1) ¿Se te ocurre/n alguna/s otra/s regla/s de BI que puedan ayudar a disminuir el fraude en la entidad bancaria? ¿Qué harías si quisieras utilizar la IA (Inteligencia Artificial) para este menester?

Para disminuir el fraude en la entidad bancaria hay que partir de lo general a lo particular como cualquier problema, es decir de los casos mas externos a los más particulares, los usuarios por lo general y mas en las personas grandes no tienden a estar tapando la contraseña en los cajeros u las que aplican el shoulder surfing y aunque lo hagan, con la tecnología hoy en día y las cámaras se puede visualizar desde la parte superior del cajero, por lo cual se deberá de implementar una doble verificación, es decir, por medio ya sea desde un mensaje o desde la aplicación general un código de autentificación (conocido como pin dinámico) a la hora de sacar dinero del cajero, de esta manera al menos que nuestro atacante tenga acceso remoto al móvil, no podrá sacar dinero aun teniendo la tarjeta, de esta forma tendremos la tarjeta física segura. Otra medida será la de no poner datos bancarios, así como mandarlos o comunicarlos en lugares públicos, esto debido a que en emergencias se usan ordenadores no propios, lo cual resultaría peligrosos por los riesgos que hay al introducir información y que otra persona la pueda obtener después sin nuestro consentimiento.

En cuestión de software desconozco si se implemente en todos los países, pero en México si quieres usar alguna aplicación bancaria se debe de tener la localización activada y concuerdo con esto, permitirá saber desde donde se hizo la transacción en caso de que sea fraudulenta, de la misma manera por cada inicio de sesión desde la banca móvil se deberá de enviar mensajes de texto tanto al correo del cliente como a su número con la opción de denegar el acceso y con ello poder cambiar la contraseña de forma inmediata, esto con el fin de prevenir que vuelvan a entrar o si se pierde el celular y lo logran desbloquear que no puedan sacar dinero de las cuentas, ya no solo es cuestión de la tarjeta física, si no, también las digitales.

Con respecto a la inteligencia artificial aunque no todos los celulares o dispositivos hoy en día cuenten con reconocimiento facial, la mayoría de ellos

cuentan con cámaras, por lo que si no se reconoce la autenticidad por reconocimiento facial o no esta disponible en el dispositivo que se tome una foto y de igual manera de haga llegar al cliente de la cuenta, con el fin de saber quien es y poder trascender en caso de que lo requiera, ir haciendo un expediente para que estas personas no puedan acceder a las cuentas ajenas, hacer una base de datos de estas personas que se dedican a hacer fraudes para que el sistema les negué el acceso y los clientes estén más seguros, así como de igual manera si el usuario lo quiere denegar el acceso personas las cuales tienden a quitar dinero.

Por último, dentro del personal encargado en administrar y controlar los accesos como lo es “atención al cliente”, estipular reglas para que no se pueda obtener información de ninguna manera por parte de ellos, de ser necesario usar VPN’s para así aislar las ips y que de esta forma si los delincuentes tienen acceso a la red que no les sea tan fácil llegar a la información. Usar un numero solo dentro de las horas laborales o bien, no estarse conectando a redes publicas para evitar un taque man in the middle así como payloads, restringir el uso de cunetas personales y redes sociales para evitar phishing, vishing y baiting con aquella personas que cargan su memoria y la conecta a ordenadores sin hacer un análisis o tener antivirus.

Todo lo anterior con el fin de disminuir el fraude de entidad bancaria tanto en clientes como en el personal del banco.

2) Dentro de los 3 ejes de la ciberseguridad CIA (Confidencialidad, Integridad y Disponibilidad) y viendo tu sistema de Big Data, no solo los sistemas operativos sino también los datos, tanto los datos en crudo como la información de negocio que sale del sistema, ¿Podrías argumentar los argumentos principales de cada uno de los 3 ejes?

Confidencialidad – No dar información, acceso e incluso datos a personas ajenas al cliente principal, esto incluye historiales, movimientos o incluso datos de la personas como las preguntas de seguridad debido a que si no se logra proteger esta información de primera mano no se podría decir que hay confidencialidad, lo anterior

con respecto al personal, por otro lado, no publicar información en la red a cerca del cliente y aunque a la hora de realizar una transferencia en un lugar físico los sistemas nos arrojan los datos de a quien le estamos haciendo la transferencia, arrojar el nombre y apellidos de la persona debería de estar prohibido de igual manera, aunque estos son para verificar la cuneta, se puede obtener muchas cosas con solo el nombre completo (En caso de México el DNI o CURP como se conoce en este país, se compone del nombre completo así como de la fecha de nacimiento, se estaría a nada de conseguir) y mas si se googlea, se puede acceder a información personal y con ello

Integridad – va de la mano con la confidencialidad, si se tiene acceso a la información relativamente podrían suplantar con ella a cualquier persona y de esta forma hacer movimientos en el sistema que no estén autorizados por el titular de la cuente, sin embargo no se queda solo en esto, se tiene que asegurar por parte de las aplicaciones no ceder permisos a usuarios pro algún error y que puedan hacer movimientos no autorizados así como que se haga extracción por uso de softwares externos ya sea en la base de datos o información del cliente por medio de sus dispositivos

Disponibilidad – Es por decirlo de alguna manera la contra parte de todos los casos planteados anteriormente, aquí el cliente principal siempre debe de tener acceso a sus cuentas, así como a su información (movimientos, registros, transacciones) por lo que es el punto en donde el equipo de ingeniería y software se involucran mas, pues son estos los encargados de administrar esta disponibilidad 24/7

3) ¿Esta infraestructura la pondrías on-premise (en los CPDs de tu empresa), en IaaS o en SaaS? Argumenta tu respuesta.

La pondría en IaaS o en SaaS por tener los datos siempre a la mano, como se tratan de servicios a través de la nube, la disponibilidad de datos en ellos estará siempre disponible para el personal autorizado. La principal diferencia de estos es

la cobertura y el precio, por lo cual , si se quiere tener un servicio premium con la disponibilidad de los datos la mejor opción seria SaaS ya que se podrá acceder a los datos desde cualquier lugar, sin embargo, esto representa un riesgo por parte de los usuarios con permisos otorgados a cambios ya que podrían modificar, hacer mal uso fuera del establecimiento o zona de trabajo.

Si el equipo cuneta con conocimiento de infraestructura se podría escoger IaaS ya que se cubrirían los puntos que no llega a cubrir esta infraestructura y se podría modificar, pero si no, la mejor opción será SaaS para tener todo seguro a la mano y solo preocuparse de su uso y dejar al proveedor a cargo del mantenimiento y la infraestructura del servicio. Al ser una entidad bancaria SaaS sería la mejor opción para evitar fallos en la infraestructura y tener siempre una alta disponibilidad.

4) A nivel de los sistemas que deberían proteger tu plataforma de Big Data:

- a) Debería estar segmentada de la red interna, junto con los sistemas transaccionales bancarios, o de lo contrario podría estar integrada dentro de alguna red interna.
    - Deberá estar segmentada, al segmentar la red tiene una mayor seguridad la plataforma de Big Data
- b) Pros y Contras de tenerla segmentada.
    - Al estar segmentada la red se tendré mayor seguridad porque los dispositivos que están conectados no están relacionados directamente con la red principal, de esta forma no se tendrá acceso a un todo de forma directa
    - Al tener la red segmentada la configuración de los sistemas con referente a la ip usada será más complicada, pues si se esta en una red trabajando con una ip y luego cambiamos a otra, esta se tendré que configurar para tener acceso a los datos de ella además de hacer el switch para no estar dejando puertas innecesarias abiertas.
- c) Si decidimos segmentarla, ¿crees necesario instalar un firewall? ¿Este sería un FW de red o de Aplicación (WAF)?

    - La instalación de firewall no debe de estar atada al si se segmenta o no la red, pues este siempre será un seguro mas para proteger los datos. La pregunta es un poco capciosa ya que el firewall de red siempre será útil, sin embargo, si se quiere proteger a nivel de seguridad la pagina o servicio de inyección sql ataques dos o ddos y manipulación de datos entonces WAF será la mejor opción.
- d) Si decidimos añadir un IPS (Intrusion Protection System), ¿Qué ganaríamos en seguridad?
    - Se ganaría el monitoreo de actividad con el fin de identificar comportamientos anormales dentro de la red

5) ¿Qué entiendes por Hardening de Servidores?

Aumentar la seguridad en cuestión de servidores, hacerlos más seguros o “Hardening”, es decir, disminuir las vulnerabilidades o su contra parte aumentar las medidas de seguridad dentro de ellos, analizando, identificando y solucionando los problemas.

6) ¿Cómo combatirías la fuga de datos de tu organización?

Implementando medidas de seguridad, así como encriptaciones y anonimizar de los datos, si bien, la fuga de los datos de la organización puede ser por empleados o directamente mediante ataques a los servidores como ordenadores, que esta información este codificada hará una barrera más para la obtención de información.

7) Imagínate que tienes que gestionar un incidente relacionado con una fuga de datos de la información ya procesada de utilidad para el negocio. Tu equipo de seguridad ha detectado un Command & Control (telecontrol de un sistema que un hacker realiza desde fuera de la empresa a través de Internet) y tienes el dilema de erradicar cuanto antes el problema para dar servicio cuanto antes o buscar evidencias Forensics, que te podría retrasar la puesta en servicio, para una posible denuncia, ¿Cuál sería tu decisión?

Como en el caso de la actividad en el foro lo primero que se debe de hacer es solucionar el problema y tapar/solucionar las vulnerabilidades que es lo principal, saber que se extrajo y a partir de que tiempo en caso de que se pueda o se tenga obtener esta información para saber qué tan grande ha sido la perdida de datos. Ya el ir y buscar evidencias forenses para proceder con la demanda creo que está en mi caso fuera de consideración ya que al ser una banca las noticias salen a la luz tarde o temprano, entonces si se llega a hacer publica la demanda se perdería seguridad ante los clientes y bajaría este nivel de aceptación en ellos, lo cual empezaría a dar malos márgenes o una mala reputación.

8) Imaginaros que la solución de Big Data es On-Premise (CPD de tu empresa). Respecto a las estrategias de Recuperación del Negocio del banco que vas a instaurar un Data Science para mejorar las ventas, teniendo en cuenta que el coste de la estrategia debe ser coherente con los datos a proteger, argumenta si utilizar un COLD, WARM, HOT SITE.

Si la es una gran cantidad de datos el Hot site será la mejor opción sin dudarlo, debido al tiempo de espera en recuperación de datos es solo de horas, si bien el tiempo de espera se puede extender de 24 a 48 hrs, es decir de uno a dos días el warm site será la opción eficiente para la restauración de datos, en especial porque estos pueden usar unidades de almacenamiento, lo cual si se requiere un dato en especifico antes de las 48 horas se podrá acceder a el dentro del almacenamiento, la tardanza en general esta ligada a que usa un cpu menos potente que la computadora principal.

9) Imagínate que tu Data Science lo tienes afinado y empieza a dar información que guía o enfoca las campañas de marketing a públicos objetivos ofreciéndoles productos que encajan a sus necesidades. Se filtra esta información a la competencia. En esta situación: ¿crees que tu empresa estaría más expuesta a un ataque APT (Amenaza Avanzada Persistente)? Argumenta la respuesta.

Sí, seria mas expuesta debido a que el factor humano, en este caso le data science, empieza a dar información sin que el mismo lo sepa, incluso el recopiladro

de datos o informante podría hacer un pretexting con el científico de datos , en otras palabras, con la ingeniería social se podría acercar al científico de datos y obtener información de él haciéndole una conversación para obtener datos. Lo anterior se logra gracias a la identificación de la víctima, investigación y observación de ella con el fin de saber como acercarse dando paso a la ejecución del plan para obtener la información.

10) ¿Por qué deberíamos anonimizar los datos de los clientes?

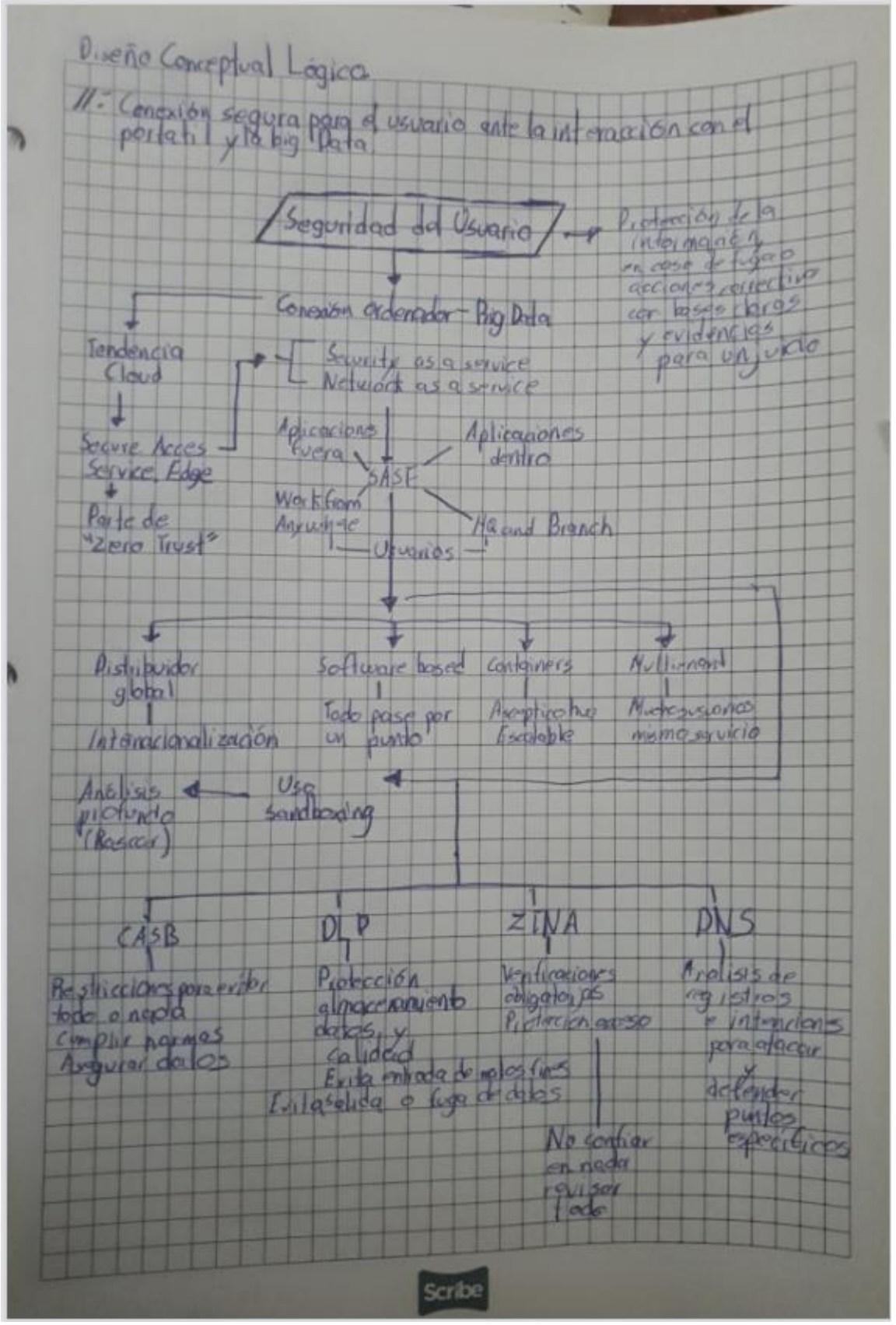
Para mitigar los riesgos, es decir, para que los datos de los clientes tengan cierta seguridad o privacidad en caso de una recopilación no autorizada de ellos, de esta manera no se podrá saber a detalle toda la información de los clientes, si se llega a conseguir algo será parcial. La privacidad de los datos privados recabados es esencial, ya que ellos podrían arrojar información para hacer un ataque directo y si se llegase a saber como obtuvieron dichos datos la imagen publica de la banca acabaría por los suelos, lo cual generaría perdidas indudables de clientes así como la seguridad de ellos.

11) Haz un diseño conceptual lógico con lo que has aprendido en la Clase 3 (SASE) para proteger al usuario y crear una conexión segura entre su portátil y el servicio BigData objeto del caso. Indica qué servicios SASE utilizarías y explica para qué.

–Parte Opcional–

Diseño Conceptual Lógica

II.- Conexión segura para el usuario ante la interacción con el portatil y la big Data.



Esta pregunta es opcional, para los que tengan cierto dominio de todos los conceptos adquiridos.

12) Imagínate una conexión remota desde tu dispositivo a un sistema Big Data en situado en Cloud IaaS: desde tu dispositivo, pasando por la red, el Cloud donde tienes el servicio albergado hasta llegar a la Aplicación en sí, enumera todos los elementos de seguridad que se te ocurrirían en cada una de las capas que hemos indicado.