CIBERSEGURIDAD EN COOPERATIVAS

Boletín FACACH

VOL. 3, EDICIÓN 1 AUTOR: RIESGOS FACACH DICIEMBRE 2022

Realidad mundial

En 2021, el fraude bancario por Internet en el Reino Unido aumentó un 117% en volumen y un 43% en valor en comparación con los niveles de 2020, por el incremento del comercio electrónico.

El "fracaso de ciberseguridad" entre los 10 principales riesgos que más han empeorado desde el inicio de la crisis de COVID-19. (Encuesta Global de Percepción de Riesgos (GRPS))

Las empresas también operan en un mundo en el que el 95% de los problemas de ciberseguridad se pueden atribuir a errores humanos. (Global Risk Report 2022)

El Ransomware se está convirtiendo en una amenaza peligrosamente creciente y presenta una gran preocupación para la seguridad pública. (Foro Económico Mundial)

Vulnerabilidades cibernéticas

- En el contexto de la dependencia generalizada de sistemas digitales cada vez más complejos, las crecientes amenazas cibernéticas están superando la capacidad de las sociedades para prevenirlas y gestionarlas de manera efectiva. A medida que las amenazas cibernéticas continúan creciendo, asegurar contra tales riesgos será cada vez más precario, y las propias aseguradoras enfrentarán ataques de represalia por intentar frenar los pagos de ataques como ransomware (uno de los mas comunes para las empresas y sus bases de datos).

- Los profesionales de TI y ciberseguridad ya sobrecargados están bajo una carga cada vez mayor, debido a la creciente complejidad de las regulaciones para los datos y la privacidad, a pesar de que tales regulaciones son fundamentales para garantizar la confianza pública en los sistemas digitales.

- Cuando se produce un ataque, las empresas se verán obligadas a pagar rescates cada vez más altos o a sufrir las consecuencias reputacionales, financieras, regulatorias y legales de los ataques cibernéticos.

(Global Risk Report, 2022).

Consideraciones organizacionales

Hace tiempo se pensaba que la seguridad informática era algo solamente posible y aplicado por los grandes bancos u organizaciones internacionales. En las pequeñas empresas, si bien, los expertos en la materia demostraban con hechos la necesidad de implementar políticas de seguridad informática eficientes, los líderes de estas organizaciones no necesariamente daban la debida atención al tema.

A medida que crece nuestra dependencia de las tecnologías digitales e Internet 3.0 se convierte en realidad, se intensifican los esfuerzos dirigidos a crear normas y definir reglas de comportamiento para todas las partes interesadas en el ciberespacio.

La ciberseguridad se ha convertido en una prioridad para los gobiernos de todo el mundo, ya que consideran que proteger a los activos disponibles a través de internet, los sistemas y las redes informáticas de los hackers es vital para el funcionamiento, la estabilidad de una nación y el sustento de su gente. A menos que actuemos para mejorar la confianza digital con iniciativas intencionales y persistentes de fomento de la confianza, el mundo digital continuará derivando hacia la fragmentación y la promesa de una de las eras más dinámicas del progreso humano puede perderse.

Iniciativas y soporte al sector cooperativo

El desafío de invertir en la seguridad informática en las instituciones, significa pensar en el problema que tienen latente y a corto plazo. La seguridad informática, es la infraestructura computacional de la institución, incluyendo la información contenida, existen una serie de estándares, protocolos, métodos, herramientas para minimizar los posibles ataques o riesgos de la información estructural de la institución.

Es por ello que en los recientes años, FACACH en coordinación con Red Tecnológica S.A. de C.V. a fortalecido la seguridad informática de los servidores mediante Firewall y la adquisición y actualización de antivirus lo suficientemente robusto para protegerse de cualquier amenaza. Así como también, se está implementando la creación de respaldos en sitios alternos para estar preparados ante cualquier eventualidad que pueda suceder y de forma mas reciente se ha realizado la adquisición e instalación del Office 365 para el personal, manteniendo respaldos en nube, haciendo mas eficiente la capacidad de almacenamiento del servidor. .

Así mismo, teniendo en cuenta el riesgo cibernético al que se exponen día a día sus cooperativas afiliadas y la importancia de la ciberseguridad en cada una de ellas, ha emprendido iniciativas de formación, brindando capacitaciones en temas de Ciberseguridad, en la que participó un total de 224 personas pertenecientes a las cooperativas federadas. De igual forma, se proporciona formación en colaboración con DGRV y CONAJOVEN a los jóvenes, en temas de Transformación digital, en consonancia con la problemática actual y de como ellos pudiesen generar soporte, apoyo y conciencia en estos temas de vital importancia en cada una de sus organizaciones cooperativas.

Las Cooperativas y sus líderes organizacionales debemos permanecer atentos a preocupaciones continuas como el cibercrimen y los ataques cibernéticos. A nivel organizacional, es vital mejorar las habilidades de los líderes en temas de ciberseguridad, invertir en el equipo tecnológico y elevar los riesgos cibernéticos emergentes a las conversaciones a nivel de la juntas, fortaleciendo la resiliencia cibernética, por ser un riesgo latente en nuestras organizaciones.