#FreshStartMonday

Aumento de Cibercrímenes y su Regulación

¡Bienvenidos a #FreshStartMonday!

Cybercrime is the greatest threat to every company in the world. -
Ginni Rommety

Derivado de la pandemia de COVID-19, muchas personas y empresas se vieron obligadas a adoptar formas de trabajo que involucran tecnología. Esto implicó que se incrementara una exposición y amenazas de cibercrímenes. De conformidad con el informe anual que realiza el Equipo de investigación y Análisis de Kaspersky, durante esta época, en América Latina, los ciberataques crecieron un 24%, generando un promedio de 35 ataques por segundo. En Guatemala, estos ataques se incrementaron en un 43%.

De acuerdo con el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos, la ciberdelincuencia "*es un conjunto de hechos cometidos en contra o a través del uso de datos o sistemas informáticos*". Debido a la rapidez con la que avanza y evoluciona la tecnología, estos ilícitos se vuelven más recurrentes y peligrosos, teniendo un alcance transnacional, requiriendo de conocimientos especializados para erradicarlos.

Los ataques más comunes en 2020, según el informe "Ciberamenzas y tendencias", son:

- *Ransomware:* que impide que el usuario utilice su dispositivo hasta pagar un rescate. En este proceso el criminal podrá exfiltrar y cifrar la información.
- *Botnets:* que infectan con un software malicioso a los equipos informáticos mediante el envío sin consentimiento de *spam*, virus y distintos ataques.
- *Código dañino avanzado:* código informático que vulnera el sistema permitiendo el robo de información, datos y cualquier otro tipo de archivo importante.
- *Ingeniería social:* ataques complejos que se dan a través de correos electrónicos, mensajes o llamadas donde el criminal busca obtener información privada manipulando al usuario haciéndose pasar por otra persona, empresa u otro.

En el año 2020, el Comité de Ministros del Consejo de Europa aprobó la solicitud del Estado de Guatemala para ser parte del Convenio sobre Ciberdelincuencia de Budapest. El objetivo del Convenio es coordinar entre los Estados parte, políticas contra la ciberdelincuencia y así proteger la integridad, seguridad y libertad de las personas en las redes. A la fecha, Guatemala no ha desarrollado aun un cuerpo normativo específico apegado a este convenio.

La importancia en conocer sobre el Cibercrimen radica en que los bienes jurídicos en peligro por su actividad son:

- Los datos personales y la intimidad informática
- La indemnidad sexual de los niños, niñas y adolescentes
- La confidencialidad
- La integridad
- La disponibilidad de la información y datos contenidos en sistemas informáticos
- El comercio y la economía

Regulación legal	Descripción del tipo
Destrucción de registros informáticos, artículo 274 A	Quién destruya, borre o de cualquier modo inutilice, altere o dañe registros informáticos;
Alteración de programas artículo 274 "B"	Al que alterare, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras.
Reproducción de instrucciones o programas de computación artículo 274 C	El que, sin autorización del autor, copiare o cualquier modo reprodujere las instrucciones o programas de computación.
Delito de Registros prohibidos, artículo 274 D	Al que creare un bando de datos o un registro informático con datos que pueden afectar la intimidad de las personas.
Manipulación de información artículo 274 E	Al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica.
Delito de uso de información artículo 274 F	Al que, sin autorización, utilice u obtenga para sí o para otro, datos contenidos en registros informáticos, bancos de datos o archivos electrónicos.
Programas destructivos artículo 274 G	Al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que pueden causar perjuicio a los registros, programas o equipos de computación.

Ante el avance del Cibercrimen, en los últimos años, se han presentado tres iniciativas de ley que buscan sancionar esta actividad criminal: En el año 2017 se presentó la iniciativa 5253, Ley de ciberdelincuencia; en el año 2018 la iniciativa 5339, Ley contra actos terroristas; y en 2019 la iniciativa 5601, Ley de prevención y protección contra la ciberdelincuencia. A la presente fecha, el Congreso de la República no ha aprobado alguna de esas iniciativas.

En estas épocas donde la virtualidad y el comercio electrónico se encuentra en auge, nuestro equipo le recomienda implementar las siguientes prácticas para evitar ser víctima de Cibercrimen:

1. Nunca revele sus contraseñas, acostumbre a cambiarlas periódicamente, y no recurra a claves sencillas.
2. No coloque información personal, claves de tarjetas o información de cuentas corrientes sin antes indagar en la veracidad y credibilidad del sitio que las solicita.
3. Antes de introducir cualquier información de pago en una página o sitio web, asegúrese de que el mismo se encuentra encriptado, comprobando su dirección. La inclusión de una "s" en el protocolo de comunicación (http) convirtiendo el mismo en "https", indica que dicha página se encuentra encriptada, pero la encriptación no garantiza que el sitio no sea vulnerable a un fraude o estafa.
4. Si cuenta con dicho medio, realice sus pagos mediante tarjeta de crédito, ya que el mismo ofrece seguros, garantías o recursos en caso de fraude sobrefacturación, mercancía no recibida o artículos devueltos. Puede presentar una reclamación ante el emisor de la tarjeta si es víctima de algún incidente.
5. No compre nada a vendedores en línea que sólo acepten pagos con tarjetas de regalo, transferencias de dinero o criptomonedas. Estos tipos de pagos son más complejos de rastrear y revertir.
6. Lea la política de privacidad de los sitios que visita o interactúa. Debería poder encontrar la información personal que el sitio recoge, por qué, y cómo se utilizará. Si la política de privacidad no está disponible o es difícil de entender, considere la posibilidad de utilizar otro sitio.

7. No descargue o abra archivos adjuntos o imágenes que provengan de correos electrónicos sospechosos.
8. No atienda o responda a mensajes que no espera. Investigue primero para cerciorarse sobre su legitimidad.

Leopoldo Zeissig

Julio Méndez