PUBLICACIÓN No. 2 | MAYO 27 DE 2020 | BOGOTÁ - COLOMBIA

CÁPSULAS SOBRE Ciberseguridad

AL DÍA CON FELABAN

FIC
FRAUD INFORMATION CONTROL
by FELABAN

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

55 AÑOS
1965 - 2020

PLANEANDO LA DEFENSA ANTE LA CIBER-EXPOSICIÓN

La ciberseguridad es un tema que está en permanente cambio, lo que exige que instituciones públicas, privadas y personas naturales, estén constantemente informándose de las tendencias y las nuevas prácticas delincuenciales que puedan poner en riesgo los datos, activos e información confidencial. Hoy en medio de la pandemia, el fraude y la seguridad virtual tiene nuevas dimensiones y desafíos. En esta segunda edición de las cápsulas de Ciber seguridad, se plasma un recorrido por los componentes básicos para tener en cuenta por las entidades, en cuanto al diseño y preparación de su plan de ciberseguridad.

Para alcanzar un nivel de cobertura que responda en cierta medida a los miles de nuevos códigos maliciosos que se disparan cada día y los millones de nuevas líneas de código que se inyectan cada año en el ciberespacio, no es solo necesario estar actualizado con la información emergente, sino también estructurar un plan que permita sistemáticamente defender desde diferentes frentes, todas las áreas que puedan estar expuestas.

De acuerdo con la publicación de EY en 2019, **"An endurance Course: surviving and thriving through 10 Major risks over the next decade"**, se plasmó el top 8 de riesgos no financieros y los respectivos progresos de implementación de procesos de administración del riesgo.

De los 3 primeros y más significativos se destaca lo siguiente:

Riesgo operacional: el 5% de los bancos se encuentran en etapas tempranas de implementación, solo el 13% se encuentran en procesos completamente terminados y el 29% lleva un progreso un poco más de la mitad en su desarrollo.

Riesgo de seguridad de la información: 9% en etapas tempranas, 8% complemente terminados y 40% por encima del 50% del progreso.

Riesgo cibernético: 13% en etapas tempranas, 4% completamente terminado y 40% por encima del 50% del progreso.

Así mismo, el mencionado documento, recopiló la información sobre los talentos que los bancos consideran que aún requieren el día de hoy. A continuación, el porcentaje de bancos que identifican la necesidad por tipo de habilidad.

Habilidades demandadas que requieren experiencia en riesgo y porcentaje de Bancos que reportaron dicha necesidad:

- Gerencia de modelos de riesgo en Inteligencia Artificial y Machine learning – 73%
- Testeos de estrés – 23%
- MRM Tradicional – 16%
- Riesgos Financieros 16%

Habilidades demandadas que no requieren experiencia en riesgo financiero y porcentaje de Bancos que reportaron dicha necesidad:

- Ciberseguridad- 77%
- Seguridad de la información: 51%
- Tecnología: 46%
- Resiliencia Operacional (Riesgo de Mercado, crédito y liquidez): 29%

Estos talentos laborales son parte de las necesidades que una entidad financiera requiere para atender los diferentes desafíos que hoy se presentan en materia de seguridad virtual. El análisis y examen de lo que se requiere para diseñar planes en este campo nos permiten sintetizar algunos puntos que a nuestro juicio son determinantes para incluir.

1- El lenguaje y Fundamentos Importan

Lo primero y más esencial es que desde la organización, se prepare integralmente el conocimiento fundamental sobre la ciber-seguridad. Es necesario incluir con claridad el lenguaje de los componentes tales como la terminología de Ciberseguridad, Ciber espacio, Dark-web, tipos de ataques, modalidades, esto con el propósito de tener una perspectiva clara sobre como detectar amenazas, para así mismo proteger los sistemas, las redes y de esta manera estar en la capacidad de anticiparse a los potenciales ciber ataques.

2- Seguridad de las Redes, Vigilia Permanente

Uno de los mecanismos de prevención de exposición a ataques cibernéticos, es la implementación de mecanismos de seguridad de la información. En este caso, la disposición de herramientas que permitan la seguridad en las redes, que además se encuentren siempre actualizadas, permitirá tener un proceso integrado de protección de los datos que pueden ser atacados tras una penetración maliciosa en las redes de la institución. Así mismo, incluir herramientas de detección de intrusiones que además recolecten la evidencia de estas, auditorias constantes de las redes para detectar puntos potenciales de penetración de los que no se esté seguros, y planes de bloqueo de transmisión de la información a través de las redes en caso de ataques materializados.

3- Informática Forense, Datos para el Análisis

Si bien los sistemas de alertamiento y monitoreo de fragilidad de los sistemas y redes pueden contribuir a la prevención y exposición de vulnerabilidades en el ciber espacio, es muy importante aprender a analizar los datos que estos sistemas arrojan, así como realizar auditorías de sistemas que permitan observar los comportamientos y dinámicas al interior de las redes y componentes informáticos conectados a las redes. La revisión de la infraestructura tecnológica constante es un mecanismo que ayuda a prevenir posibles brechas, que los sistemas de monitoreo tradicionales pueden no estar detectando. Así mismo, la informática forense y el análisis de los datos permiten realizar una investigación de comportamientos maliciosos, potenciando la oportunidad responder al incidente de manera inmediata. La aplicación de técnicas y herramientas para aplicar la investigación digital forense arroja a la institución los datos relacionados a los crímenes computacionales generando un mapa de las vulnerabilidades que se extrapolará al plan de ciberseguridad.

4-Estrategia de Gerencia del Riesgo de Ciberseguridad

La estrategia de la gerencia del riesgo de la Ciberseguridad, depende de cada organización. Cada entidad tiene diferentes vulnerabilidades, diferentes tipos de accesos, controles y tecnología. Es por esto, que al tener la claridad sobre cómo la organización entiende la ciberseguridad, el nivel de exposición y la capacidad de seguridad en sus redes, cada entidad puede ajustar el plan de ciberseguridad de diferentes maneras. Los resultados de análisis de los procesos forenses y el apoyo del análisis de los campos anteriormente mencionados metodologías cualitativas y cuantitativas dan vía a establecer los principales vacíos, análisis del nivel de riesgo de cada uno y realizar un plan de mitigación de esos riesgos, alcanzando aún más la personalización de la estrategia.

5- Capacitación y Personal Especializado

La continua actualización frente a la dinámica constante de lo que ocurre en el ciber espacio, las modalidades y tipos de ataques es primordial. Contar con personal capacitado y especializado en estas áreas debe ser una prioridad de las organizaciones. Si bien es muy regular encontrar que las empresas que optan por tercerizar estos servicios a quienes tiene como negocio central la ciberseguridad e implementación de soluciones de tecnologías de la información, contar con expertos al interior de la organización permitirá no solo auditar el proceso del proveedor, sino también, hablar en los mismos términos con estos terceros, al final la estrategia y protección será ejecutada por el proveedor, pero diseñada y gerenciada por la organización.

La ciber-seguridad y la prevención del fraude, son temas que ganan importancia para personas, empresas, gobiernos y todo tipo de usuarios. Si el tema era importante hace 6 meses, hoy en medio de una emergencia global, el tema empieza a ser crítico por la avalancha de actividades que las personas y empresas realizan virtualmente de manera cotidiana. De seguro la industria de los servicios financieros en particular tiene retos y desafíos frente a otorgar más servicios financieros por los canales virtuales, con una mayor dosis de seguridad y confianza para los clientes. La banca que es un administrador de los pagos de bajo valor de la economía, tiene entonces un importante camino por recorrer.

Bibliografía recomendada sobre el tema

- The importance of Cybersecurity strategy for the industry, INCIBE- Instituto Nacional de Ciberseguridad de España, Agosto de 2019, en: https://www.incibe-cert.es/en/blog/importance-cybersecurity-strategy-industry
- Tienes ya la hoja de ruta de ciberseguridad de tu empresa?, INCIBE- Instituto Nacional de Ciberseguridad de España, Mayo de 2020, en: https://www.incibe.es/protege-tu-empresa/blog/tienes-hoja-ruta-ciberseguridad-tu-empresa
- Cibersecurity is Everyone´s Job, NIST- National Institute of Standards and Technology, Octubre 2018, en: https://www.nist.gov/system/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf
- Questions Every CEO Should Ask About Cyber Risks, Cybersecurity &Infraestructure Security Agency, Diciembre 2018, en: https://www.us-cert.gov/ncas/tips/ST18-007
- Tenth annual Global Risk Management survey: An endurance Course: surviving and thriving through 10 Major risks over the next decade, EY, 2019, en: https://www.ey.com/Publication/vwLUAssets/ey-iif-tenth-annual-global-bank-risk-management-survey/$FILE/ey-iif-tenth-annual-global-bank-risk-management-survey.pdf
- Europol Strategy 2020+, Europol, Febrero 2019, en: https://www.europol.europa.eu/publications-documents/europol-strategy-2020
- Global Landscape on COVID-19 Cyberthreat, Abril 2020, en: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats
- Global Cybercrime strategy, Interpol, 2017.
- Investigative support for cybercrime, en: https://www.interpol.int/en/Crimes/Cybercrime/Investigative-support-for-cybercrime
- Cybersecurity for small business, Federal Communications Commission, en: https://www.fcc.gov/general/cybersecurity-small-business
- Tips for secure web navigation an transactions, Federal Communications Commission, en: https://www.fcc.gov/consumers/guides/secure-web-navigation-and-transactions

SECRETARÍA GENERAL DE FELABAN

GIORGIO TRETTENERO CASTRO
Secretario General
gtrettenero@felaban.com

JORGE ARTURO SAZA G.
Director Económico
jsaza@felaban.com

DANIEL JUVINAO
Director Concentrador de Fraudes Regional
y Proyectos especiales
djuvinao@felaban.com

LAURA M. GORDILLO V.
Directora Adjunta Concentrador de Fraudes
Regional
lgordillo@felaban.com

ADRIANA RODRÍGUEZ
Diseñadora Gráfica
arodriguez@felaban.com

FIC FRAUD INFORMATION CONTROL by FELABAN

FELABAN FEDERACION LATINOAMERICANA DE BANCOS 55 AÑOS 1965 - 2020

siganos en: