Arcila & Sotomayor
DERECHO PENAL

"NECESIDADES DEL NEGOCIO VS. MITIGACIÓN DE RIESGOS"

Con el surgimiento del internet, las modalidades de trabajo y estudio empezaron una transformación paulatina gracias a la eliminación de las fronteras debido a las facilidades de comunicación. En los últimos años hemos visto como las plataformas virtuales han reemplazado los cafés, las oficinas, las aulas de clase, las estanterías de los supermercados y los almacenes de los centros comerciales, dado que podemos acceder a los mismos beneficios que estos espacios nos brindan a través de una pantalla desde la comodidad de nuestros hogares. Aplicaciones, como Facebook, WhatsApp, Instagram, Twitter, YouTube, Amazon, Telegram, Olx, MercadoLibre, Open English, entre muchas otras, son un claro ejemplo de lo anterior.

Es así como muchas modalidades de negocio se han inclinado a adecuar la prestación de sus bienes y servicios con este fenómeno conocido como "economía cerrada" o "economía confinada"[1], La cual permite a los trabajadores cumplir con sus funciones desde sus casas.

Aún cuando se trataba de un fenómeno en alza, su acogida se había producido de forma paulatina, razón por la cual, la prestación personal del servicio seguía desempeñando un papel fundamental en la economía de mercado. Sin embargo, con la propagación del COVID-19 y la declaración de emergencia sanitaria a nivel mundial, la adopción de medidas virtuales en los puestos de trabajo y educación dejó de ser una opción para convertirse en una necesidad.

De esta manera, las universidades han recurrido a la educación virtual, los establecimientos de comercio ofrecen sus productos en redes sociales o plataformas destinadas exclusivamente para estos, los gimnasios ofrecen programas de entrenamiento en línea, los restaurantes envían sus platillos a través de domicilios y las conferencias virtuales se han convertido en el medio más eficaz para realizar reuniones de trabajo.

No obstante, con la adaptación de estos mecanismos en las empresas, vienen aparejados una serie de riesgos ligados a la seguridad informática, la cual se encuentra en grave peligro debido al incremento de conductas delictivas orientadas al ataque, con fines maliciosos o económicos, de la información personal o de la empresa.

Si bien los riesgos y las medidas de seguridad se diseñan a partir de las necesidades concretas de cada negocio, el Ministerio de Tecnologías de la Información y Comunicaciones ha trazado una serie de medidas genéricas que se pueden emplear en las pequeñas, y medianas empresas. Esto sin perjuicio de las normativas aplicables para el caso de las grandes empresas que

[1[1] Matter. The Shut-In Economy. In the new world of on-demand everything, you're either pampered, isolated royalty — or you're a 21st century servant, 23 de marzo de 2015. Disponible en: https://medium.com/matter/the-shut-in-economy-ec3ec1294816

aseguren la confidencialidad e integridad de la información disponible.

Las recomendaciones planteadas por la entidad son las siguientes[2]:

- Actualice y licencie su cortafuegos y antivirus
- Realice revisión periódica de su listado de contactos y practique la utilización de firma digital o autenticación del mensaje a través de hash.
- No realice transacciones desde páginas web no confiables
- No instale herramientas de escritorio remoto, siempre y cuando no se almacene un llavero de claves seguro y confiable.
- Evite conectarse desde redes inalámbricas abiertas que no tienen ninguna seguridad.
- Cerciórese de la información de contacto con el fin de verificar el auténtico originador del mensaje.
- No descomprima archivos de extensión desconocida sin antes verificar el "vista previa" el contenido del mismo.
- Elimine correos electrónicos "Spam", de esta forma evitará ir a sitios web no seguros.
- Actualice los parches de seguridad del navegador web.
- Gestión adecuada de información confidencial y de terceros (títulos financieros, chequeras, tarjetas, productos crediticios, etc.)
- Implemente servidor de correos electrónicos SPF (Sender Polcy Framework).

Las sugerencias que se establecen por parte del Ministerio de Tecnologías de la Información y Comunicaciones y la Policía Nacional en caso de ser víctima son:

.

- Debe preservar la página, sitio web, correo
- electrónico, objeto del ataque, apóyese del área de sistemas para tomar esta evidencia que será útil dentro de la investigación formal.
- Documente la evidencia recolectada y haga uso de los protocolos de cadena de custodia.
- Aísle los navegadores no configurados o sin actualizar.
- Active la configuración del cortafuegos/filtrado de spam.
- No Instale herramientas de acceso remoto o desactive las mismas al momento de dejar en desuso el equipo de cómputo.
- Revise la configuración del cliente de correo de correo de su empresa de manera confiable.
- Clasifique la Información de su empresa de manera que los ciberdelincuentes no tengan acceso a información financiera.
- Realice respaldos o Backups de su información .
- Haga una lista de chequeo de los sitios web visitados o consultados para que sean validados como fuentes originales de sitios transaccionales.
- Ajuste me manera periódica las políticas de uso de antivirus
- Revise constantemente la prestación de servicios ante terceros y servicios de soporte

Los anteriores "tips" de seguridad nos ayudarán a prevenir cualquier ataque informático y evitar por tanto que seamos víctimas de los ciberdelincuentes.

[2] Disponible en: https://www.mintic.gov.co/gestionti/615/articles 5482_Guia_Seguridad_informacion_Mypimes.pdf