La Ciberseguridad en Guatemala

Introducción

La seguridad informática, también conocida como ciberseguridad, seguridad de tecnología de la información o seguridad cibernética, se enfoca en la protección de la infraestructura computacional y comprende el software (bases de datos, metadatos, archivos), hardware, redes de computadoras, y toda organización que valore riesgos ante posibles efectos, entre otros, por el robo o destrucción de información, anulación del funcionamiento de los sistemas, suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, robo de dinero, estafas, etcétera.

Los riesgos pueden ser causados por usuarios, programas maliciosos (malware), errores de programación, intrusos, siniestros, personal técnico interno o fallos electrónicos o lógicos de los sistemas informáticos en general.

Definición de seguridad cibernética

Para la Unión Internacional de Telecomunicaciones de la Organización de Naciones Unidas, *"Seguridad Cibernética es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno."*

Reporte 2020 BID/OEA

De acuerdo al Reporte 2020 del BID y la OEA "CIBERSEGURIDAD, Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe" la crisis propiciada por la pandemia del COVID-19 ha puesto de relieve que la vida diaria gira alrededor de actividades cada vez más digitalizadas y, por consiguiente, más sensibles a amenazas cibernéticas. De ello la inteligencia artificial, big data, redes de quinta generación, computación en la nube, IoT y computación cuántica, si bien ofrecen inmensa eficiencia e innovación, amplifican la superficie de ataque. El crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo, los daños económicos por ataques cibernéticos podrían sobrepasar el 1% del Producto Interno Bruto (PIB) en algunos países, y los ataques a la infraestructura crítica, podría alcanzar hasta el 6% del PIB.

Según el Reporte antes mencionado, basado en el Modelo de Madurez de la Capacidad de Ciberseguridad, que mide el nivel de respuesta de los países dentro de cinco dimensiones o indicadores, Latinoamérica aún no está suficientemente preparada para enfrentar ataques en el ciberespacio, únicamente 7 de 32 países cuentan con un plan de protección de su infraestructura crítica, sin embargo, desde el 2016 a la fecha, la región ha mejorado. El promedio regional todavía está entre 1 y 2, donde 1 significa la etapa inicial, 2 formativa (comenzando a crecer), 3 consolidada (instalados y funcionando), 4 estratégica (decisiones importantes) y 5 dinámica (respuesta tecnológica frente a amenazas). Centroamérica presentó un nivel de madurez promedio de 2 en las dimensiones "Cultura y sociedad" y "Educación, capacitación y habilidades", en "Política y estrategia" y "Estándares, organizaciones y tecnologías" un puntaje inferior a 2. En la dimensión "Marcos legales y regulatorios" un nivel de madurez de entre 2 y 3. Finalmente "Divulgación responsable" con el puntaje más bajo asociado a la falta para compartir vulnerabilidades descubiertas.

Por su parte Guatemala en junio de 2018, lanzó su estrategia de seguridad cibernética, además de contar con un equipo de respuesta a incidentes, bajo la supervisión del Ministerio de Gobernación. Sin embargo, no evidencia muchas oportunidades para continuar la educación terciaria en ciberseguridad.

A continuación, se presenta un resumen del resultado de avance de Guatemala entre 2016 y 2020 en los cinco indicadores (con los sub indicadores respectivos). En los que no hubo mejora se usa el signo (=), en los que tuvieron una mejora leve se usa el signo (+), y en los que tuvieron una mejora se usa el signo (++):

Ilustración 1. Avance de la situación de ciberseguridad en Guatemala, 2016-2020

1. Política y Estrategia de Seguridad Cibernética	• Estrategia Nacional de Seguridad Cibernética (++) • Respuesta a Incidentes (+) • Protección de la Infraestructura Crítica (=) • Manejo de Crisis (=) • Defensa Cibernética (=) • Redundancia de Comunicaciones (+)
2. Cultura Cibernética y Sociedad	• Mentalidad de Seguridad Cibernética (+) • Confianza y Seguridad en Internet (+) • Comprensión del Usuario de la Protección de la Información en Línea (++) • Mecanismos de Denuncia (+) • Medios y Redes Sociales (++)
3. Educación, Capacitación y Habilidades en Ciberseguridad	• Sensibilización (=) • Marco para la Formación (=) • Marco para la Capacitación Profesional (=)
4. Marcos Legales y Regulatorios	• Marcos Legales (++) • Sistema de Justicia Penal (+) • Marcos de Cooperación para Combatir el Delito Cibernético (++)
5. Estándares, Organizaciones y Tecnologías	• Cumplimiento de los Estándares (+) • Resiliencia de la Infraestructura de Internet (=) • Calidad del Software (++) • Controles Técnicos de Seguridad (+) • Controles Criptográficos (++) • Mercado de Seguridad Cibernética (+) • Divulgación Responsable (=)

Fuente: CIEN, elaboración propia con base a información del BID.

Finalmente, en el Reporte se menciona que, la ciberseguridad no ha ganado presencia en la agenda política, si bien identifican el peligro, no toman las medidas contra las amenazas y crímenes del ciberespacio, actividades maliciosas que no sólo amenazan las economías, sino también el funcionamiento mismo de las democracias, libertades y valores. También identifica la poca capacidad para investigar los delitos que se cometen en el ciberespacio, más aún, que dichos delitos resulten en juicio. Por lo que las políticas y los marcos legales deben ajustarse y todas las partes interesadas de la sociedad, sectores público y privado, deben trabajar para crear una cultura de ciber conciencia y capacitar a profesionales calificados para construir una estrategia.

El entorno internacional

La Asamblea General de las Naciones Unidas del 14 de julio de 2021, el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, reafirmó que la soberanía de los Estados y las normas y principios internacionales, le son aplicables a la realización por los Estados de actividades relacionadas con las TIC y su jurisdicción sobre la infraestructura tecnológica que se halle en su territorio.

Bajo el principio de no intervención, los Estados no deben intervenir directa o indirectamente en los asuntos internos de otro Estado, incluso por medio de las TIC. También reafirma que los Estados deben tratar de garantizar que su territorio no sea utilizado por actores no estatales para cometer actividades contra la paz y la seguridad internacional.

El entorno nacional

El Ministerio de Gobernación en marzo de 2018, publicó el Documento Técnico No. 1 de la Estrategia Nacional de Seguridad Cibernética, para dar cumplimiento a la Resolución de la Organización de Estados Americanos AG/RES. 2004 (XXXIV-0/04) denominada "Adopción de una estrategia interamericana integral de seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética". Actualmente no existe entidad que coordine a nivel nacional la respuesta a incidentes cibernéticos, por ello se pretende abordar el tema dentro del marco del Sistema Nacional de Seguridad y conformar un Comité Nacional de Seguridad Cibernética.

En Guatemala, no existe normativa específica que aborde los delitos cibernéticos acorde a estándares internacionales, para lo que el Gobierno ya expresó el interés por adherirse al Convenio de Budapest (2001). Por su parte, el Código Penal tipifica delitos informáticos como la destrucción de registros informáticos, alteración de programas, reproducción de instrucciones o programas de computación, registros prohibidos, manipulación de información, uso de información, programas destructivos y alteración maliciosa de número de origen. La pornografía infantil, como delito cibernético, está regulada en la Ley Contra la Violencia Sexual, Explotación y Trata de Personas. Por lo que pese haberse presentado en el Congreso de la República las iniciativas de ley 5254, 5239 y 5601 en los años 2017, 2018 y 2019, relativas a la Ley Contra la Ciberdelincuencia, Ley Contra Actos Terroristas y la Ley de Prevención y Protección contra la Ciberdelincuencia, aún sigue faltando la tipificación apropiada frente los delitos cibernéticos dificultando la coordinación a nivel internacional.

Conclusiones

1. A medida que los Estados se vuelven cada vez más dependientes de las TIC, es esencial que se observe un marco común de comportamiento estatal responsable en el contexto de la seguridad internacional.
2. En Guatemala, no existe normativa específica que aborde los delitos cibernéticos acorde a estándares internacionales.
3. Actualmente no existe una entidad que coordine a nivel nacional la política de prevención y respuesta a incidentes cibernéticos.

Recomendaciones

1. Considerar la adhesión al Convenio de Budapest, como instrumento para generar y fortalecer vínculos de coordinación y cooperación internacionales.
2. Aprobar una ley contra la ciberdelincuencia, con referencia en estándares internacionales aplicados a la realidad guatemalteca.
3. Conformar el Comité Nacional de Seguridad Cibernética, como ente coordinador oficial frente a incidentes informáticos.
4. Modernizar las instituciones del sector justicia y adecuar normas y estándares en los procesos judiciales y el manejo de la evidencia digital.