



Relatoría del XXXVIII Congreso Latinoamericano de Seguridad Bancaria realizado en Ciudad de Panamá, Panamá

Acto Inaugural

El Secretario General de FELABAN dio la bienvenida a todos los participantes, agradeciendo a Asociación Bancaria de Panamá, al Comité Organizador y a todos los que hicieron posible el Congreso de CELAES en versión presencial logrando convocar a YYY asistentes de XX países. El Presidente del CELAES compartió los aspectos más importantes tratados en la reunión del Comité, resaltando la similitud de los riesgos que enfrentan todos los países de la región, evidenciando que el crimen organizado opera en todos los países de la región, declarando la necesidad de compartir información usando tecnología en el entendimiento de que **“En Seguridad no se compite, se comparte”**.

La Migración en Latinoamérica, Impacto Social, Económico y de Seguridad en la Región. La migración en Latinoamérica es un fenómeno complejo para la región en términos sociales, económicos y de seguridad, habiendo experimentado un aumento constante en las últimas décadas, generando gran impacto en el aspecto económico, social y de seguridad. El tráfico de personas, la inseguridad en el traslado, las crisis humanitarias y el incremento en los niveles de violencia son la consecuencia del desplazamiento de estas familias que se evidencian en los países tanto de tránsito como de destino.

La Transformación Digital y los Riesgos de Fraude. La pandemia del SARS COVID-19 fue un activador de la transformación digital ya que todas las entidades financieras tuvieron que acelerar el proceso para atender la demanda exigida por las personas que no podían desplazar libremente, dando oportunidad para introducir nuevas herramientas basadas en Inteligencia artificial, la ciencia de datos, la productividad y la experiencia cliente. Sin embargo, estas nuevas oportunidades vinieron acompañadas de nuevos riesgos cibernéticos que tuvieron que ser afrontados con mecanismos de autenticación, servicios de monitoreo y respuesta a incidentes de ciberseguridad y educación de clientes. Destacando los casos de fraude financiero, la ingeniería social, fraude en el comercio electrónico, el secuestro de datos y la suplantación de identidad.

Más Allá de la Regulación: Desarrollo Ágil y Seguro. La transformación digital ha cambiado la forma en que las organizaciones desarrollan software y ofrecen soluciones a los clientes. La agilidad y la seguridad se han vuelto cruciales para sobrevivir en un mercado en constante evolución y para mantener la confianza del cliente en un entorno de amenazas cibernéticas crecientes. El desarrollo ágil y seguro es esencial en un mundo digitalizado y altamente competitivo. Las organizaciones que buscan destacar y mantener la confianza del cliente deben optar por la agilidad y la seguridad como parte integral de su estrategia de desarrollo. Al hacerlo, no solo cumplirán con las regulaciones, sino que también obtendrán una ventaja competitiva y garantizará un futuro sostenible en un mercado en constante cambio.

Aprendizajes del Primer Piloto de Fraude y Ciberseguridad en 11 Países de Latinoamérica. La ponencia inició explicando el marco de trabajo del modelo de colaboración desarrollado por FELABAN, observando tanto la dinámica de los ciclos de notificaciones de incidente como la forma de tratar datos transaccionales referidos a un producto financiero. Se comentaron algunas técnicas utilizadas para el encubrimiento de compras de bitcoin para realizar fraude posteriormente, también se mostró el impacto financiero generado por uno de los casos reportados durante el ejercicio con el objetivo de tener claramente cuanto es la exposición real a casos de fraudes. Desde ataques simultáneos, variables ofuscadas y patrones de fraude inteligente frente a todo un país se vieron reflejados en los distintos gráficos de la presentación. Algunas conclusiones con respecto a la forma de alinear modelos colaborativos a una comunidad bancaria, integrando factores internos y externos para convertirlos en información valiosa. El fraude electrónico y los incidentes de ciberseguridad están muy relacionados y ambos tienen en común las fases de preparación, detección, contención y recuperación. Por lo tanto, el factor importante es alinear los modelos de datos de ambos para encontrar similitudes y por ello se FELABAN propone una matriz universal de datos que nos permita compartir información de manera segura, organizada y fluida.

Lucha Contra el Ransomware Mediante Validación en el SOC en Tiempo Real. El Ransomware es una modalidad de ciber fraude que viene creciendo en la región y representa una amenaza para la continuidad de las operaciones, la confianza y la seguridad del sistema financiero. Es necesario implementar soluciones en tiempo real para poder detectar y estas amenazas oportunamente, tener respuestas rápidas e inmediatas para contener la amenaza y proteger los datos críticos, minimizando los daños y evitar que este malware cause un daño significativo, evitando el pago de rescate para recuperar la información comprometida que en muchos casos no es posible obtener y fomentar un círculo vicioso bajo este esquema de fraude. Por eso es importante implementar un Security Operation Center (SOC) como estrategia de continuidad de negocio, para mantener la operación de los productos y servicios financieros a disposición de nuestros clientes

Gestión de Riesgo: Resiliencia para la Continuidad de Negocio. La gestión de riesgos y la resiliencia son factores importantes para garantizar la continuidad de los negocios en un mundo en constante cambio. Las organizaciones que invierten en la identificación, evaluación y mitigación de riesgos, así como en planes de continuidad de negocios, están mejor preparadas para enfrentar desafíos inesperados. La resiliencia es la clave para mantener la estabilidad y la competitividad de un entorno empresarial en constante evolución. La gestión de riesgos y la resiliencia son inversiones críticas para el éxito a largo plazo de cualquier organización.

Alianzas Estratégicas con la Industria Fintech. Las alianzas estratégicas con la industria Fintech representan una oportunidad para instituciones financieras tradicionales de abrazar la innovación y mejorar sus servicios. Al seguir las mejores prácticas y mantener una mentalidad abierta hacia la colaboración, las instituciones financieras pueden beneficiarse significativamente de estas alianzas. La clave está en encontrar socios Fintech adecuados, establecer objetivos claros y mantener una comunicación constante para aprovechar al máximo estas colaboraciones y ofrecer soluciones financieras más avanzadas y competitivas.

Panel: Experiencia y Buenas Prácticas Corporativas de Seguridad Integral. La seguridad integral en el entorno corporativo es un desafío que las organizaciones deben

abordar de manera proactiva. Hoy las experiencias y las mejores prácticas corporativas destacadas en este informe muestran que una aproximación integral a la seguridad es esencial para proteger los activos y garantizar la continuidad de las operaciones la combinación de políticas de seguridad sólida, contar con la infraestructura necesaria, desarrollo del talento humano, gestión de la Información, demostrar con cifras la gestión, desarrollo de una cultura de seguridad, capacitación en temas de interés y evaluación constante es clave para el éxito en este aspecto. Hoy la seguridad integral no solo protege los activos, sino que también construye la confianza de los clientes y socios lo que es fundamental en el entorno empresarial actual.

Orquestando el SOC con los Servicios de Detección y Respuesta. Los principales beneficios de la orquestación generan la reducción de falsos positivos, una mayor eficiencia por la automatización de procesos y respuestas a incidentes cibernéticos, siguiendo procedimientos y políticas predefinidos que garanticen respuestas coherentes y de alta calidad. Como mejores prácticas resulta indispensable el establecimiento de procedimientos y flujo de trabajo claros, definir una política para formar y mantener capacidades de los colaboradores y entrenarlos en servicios de detección y respuesta; sometiendo a evaluación continua tanto las herramientas como los procesos y respuesta para mantener alineadas las capacidades para enfrentar las amenazas cibernéticas, a fin de proteger los activos de información y la continuidad de las operaciones.

Continuidad de Negocio: Ciber resiliencia en Entorno Cambiante. La ciber resiliencia es una parte esencial de la estrategia de continuidad de negocio en un entorno empresarial en constante cambio. Las organizaciones deben estar preparadas para adaptarse a las amenazas cibernéticas en constante evolución y para mantener la continuidad de las operaciones, incluso en situaciones adversas. La combinación de evaluaciones de riesgos regulares, planificación de continuidad, Protección de Datos y capacidad de respuesta rápida son elementos clave en la construcción de una estrategia de ciber resiliencia efectiva. La inversión en ciber resiliencia no solo protege los activos de la organización, sino que también asegura la confianza y la reputación del cliente en un mundo digital cada vez más interconectado.

Panel: Uso de la Analítica de Video en la Gestión del Negocio. Dentro de las principales aplicaciones de la analítica de video identificamos la seguridad, detectando intrusiones, vigilancia, y seguimiento de actividades sospechosas. El comportamiento del cliente dentro de las oficinas o tiendas lo que permite tomar decisiones basadas en información para mejorar la experiencia cliente. La gestión de instalaciones para el control de acceso, la supervisión de sistemas de climatización y conservación de energía entre otros beneficios. Reduciendo costos, mejorando la seguridad y satisfacción del cliente. A pesar de los beneficios que genera esta tecnología también nos plantea desafíos importantes relacionados con la privacidad de datos, el almacenamiento y procesamiento de las imágenes.

El Estado de la Ciberseguridad y el Impacto en el Sector Financiero Global. El Rol de la Mujer en la Seguridad Corporativa en Instituciones Financieras El papel de las mujeres en la seguridad corporativa de instituciones financieras es esencial para aprovechar la diversidad de habilidades y perspectivas que ofrecen. La promoción de la igualdad de oportunidades y la eliminación de prejuicios son pasos fundamentales para garantizar que las mujeres tengan un lugar significativo en este

campo. Las organizaciones que valoran y promueven la diversidad y género en sus equipos de seguridad corporativa pueden lograr un ambiente de trabajo más inclusivo y mejorar la efectividad en la gestión de riesgos y seguridad la contribución de las mujeres en la seguridad corporativa es un recurso valioso que debe aprovecharse.

Cierre de la Conferencia.

El resultado de CELAES 2023 ha sido satisfactorio, destacando los temas tratados, expositores, agenda académica, la variada oferta de servicios presentados en la zona de exposición y la información compartida, identificándose la necesidad de compartir información entre los países de Latinoamérica a través de mecanismos automatizados por el alto volumen de información y la oportunidad de contar con información de riesgos que afectan el normal funcionamiento de los sistemas, productos y servicios financieros, así como la importancia de participar en este tipo de eventos en formato presencial debido al valor que genera la interacción personal.

Se anunció como Sede del CELAES XXXIX la Ciudad de Miami, el cual se desarrollará en el mes de junio de 2024, invitando a los asistentes a participar de los próximos congresos organizados por FELABAN.

**Preparado: Junta Directiva Comité CELAES
Octubre de 2023**