congreso-aprueba-ley-de-prevencion-y-proteccion-contra-la-ciberdelincuencia-y-esto-se-sabe-de-la-normativa/

3. Companies that offer cybersecurity solutions for different types of organizations and even government entities are also growing in the country.
    a. SISAP
    b. Devel
    c. GBM
4. Universities have developed cybersecurity tracks to develop new professionals specialized in this very specific and crucial area of IT.
    a. Universidad Galileo
    b. Universidad Panamericana
    c. Universidad del Valle
    d. Universidad Mariano Gálvez
5. The greatest challenges are basically knowledge and cost.
    a. Efforts are being made to inform people and organizations about the importance of cybersecurity and the need to take concrete action to protect information, personal data, etc.
    b. An important challenge, especially for businesses, is cost. Intermediation costs, import tariffs and taxes increases the cost of doing business and implementing the solutions needed to protect information.
    c. Transaction costs (especially credit card commissions, for example) are also high, so the incentive to innovate and get updated is still low, especially for small and medium businesses.

3. Solutions
    a. 100% Government
        i. Government mandated cybersecurity standards through legislation and regulations for all businesses.
        ii. Price fixing of minimum requirements to pass cybersecurity standards assessments.
        iii. Legal, judicial, and penal code reforms to investigate, pursue, judge, and punish cybercrime.
        iv. Adopt international standards like HIPAA to enforce data privacy regulations and standards in the country.
    b. 100% Market
        i. Companies understand, through training and organizations like INCIBEGT who raise awareness, their need to adopt cybersecurity measures to protect their information as well as their customers.
        ii. Companies contract solutions from international providers.
        iii. Academia understands the need and begins offering education and certification.
        iv. Local cybersecurity companies begin to appear and offer competitive solutions and prices.
        v. Local private entities, such as INCIBEGT, begin to develop shared standards and consensus around important cybersecurity frameworks to better protect

companies and end users. These entities help draft basic legal frameworks to investigate, pursue and punish cybercrime.

vi. Companies and end users are held 100% accountable for the consequences of improper use of IT technologies, cybercrime, and privacy breaches.

vii. Companies begin to demand from suppliers basic cybersecurity standards in order to do business with them.

c. Corporations seeking to satisfy shareholders and stakeholders.

i. This approach would look very similar to the market approach although a major difference might be stronger lobbying from "cybersecurity guilds" to block foreign entrants, require certain legal licenses to offer services and to legally require companies to abide by standards that are way beyond their needs and might make them less competitive.

ii. Corporations might also promote the blocking of specific legislation and regulations that protect individual data privacy so that they can exploit it, sell it or use it for marketing purposes.

4. Discuss the advantages and disadvantages of each approach and include opportunity costs.

a. Government

i. Advantages

1. Centralized control of policy, regulation, and standards.
2. Price fixing can allow smaller companies to afford solutions.

ii. Disadvantages

1. Minimum standards can disincentivize companies from adopting stronger measures to protect their information and their customers.
2. More qualified solution suppliers can withdraw given price caps.
3. Corporations can lobby for looser legislation and regulation for their practices.
4. Corporations can also lobby for licenses for new entrants in the cybersecurity solutions space in order to protect local industry.
5. Legislation and regulation can easily fall behind compared to the rapid advances in technology.

b. Market

i. Advantages

1. Competition promotes innovation around the cybersecurity space.
2. Companies assume responsibility and are accountable by the market for how the protect their information and their customers'.
3. New businesses and new academic tracks for IT professionals can develop around the cybersecurity space.
4. Companies can choose from a variety of solutions to set up in their business and customers are more empowered to choose whether to share private information and whether to authorize companies to use it.

ii. Disadvantages

1. No minimum, legally mandated standards.
2. Customers might not have legal recourse when privacy is violated.

3. With no standards or regulation, fake businesses can be set up that cheat companies and users by selling bogus cybersecurity solutions.

c. Corporate
    i. Advantages
        1. Corporate consensus around standards allows for better protection of private or sensitive information.
        2. Corporate pressure can help prosecute cybercrime.
        3. Corporate pressure can motivate more companies to adopt cybersecurity measures and standards.
    ii. Disadvantages
        1. Corporations can lobby and promote legislation and regulation that benefits them, and leaves end users unprotected.
        2. Corporations can lobby for licenses that prevent new entrants from competing in the market.
        3. Corporations have more resources to defend themselves from lawsuits and through LLC regulation, avoid personal responsibility and accountability for cybercrime.

5. Take an informed stance with a rationale.
    a. I will always advocate for a market approach to the cybersecurity issue, with a basic legal framework that gives recourse to the investigation, pursuit and prosecution of cybercrime and data privacy violations.
    b. It is important to foster private efforts to educate the population, and form new, well trained cybersecurity professionals that can build new companies that offer a wider array of options and solutions.
    c. It makes sense that the government invests in training police, prosecutors, and judges in understanding cybercrime in order to better engage these issues as they arise.
    d. Private NGO's like INCIBEGT are key to form a stronger cybersecurity culture in the country that helps protect businesses and individuals.