SESIÓN ORDINARIA 821

Acta de la sesión ordinaria **OCHOCIENTOS VEINTIUNO** de la Junta Directiva de Popular Valores, Puesto de Bolsa, S. A., celebrada de manera virtual mediante la modalidad de videoconferencia, la cual se llevó a cabo en forma interactiva, simultánea e integral a las **DIECISÉIS HORAS CON SIETE MINUTOS DEL JUEVES VEINTIUNO DE MAYO DE DOS MIL VEINTISÉIS**. La convocatoria a la presente sesión se efectuó de conformidad con lo dispuesto en la ley. Asistentes: el presidente Sr. Raúl Espinoza Guido, la vicepresidenta Sra. Shirley González Mora, el secretario Sr. Álvaro Ramírez Sancho, la tesorera Sra. Kimberly Grace Campbell McCarthy, la vocal Sra. Silvia Morales Jiménez y el fiscal Sr. Steven Oreamuno Herra.

Asimismo, asistieron: la gerente general Sra. Mónica Ulate Murillo, el auditor interno Sr. Carlos Cortés Hernández, el subgerente general de Operaciones Sr. Daniel Mora Mora, el representante de la Dirección Corporativa de Riesgo Sr. Johan Rojas Fonseca y el director jurídico corporativo Sr. Ricardo Azofeifa Castillo.

ARTÍCULO 1

Inicia la sesión.

El presidente Sr. Espinoza Guido saluda a los participantes y les agradece la participación en esta sesión n.° 821 de la Junta Directiva de Popular Valores.

Acto seguido, comprueba el cuórum para la sesión.

Comprobado el cuórum, pasa al orden del día:

"1.- Aprobación del acta n.° 820.

2. - Asuntos de Presidencia

3.- Asuntos de Directores

4.- Asuntos Resolutivos

4.1.1.- La Sra. Mónica Ulate Murillo, gerente general, remite la capacitación titulada *AI y Ciberseguridad: Un enfoque actual.* Esta exposición se presenta como parte del Plan de Capacitación 2026 de la Junta Directiva de Popular Valores Puesto de Bolsa, S. A. (Ref.: oficio PVSA-282-2026).

4.3.-Asuntos de Auditoría.

4.3.2.- El Sr. Carlos Cortés Hernández, auditor interno, somete a consideración, la solicitud de vacaciones por un espacio 9 días, comprendidas del viernes 26 de junio al miércoles 8 de julio 2026 (Ref.: Oficio PVAI-057-2026)

4.4.- Asuntos de la Secretaría General.

4.5.- Correspondencia Resolutiva.

4.6.- Criterios Legales.

5.- Asamblea de Accionistas.

6.- Asuntos Informativos.

7.- Asuntos Varios."

El presidente Sr. Espinoza Guido pregunta si hay observaciones al orden del día.

La gerente general Sra. Ulate Murillo propone trasladar, como tercer tema resolutivo, el punto 4.2.1. dado que el administrador de proyectos Sr. Pablo Barrantes Rivera y el jefe de Tecnología de Información Sr. Castro Lee, también presentarán el estudio de factibilidad, que es el segundo punto resolutivo.

El presidente Sr. Espinoza Guido señala que el punto 4.2.1. se vería luego del 4.1.2., es decir, después del estudio de factibilidad.

Acto seguido, consulta si todos están de acuerdo.

Todos los directores manifiestan estar de acuerdo con la propuesta.

Al respecto, la Junta Directiva acuerda por unanimidad:

> **"Modificar el orden del día de esta sesión ordinaria n.° 821 de la Junta Directiva de Popular Valores Puesto de Bolsa S. A., y analizar el punto 4.2.1. como tercer tema en Asuntos Resolutivos".**
>
> **ACUERDO FIRME.**

ARTÍCULO 2

Aprobación el acta de la sesión n.° 820.

El presidente Sr. Espinoza Guido consulta por comentarios al acta n.° 820.

Acto seguido, pide la aprobación mencionada.

Todos los directores manifiestan estar de acuerdo con la propuesta.

Al respecto, la Junta Directiva acuerda por unanimidad:

> **"Aprobar, sin observaciones, el acta de la sesión n.° 820 de la Junta Directiva de Popular Valores Puesto de Bolsa, S. A., celebrada el 14 de mayo de 2026".**
>
> **ACUERDO FIRME.**

ARTÍCULO 3

Asuntos de Presidencia

El presidente Sr. Espinoza Guido recuerda la sesión de la próxima semana, es decir, del jueves 28 de mayo. Esta iniciará a las 4:00 p. m. de forma virtual.

ARTÍCULO 4

4.1.1.- La Sra. Mónica Ulate Murillo, gerente general, remite la capacitación titulada *AI y Ciberseguridad: Un enfoque actual.* Esta exposición se presenta como parte del Plan de Capacitación 2026 de la Junta Directiva de Popular Valores Puesto de Bolsa, S. A. (Ref.: oficio PVSA-282-2026).

Al ser las **dieciséis horas con trece minutos**, inician su participación virtual los representantes de la empresa Sofistic Cybersecurity Sr. José Navarro Hudson y Sra. Karina Roque. Asimismo, el encargado de Seguridad Informática Sr. Rolando Araya Martínez, el jefe de Tecnología de Información Sr. José Castro Lee, la Supervisora de la Auditoría Interna Sra. Leonor Cordero Fuentes y la auditora de Tecnología de Información Sra. Shirley Calvo Calderón.

El presidente Sr. Espinoza Guido saluda a todos los expositores e invitados a esta capacitación titulada *AI y Ciberseguridad: Un enfoque actual.*

Espera que esta presentación sea no solo un tema de actualidad para todos, sino que los haga reflexionar en aquellos aspectos donde la inteligencia artificial ha contribuido a las empresas, a las organizaciones y a las personas. No obstante, hace referencia también a los cuidados que deben tenerse y a los riesgos del mal uso.

Le cede la palabra al expositor y le da nuevamente la bienvenida.

El encargado de Seguridad Informática Sr. Araya Martínez introduce el tema y explica que buscan continuar con la concientización al personal de Popular Valores y, evidentemente, también a la Junta Directiva, para así tener todos una pincelada de lo que es la inteligencia artificial.

Sabe que este Órgano Director tiene ese *feedback* por otros canales, sin embargo, el compromiso es ir más allá y compartirles parte de los controles y del conocimiento que, por supuesto, ha avanzado desde que inició la IA.

En este caso les colaborará la empresa Sofistic, a través del Sr. José Navarro Hudson, quien es un experto en seguridad ciberseguridad e inteligencia artificial.

Aclara que cualquier consulta que se tenga, pueden hacerla para aclararla punto por punto. Al final, ser hará un resumen de cómo han abarcado el tema de la inteligencia artificial en Popular Valores.

El representante de la empresa Sofistic Cybersecurity Sr. Navarro Hudson saluda a todos los miembros presentes, expresa su alegría de estar aquí hoy, además, súper agradecido por la invitación. Se presenta, su nombre es José Navarro y forma parte de la compañía Sofistic Cybersecurity, empresa dedicada a aspectos de ciberseguridad.

En esta oportunidad hablarán sobre inteligencia artificial y ciberseguridad, un enfoque actual, la razón por la que presentarán este tema es por el gran impacto que tiene últimamente. Como todos bien saben, desde hace unos años se ha presentado una crecida exponencial en cuanto a la IA. Hoy forma parte del conjunto de instrumentos diarios, está en la caja de herramientas, independientemente a lo que se dediquen y está más que seguro que muchos de los aquí presentes utilizan la inteligencia artificial en su día a día.

Ahora bien, el uso de la IA, como tal, si no se hace de forma responsable, de la manera que debe ser, pues, al igual que cualquier otro proceso, conlleva muchos riesgos y sobre eso hablarán hoy.

Explicará cómo se combina la inteligencia artificial con la ciberseguridad, aquellos riesgos a los que todos pueden enfrentarse al utilizarla y cómo protegerse.

Hace hincapié en la definición de inteligencia artificial, reconoce que actualmente hay muchas definiciones y dependen mucho de los gustos de las personas y los matices en los que quieran enfocarla.

La inteligencia artificial, como tal, es una parte de la informática que se ocupa en diseñar sistemas informáticos inteligentes, es decir, sistemas que exhiben característica que se asocian con la inteligencia en el comportamiento humano.

La IA busca crear sistemas que se asemejen a cómo piensa un ser humano y, como es bien sabido, resulta muy complejo entender el pensamiento humano. Es muy difícil definir cómo piensa un humano, pero la IA busca, a través de algoritmos, de matemática y programación, simular cómo pensaría un ser humano y lo hace a través de procesos de comprensión del lenguaje y a través del aprendizaje.

Los modelos de inteligencia artificial, al igual que un ser humano, pasan por una fase de aprendizaje donde aprenderán de los datos que se le brinden. Cita como ejemplo, los modelos de inteligencia artificial, el ChatGPT y Copilot, entre otros muy comunes; estos tuvieron su fase de aprendizaje que, básicamente, se basó en Internet.

Especifica el hecho de leer artículos expuestos en Internet, aprendieron a programar a través de foros de programación y repositorios de código. Al igual que un ser humano, la inteligencia artificial también debe aprender y es muy importante que el aprendizaje que se le dé vaya de acuerdo con lo que buscan que este modelo de inteligencia artificial realice.

En cuanto a otras características del comportamiento humano que busca simular la inteligencia artificial, destaca el razonamiento, todos saben que el razonamiento humano es algo increíble, la inteligencia artificial busca simularlo, además, la resolución de problemas. Confirma que precisamente, la IA procura solucionar problemas; se utiliza día a día para solucionar problemas, responder alguna duda, buscar algo que no se sepa, por lo que es importante que, al momento de entrenar una inteligencia artificial, esta sea una de las características más importantes de la misma.

Detalla los usos de la inteligencia artificial que se le da actualmente y considera que los espacios más populares donde se ve la inteligencia artificial son los *chats* de inteligencia artificial, como puede ser ChatGPT, Copilot, DeepSig, Cloud y LLM (Modelo de Lenguaje Largo), este último es un tipo de inteligencia artificial que se hace de forma privada. La inteligencia artificial hoy es capaz, a través de *chatbots*, de resolver casi que cualquier problema que se presente.

Cita como ejemplo la posibilidad de pedirle, a través al algún *chat* de IA, que realice un código, que programe algo y la inteligencia artificial podrá hacerlo.

Menciona también temas relacionados con ciencia ficción y presenta, como ejemplo, la posibilidad de preguntar cuándo comenzarán los viajes interplanetarios. A esto, la Inteligencia artificial respondió: *es difícil predecir con certeza cuándo comenzarán los viajes interplanetarios de forma regular*.

Hace referencia a otras áreas como la matemática donde también es muy útil, en esta oportunidad se le pidió explicar el Teorema Fundamental del Cálculo, esto corresponde a matemática avanzada y la IA fue capaz de explicarlo.

Lo anterior demuestra que la inteligencia artificial es capaz de resolver casi cualquier tema y cita casos reales: la empresa Huawei develó cómo maximizar el valor de las redes 5G en la era de la inteligencia artificial. Además, Vodafone y Ericsson la utilizan para mejorar la eficiencia energética del 5G.

La IA se utiliza muchísimo para la investigación, para el desarrollo de nuevas tecnologías y esto evidencia que tiene muchas capacidades que, por supuesto, se usan de forma positiva, pero también de manera negativa.

Ahora bien, es importe entender qué es ciberseguridad, también se conoce como *seguridad digital* o *seguridad informática*, es la práctica de proteger la información digital, dispositivos, activos tecnológicos y los dato. La ciberseguridad se enfoca en la protección de infraestructura técnica y de la información contenida en los dispositivos o aquella que circula a través de la red.

La ciberseguridad comprende desde el *software,* como pueden ser bases de datos, archivos; el *hardware*, que es la parte tangible, una computadora, un dispositivo móvil. Además, las redes de computadoras y todo aquello que pueda considerarse como información.

Bien es sabido que los datos, en la mayoría de las veces, ya están de forma digital, se tienen bases de datos con mucha información sensitiva, números de cédulas, información bancaria y datos relacionados a los trabajos que cuestan mucho. Hay muchas personas afuera, muchos cibercriminales que no dudarían en comprar bases de datos expuestas. Confirma que estos datos son muy valiosos ya que corresponde a información que identifica a las personas.

La ciberseguridad busca proteger que los datos no puedan ser accedidos por otras personas. Al hablar de ciberseguridad, se mencionan tres pilares principales y se usa en acrónimo CIA. Cuando se habla de CIA, se utiliza para representar precisamente los tres pilares de ciberseguridad que son:

- ✓ Confidencialidad
- ✓ Integridad
- ✓ Accesibilidad

Especifica que la confidencialidad procura *mantener los secretos y garantizar que solo los usuarios autorizados puedan obtener acceso a sus archivos y cuentas*.

Por su parte, la integridad busca *garantizar que su información es la que debe ser y de que nadie ha insertado, modificado o eliminado cosas sin su permiso. Por ejemplo, cambiar de forma malintencionada un número en una hoja de cálculo.*

Aplica lo anterior al sector financiero, reconoce que cambiar un número significaría algo crítico. Se sabe que por un cálculo que no cuadre ya nada sirve y cada dólar, cada colón debe ser reportado a entidades financieras y si un solo número no encaja, pues es un problema muy grande y, por supuesto, en este espacio entra en juego la integridad.

Finalmente, el tercer pilar es la accesibilidad que pretende *garantizar que pueda tener acceso a su información y sistemas cuando lo necesite. Un ejemplo de un problema de acceso sería una denegación de servicio, donde los atacantes desbordan el sistema con tráfico de red para hacer que el acceso sea casi imposible; o ransomware que cifra el sistema e impide que se use.*

Bien es sabido que, en un sistema financiero, en un sistema bancario, el hecho de que un cliente no pueda acceder significa mucho dinero perdido y esto hace que la accesibilidad sea un pilar un importante.

Resume que la ciberseguridad busca proteger a estos tres pilares.

Pasa a la ciberseguridad mezclada con IA, a casos reales y presenta la siguiente imagen:

Explica que la imagen de un pingüino con la incripción *Dirty Frag* en su pecho se usa para representar una vulnerabilidad muy reciente que salió escasas dos o tres semanas y le permite a un atacante tener control total de un sistema al que tenía un acceso mínimo.

Esto quiere decir que, si un atacante lograba explotar esta vulnerabilidad en un sistema, automáticamente tenía privilegios máximos que le permitían modificar, eliminar, realizar lo que quisiera, comprometiendo los tres pilares vistos anteriormente, es decir, la confidencialidad, integridad y accesibilidad.

Precisamente esta vulnerabilidad fue descubierta utilizando inteligencia artificial, una persona tomó un sistema operativo, empezó a analizarlo utilizando la IA y descubrió una falla en el sistema. Al hallar esta falla, descubrió la forma de explotarla y confirmó que IA es bastante poderosa, mucho más poderosa, incluso, en sentidos que muchas personas no lo ven porque no están relacionadas con el tema y cita, precisamente, la seguridad informática.

La inteligencia artificial dentro de la ciberseguridad puede tomar dos bandos y posicionarse del lado rojo, pero también del lado azul, tal como se representa en la siguiente imagen:

Al habar del lado rojo y del lado azul en la ciberseguridad, se hace referencia al punto ofensivo o defensivo. El lado rojo simboliza a los atacantes, a aquellas personas que, de forma autorizada o no autorizada vulneran los sistemas. Aclara que hay atacantes autorizados a vulnerar los sistemas y este servidor es uno de ellos.

Explica que en su día a día se le autoriza a atacar los sistemas para buscar brechas de seguridad que un atacante podría transgredir y de esa forma remediar lo necesario para que una persona malintencionada no logre explotarlos. Siempre se representa del lado rojo aquellos atacantes, sean autorizados o no autorizados. Mientras que, del lado azul, están aquellas personas que defienden los datos de las personas.

La inteligencia artificial puede ser utilizada en ambos bandos. Del lado rojo, como atacante, para alguien que la utiliza de forma ofensiva y le sirve para encontrar nuevas vulnerabilidades o nuevos métodos; también para realizar otro tipo de ataques.

La IA también les ayuda a las personas que están del otro lado, defendiendo los sistemas ya que les permite entender qué está haciendo un atacante en tiempo real, cuál puede ser el siguiente movimiento. Se sabrá esto a partir de la información de ataques realizados previamente, podrá prever qué es lo más probable que haga el atacante; tendrán ese conocimiento utilizando inteligencia artificial.

En cuanto a lo que puede hacer la inteligencia artificial en la organización, pues puede aplicarse para muchos procesos, por ejemplo, como un asistente virtual para la Administración, que programe reuniones, envíe recordatorios o coordine las agendas de múltiples participantes. Esto permite optimizar el tiempo y la eficiencia porque ya no se necesita a una persona que se encargue de hacerlo, sino que puede tenerse un agente de inteligencia artificial o un asistente virtual que se ocupe.

Asimismo, permite automatizar tareas administrativas repetitivas, como la organización de los archivos, gestionar correos electrónicos, crear informes. Acota que muchas veces deben crearse informes diarios, semanales o mensuales y la inteligencia artificial puede ahorrarles muchísimo tiempo.

Destaca el área de Recursos Humanos donde también puede ser útil, podría filtra currículos, por ejemplo, puede mostrársele distintos currículos y pedirle que filtre a quienes tengan determinados requisitos y características idóneas para una persona que ocuparía ese puesto. La IA escogería únicamente la cantidad de currículos que se le pidieran y que pensaría son los mejores. Afirma que una IA es capaz de hacerlo; también es capaz de programar entrevistas, enviar correos electrónicos automatizados a los candidatos y así agilizar el proceso de contratación, por ejemplo.

Igualmente, puede ayudar a calcular y a procesar nóminas, asegurando que todos los empleados reciban sus pagos en los momentos que deben recibirlo. En temas de contabilidad, también puede ser útil, puede automatizar la conciliación de cuentas bancarias e identificar discrepancias. Como todos saben, si un decimal no cuadra, entonces hay que realizar todo de nuevo y con inteligencia artificial esto puede ser automatizado.

Destaca la generación de los informes, la AI se utiliza mucho para automatizar la creación y el envío de facturas a los clientes y para los seguimientos de los pagos.

El secretario Sr. Ramírez Sancho hace referencia a todo lo que puede realizar Copilot, pero consulta si al ofrecérsele información a esa herramienta, se la está haciendo pública o accesible, directa o indirectamente para otros usuarios de la inteligencia artificial.

El representante de la empresa Sofistic Cybersecurity Sr. Navarro Hudson señala que es una muy buena pregunta y le cede la palabra al encargado de Seguridad Informática Sr. Araya Martínez.

El encargado de Seguridad Informática Sr. Araya Martínez explica que, en este caso, al contar con una IA que es comercial y que está controlada, los usuarios tienen claro que no debe subirse información de clientes. Además, al ser una herramienta comercial, estas no utilizan el contenido para alimentar la misma inteligencia artificial, de modo que no es posible que utilicen sus datos.

Repite que el usuario sí tiene la conciencia, además, a nivel técnico se aplican los controles para que, a través de herramientas como DLP (*Data Lost Prevention*), no pueda subirse información a otra IA, inclusive, a la misma que se tiene en el entorno de Popular Valores y que se llama Tenant.

Añade que, si se subiera algo, pues la información está en manos de TI de Popular Valores, entonces, no es posible que la IA utilice información.

Hay otros escenarios donde esto sí es muy común y corresponde a espacios con herramientas de IA que son gratuitas.

Finaliza y confirma que no sería posible.

El representante de la empresa Sofistic Cybersecurity Sr. Navarro Hudson añade que, en múltiples ocasiones, las organizaciones contratan servicios que utilizan inteligencia artificial, *chats* de inteligencia artificial, como puede ser Copilot. En este caso, al ser un servicio contratado, que paga la empresa, se aseguran de que los datos que se ingresen a la misma se mantengan ahí y no sean utilizados para fines de entrenamiento, tampoco se vayan a los servidores de los proveedores.

Sin embargo, al utilizar las capas gratuitas de muchas de estas herramientas, estas sí se usan para entrenamiento, por lo que siempre es importante poseer las herramientas de inteligencia artificial previamente autorizadas y que sean controladas por la organización.

Otro ejemplo de lo que la IA puede hacer por una organización gira en torno al desarrollo de negocios; al tener los datos de mercado es posible recopilar y analizar esta información, utilizar la inteligencia artificial para generar informes, nuevas recomendaciones y buscar nuevas oportunidades de negocio.

Ahora bien, cómo pasa la IA de aliado a enemigo, cuáles son los principales riesgos que se tiene y asegura que el mal uso de esta herramienta también puede comprometer la operativa de una empresa, precisa el nivel de *compliance*, por la fuga de información. Esta fuga de información puede ser el punto de partida de un ataque cibernético muy complejo.

Prosigue con los principales riesgos a los que se enfrentan con el uso de la inteligencia artificial; uno: la exposición de los datos confidenciales. Sin una configuración adecuada, aunque una inteligencia artificial paga, hasta cierto punto, permite omitir este punto. No obstante, si se utiliza la capa gratuita de un modelo de inteligencia artificial o no se configura adecuadamente, esta puede exponer datos sensibles y esta exposición permite accesos no autorizados.

Por lo anterior, es muy importante que se implementen las políticas de seguridad, políticas de DLP (*Data Loss Prevention*) y la gobernanza de los datos para que se proteja la información confidencial dentro de la organización.

Destaca también el rendimiento inconsistente, la falta de preparación puede ser un rendimiento inconsistente de la IA que puede afectar la productividad y la experiencia del usuario.

También las interrupciones en el trabajo y ocurre con las personas ya están muy acostumbradas a utilizar la IA; añade que si, por determinado motivo, el servicio no está funcionando debido a su mantenimiento, porque hay algún problema a nivel macro que no permita que el sistema funcione o, simplemente, porque hay una gran cantidad de personas que utilizan este servicio y no puede funcionar el modelo de inteligencia artificial, pues muchas personas ya no podrán trabajar sin esta, lo cual lleva una interrupción del trabajo.

Comenta también los aspectos de cumplimientos y regulaciones; si esto no se configura de forma adecuada puede infringir regulaciones y políticas de cumplimientos. Detalla también el daño reputacional que también es muy importante; si no se controlan los *prompts*, es decir, las peticiones, las consultas que se le hace a un modelo de inteligencia artificial, los usuarios incluso podrían utilizar el resultado que le da la inteligencia artificial para generar contenido falso, incluso, contenidos sesgados.

Y, por último, se refiere al uso de los datos para el entrenamiento, es muy importante validar que los datos que estén dándoseles a los modelos de inteligencia artificial se utilicen para entrenar la misma inteligencia artificial. También debe considerarse el periodo de almacenamiento, la ubicación de los datos y, en este caso, como se usa un modelo de pago, controlado por la organización y señala que no hay que tenerle tanto miedo de esto.

Reconoce que siempre es importante el cuidado al utilizar agentes de inteligencia artificial en su capa gratuita. Hace referencia al ChatGPT, la primera vez que un usuario los usa, el ChatGPT le dice que es una muestra gratis e informa que las conversaciones pueden ser utilizadas por los entrenadores de la IA para mejorar los sistemas. En este caso no debe compartirse información sensible en la conversación.

Precisa que, en muchas oportunidades, simplemente quiere probarse la herramienta sin leer los términos, las condiciones y se ignora totalmente esa información. Explica que la organización creadora de ChatGPT está cumpliendo porque, efectivamente, está avisando que no debería subirse ninguna información sensible ya que la conversación puede ser revisada por un entrenador de inteligencia artificial. El hecho es que las personas no siempre leen ese tipo de datos.

Pasa a otro peligro que puede involucrar la IA y son los ataques de ingeniería social. Este es un tipo de ataque informático donde los cibercriminales buscan ganarse la confianza de las víctimas y que esta simplemente ofrezca o dé la información porque confían exactamente en lo que hace el atacante.

Confiesa que la IA ha ayudado mucho a la ingeniería social y a los ataque derivados de esta, cita los *emails* que les llegan y a través de los cuales quieren robarles las credenciales. Menciona, como ejemplo, un correo donde se señala que la cuenta de Netflix ha sido bloqueada, debe incorporarse el usuario y la contraseña para poder acceder.

Un segundo ejemplo es un correo corporativo se sería cerrado por falta de uso y debe ponerse el usuario y la contraseña para recuperarlo. Confiesa que la IA ya ha hecho que estos ataques no sean para nada básicos y ahora se utilizan para muchos ataques a nivel macro como los correos de *phishing*.

Aprovecha para aclarar que el *phishing* es una técnica de ingeniería social donde el atacante envía correos electrónicos a la víctima con el objetivo de que esta última realice alguna acción sobre este correo electrónico. Recuerda que, en el pasado, cuando se realizaban estos ataques, era muy fácil detectarlo porque el logo de la empresa que simulaban ser, pues no era exactamente el logo de esa compañía. Además, el lenguaje utilizado era creado por una persona que no sabía español y los ataques se detectaban fácilmente.

No obstante, hoy en día, con el uso de la IA, es muy fácil crear un correo electrónico que se vea realista, que dé la sensación de que, efectivamente, está ocurriendo algo sobre la cuenta de la persona y que esta debe ingresar su correo y su contraseña para evitar que algo malo suceda.

Destaca también el *smishing* que es una técnica de ingeniería social que busca engañar a la víctima, pero en este caso, en vez de correo electrónico, utilizan mensajes de texto, mensajes SMS, incluso, mensajes por WhatsApp que incitan a un receptor a llamar a un teléfono de contacto falso, incluso, acceder a un sitio *web* falso, muy similar al *phishing*.

Con ayuda de inteligencia artificial, el *smishing* se dispara muy similar al *phishing*, pues los mensajes ya irán bien redactados, de forma que podría creerse que, en realidad, se habla con alguien legítimo.

Explica también el *vishing* que es un ataque de ingeniería social donde la víctima llama a las personas por teléfono, habla con la persona y se hace pasar por otra persona. Le dicen a la víctima que son su hermano, su hijo o su pariente. Al principio, antes del *boom* de la inteligencia

artificial, era mucho más fácil detectarlo, porque las personas sabían cómo habla el pariente, su acento y se percibía que su tono de voz habitual.

En estos momentos, existen modelos de inteligencia artificial que se dedican únicamente a crear audios, utilizando texto, es decir, se le escribe a la inteligencia artificial lo que se quiere decirse, pero que lo diga con una voz que se le dé. Los atacantes toman un audio grabado con determinada voz, lo graban en un audio, lo pasan por un modelo de inteligencia artificial y le piden que diga lo que ellos requieren.

Cuando la víctima escucha ese audio, aye que la voz suena natural, suena con el acento de esa persona, con el tono de voz que habla esa persona y caen fácilmente. Esto se da con ayuda de la IA, luego la víctima se da cuenta de que no es la persona que decía ser y que, simplemente, utilizaron la voz para perpetuar el ataque.

Lo mismo ocurre con el QRShing, el ataque utiliza los códigos QR falsos que redirige a los usuarios hasta sitios *web* falsos para que se registren o ingresen a algún tipo de datos sensible.

El encargado de Seguridad Informática Sr. Araya Martínez comenta que, en este momento, muchos ven este tipo de ataques como muy remotos. Sin embargo, muchas veces sí llegan un mensaje de alguno de los contactos que se tienen, inclusive, puede ser un audio donde la IA puede replicar el tono de voz de alguien con solo haberlo escuchado por un minuto.

Lo ideal es que para estos casos pueda complementarse, con otro tipo de canal, una validación de lo que se solicita a nivel profesional. La idea es hacer una llamada, mandar un correo, un mensaje por Team, WhatsApp o una llamada telefónica. Reconoce que eso puede ponerlos un poco paranoicos en algunos casos, sin embargo, es importante validar o hacer un doble *check* por otro canal, por otro medio y confirmar esa información.

Lo anterior ya es una realidad, ya existen casos de ataques simulados por la IA donde personifican una acción y una solicitud. Evidentemente, ya se tiene un doble factor para la autenticación a una red donde porque no pueden fiarse de un usuario y contraseña y deben utilizar un código que cambia cada cierto tiempo.

De igual manera, habrá casos donde cada persona deba aprender a valorar si ese comportamiento no tan frecuente o esa solicitud inusual deba validarse por otro medio para realizar lo que se les solicita.

El representante de la empresa Sofistic Cybersecurity Sr. Navarro Hudson estima que estos ataques podrían parecer remotos, pero verdaderamente todos los días hay personas que realiza ataques, porque, como lo mencionó al principio de la presentación, los datos son muy valiosos. Los atacantes buscan robar datos, la información es muy valiosa y harán todo lo que sea necesario para conseguirla.

Por lo anterior, es muy importante tener otros mecanismos para comunicarse con otras personas en cuanto se recibe, por ejemplo, un correo falso o una llamada. Ante esta situación, puede validarse por otro lado y así asegurarse de que, en realidad, sea la persona quien dice ser; esto antes de realizar cualquier acción.

Reitera que los ciberdelincuentes usan la IA y precisa que pueden perfectamente crear rostros de personas que no existen realmente. Asegura que los cibercriminales utilizan muchísimo la inteligencia artificial para generar identidades falsas porque muchas veces necesitan una identidad para realizar alguna acción, por ejemplo, crear una cuenta en una red social o, por ejemplo, en LinkedIn, que es una red social profesional y la utilizan muchísimo para conseguir datos.

Avisa que para esto se necesita tener una foto real, una cara real y utilizan la IA, precisamente para generar rostros. Las imágenes son realistas y trae a colación la aplicación FaceApp que utilizaban las personas para tomarse una foto y ver cómo se verían en distintas edades.

Destaca también aquellas aplicaciones para crear emojis, animes a partir de una foto real. Asegura que las personas, en realidad no se daban cuenta que estaban regalando sus datos preciados, su biometría, sus caras al utilizar aplicaciones; tampoco sabían qué se hacían con esas imágenes.

Afirma que las imágenes de persona son tan realistas porque aplican algoritmos para aprender cómo es un rostro humano, cómo se ve una cara real y a partir de la cantidad de rostros que poseen, pues les es mucho más fácil a los modelos de inteligencia artificial generar rostros que se vean realistas.

Pasa a algunos ejemplos de la noticia, confirma que existen muchísimos y cita una nota que dice que en México, Colombia y Argentina durante el 2020 han aumentado en un 67% las estafas bancarias con ayuda de robot telefónicos. Dice rápidamente que el 2020 es anterior el gran conocimiento de la inteligencia artificial.

Observa otra nota sobre el último ataque de *ransomware* en España. Aclara que *ransomware* es un tipo de *malware* que busca cifrar, encriptar la información que se tiene para después cobrar. Es decir, secuestran la información y confirma que los últimos ataques de *ransomware* en España ya manejan IA.

Nota otra noticia que confirma que utilizaron inteligencia artificial para imitar la voz de un CEO y robar $240.000.

Observa otro artículo donde se cita que un directivo de Binance (una empresa de criptomonedas) aseguró que han creado un *deepfake* de él para perpetrar estafas en la plataforma y usan su imagen en entrevista. Un *deepfake* es básicamente cuando toman la imagen de una persona, un audio o un video de esa persona y lo modifican con IA para que parezca que está haciendo o diciendo algo.

Prosigue con otra nota, esta vez relacionada con *Deep Voice*, se precisa la tecnología que falsifica la voz y con la que se han robado $35.000.000. Reconoce que es cada vez más frecuente el uso de *deepfaker* en entrevistas de trabajos remotos y el objetivo es acceder a datos confidenciales.

De hecho, hace algunos meses en Colombia se encontró a una persona que estaba haciendo *deepfake* y usaba *deep voice*, es decir, voces y caras falsas para realizar una entrevista de trabajo para una compañía en ese país. Cuando se realizó la investigación, se descubrió que, en realidad, era un cibercriminal de Corea del Norte y quería ingresar a Colombia, a una compañía colombiana, para tener acceso a datos confidenciales.

Asegura que la inteligencia artificial no es buena ni mala por sí sola; es una herramienta poderosa y depende de quién la use y cómo se configure. Entonces, se pregunta cuáles son los riesgos de la exposición a Internet y aclara que, al exponerse a Internet, al conectarse y compartir en línea, pues todos se arriesgan a la exposición de la información personal, es decir, los nombres, las ubicaciones y los gustos.

Hace referencia al entrenamiento de la inteligencia artificial sin el consentimiento y reitera que las fotos de las personas pueden ser utilizadas para alimentar algunos modelos sin que se sepa.

Retoma el robo de la identidad digital, la suplantación en redes sociales o en las aplicaciones. Además, utilizan a las personas para perfilarlas, realizar estafas en línea y hacer campañas de *phishing* con los datos de esas personas. Lo utilizan mucho para la falsificación de las voz, rostros o personalidades a través del *deepfake* y *scams* por IA, es decir, estafas a través de inteligencia artificial.

También es importante la exposición de los datos, es relevante no dar datos confidenciales y esto sucedió en Samsung, una empresa muy importante, muy grande. Reporta que sus ingenieros utilizaron ChatGPT al principio cuando estaba saliendo y accidentalmente filtraron datos confidenciales. Por esto, Samsung les prohibió a sus empleados utilizar ChatGPT y así evitar que se filtre información confidencial.

Esto sucede, como puede verse, desde las empresas más pequeñas hasta las más grandes donde, accidentalmente, se filtraron los datos. Sugiere tener mucho cuidado con los agentes de inteligencia artificial, especifica los *chatbots* ya que estos pueden ser manipulables.

No hay que creer todo lo que dice un *chatbot* y trae a colación uno usado en la atención de clientes de un supermercado de España al que una persona simplemente manipuló y le dijo que programara algo. Aclara que el *chatbot* no está diseñado para programar, no tiene nada que ver con informática, no es programador. No obstante, una persona le dijo que escribiera un programa en Python, que es un lenguaje de programación que sirve para calcular dos cifras. Al hacer esto manipuló la inteligencia artificial y esta le dio todo el código de ese programa.

Por consiguiente, debe tenerse mucho cuidado y no creer todo lo que dice una IA, porque esta también puede ser susceptible a ataques cibernéticos y puede ser manipulables.

Pasa a las conclusiones, hace hincapié en las buenas prácticas en seguridad, es muy importante ser el primer eslabón de seguridad, los seres humanos son el más importante y, a su vez, el eslabón más débil en la cadena a la ciberseguridad.

Primeramente, debe evitarse compartir información sensible en *chatbots* de IA, en correos o en plataformas no corporativas. Realmente no se sabe qué datos están dándose, al final, ni tan siquiera es posible darse cuenta de que se comparten datos y dónde van a parar.

También deben verificarse los términos y condiciones de uso antes de entrar a utilizar alguna aplicación de moda o alguna inteligencia artificial gratuita. Como lo mencionó, estas aplicaciones están obligadas a siempre decirle al usuario qué es lo que harán con sus datos, cómo entrenarán otros modelos, utilizando los datos de las personas. Si no lo hacen, están incurriendo en un delito.

El tema es que muchas veces las personas son perezosas, no se sientan a leer detalladamente los términos y las condiciones de las aplicaciones, tampoco se dan cuenta de que los datos serán utilizados para entrenar a otros modelos. Incluso, tan siquiera se sabe para qué serán utilizados.

Recomienda desconfiar de los enlaces desconocidos y no esperados. Si se recibe un enlace a través de correo electrónico y es algo que no estaba esperándose, lo más probable es que sea un ataque cibernético.

Finalmente, desea decirles que la seguridad informática no se logra el día que se escribe una norma, sino cada vez que un colaborador decide seguir rigurosamente el protocolo.

Agradece la atención, espera que esta presentación haya sido del agrado de quienes la escucharon y queda atento para responder cualquier consulta que se tenga.

El fiscal Sr. Oreamuno Herra agradece la presentación y precisa que desde el momento en el que se sube una imagen o cualquier información a una red social, pues ya no es para la persona que la subió y pasa a estar en toda la red.

Aprecia que la mayoría de la IA es generativa, sale a partir de información, hace comparaciones, incluso, hay Inteligencia artificial que humaniza lo que hace determinada persona y consulta si han tenido experiencia en cómo detectarla.

Precisa brevemente que también hay inteligencia artificial para detectar esa humanización.

Pregunta si han tenido experiencia en alguna institución, saben de alguien o alguna organización que ayude, por supuesto, teniendo claro que el primer eslabón es la persona.

Asegura que ahora es difícil detectar una inteligencia artificial y repite sí han tenido experiencia con organizaciones que también tengan inteligencia artificial para detectar eso y para ayudar.

El representante de la empresa Sofistic Cybersecurity Sr. Navarro Hudson confiesa desconocer si hay alguna organización como tal que funcione para realizar esto, pero sí sabe que en las universidades utilizan distintos *software* para validar. En realidad, la inteligencia artificial puede avanzar mucho, pero sigue siendo fácil identificar un texto cuando es escrito con inteligencia artificial.

Especifica que repite mucho las palabras, reitera algunas palabras una y otra vez, así pueden darse cuenta de que fue una inteligencia artificial quien generó el texto. Por ejemplo, al hablar de ciberseguridad, notarían que se repite alguna palabra clave y que no debería repetirse tanto.

El subgerente general de Operaciones Sr. Mora Mora agradece la información e informa que, en Costa Rica, el 29 de abril entró en vigor una ley que obliga a los bancos a indemnizar a los clientes en el caso de que se genere una estafa, una transferencia no autorizada o una sustracción de fondos de clientes.

Esta legislación obliga al Banco a indemnizar a los clientes y la carga de la prueba ya no es del cliente, sino del Banco.

Consulta si el expositor conoce de algún país que aplique este tipo de leyes y cuál ha sido el efecto. Pregunta lo anterior porque por que se crea una zona de vulnerabilidad precisamente por la inteligencia artificial y la cibercriminalidad que existe en este sentido.

En cuanto a lo que se ha podido hacer, pues es muy poco, el Banco ha comenzado a resolver reclamos que creen no son justos, pero la ley los obliga a pagar y luego ir a los tribunales para demostrar que la institución tenía los controles suficientes y que la persona se prestó a hacer negocios no adecuados.

El representante de la empresa Sofistic Cybersecurity Sr. Navarro Hudson confiesa no conocer, dice que al menos en Panamá, donde está ubicado, pues no funciona así y desconoce sobre algún otro país donde sea así, es decir, donde el banco deba indemnizar a las personas.

No obstante, sí puede decir que la evidencia digital prevalece y puede resolver casi cualquier dilema relacionado con si la persona se prestó o no. Esto puede hacerse a partir de los registros y precisa que todas las aplicaciones, especialmente en el sector financiero, ya cuentan con un registro sobre todas las acciones que realice un usuario. Es decir, desde que inició sesión, ya automáticamente registró dónde se inició la sesión, a qué hora fue, por cuánto tiempo estuvo en la sesión. Todos estos datos pueden ser utilizados para realizar un análisis forense y determinar si la persona se prestó para eso o si ocurrió en algún fraude interno o algo similar.

La evidencia digital es muy poderosa, muchas veces se subestima lo mucho que puede ayudar y apoyar.

Reitera que desconoce sobre algún otro país que aplique esta ley, por lo que también desconoce los efectos que haya tenido esta legislación, pero sí puede recomendar tener la evidencia digital de todo lo que se realiza.

El secretario Sr. Ramírez Sancho piensa en los aplicativos de la IA para Popular Valores y cuenta haber visto algunos ejemplos de personas que utilizan algoritmos para tomas de decisiones de inversión. Lo ha visto principalmente en *stocks* y en acciones, no así en títulos de deuda o similares.

No deja de ser interesante porque, de alguna manera, ayuda, aunque no sustituye el análisis técnico tradicional de las inversiones.

Además, puede resultar con mucho potencial en las áreas de riesgo precisamente para el análisis de riesgo, donde sí ha visto un aplicativo específico.

Ahora bien, con la información recibida en esta capacitación y en otras, pues lo visualiza funcionando para una organización como esta en esos temas, precisamente.

El representante de la empresa Sofistic Cybersecurity Sr. Navarro Hudson comenta sobre las personas que utilizan los datos para la toma de decisiones financieras en las bolsas de valores y precisa que, a fin de cuentas, la IA es un algoritmo, es un proceso matemático que simplemente compara millones de datos y eso le permite tomar decisiones.

Estima que este tipo de toma de decisiones puede ser arriesgada, conlleva un gran riesgo porque no saben, no puede predecirse el futuro y mucho menos lo logrará la IA. Sugiere ser muy cuidadosos al implementar este tipo de aplicativos.

En cuanto al análisis de riesgo, pues sí se utiliza la IA para realizar análisis de riesgo, existen aplicativos y muchas personas también crean aplicativos propios basados en inteligencia artificial para realizar análisis y tomar decisiones basadas en IA.

El secretario Sr. Ramírez Sancho dice que no deberían extrañarse que en un tiempo los clientes, además de la recomendación de los corredores y su análisis técnico, les pidan insumos adicionales informáticos de cómo se llegó a esa recomendación de compra o de venta de un título.

No ve tan lejano que sea un *must have,* algo que debería tenerse para ofrecerlo en el servicio de esta Sociedad.

La tesorera Sra. Campbell McCarthy le consulta al equipo de Popular Valores sobre cuáles son los procesos actuales disponibles en Popular Valores que usan ya la IA.

El jefe de Tecnología de Información Sr. Castro Lee responde que dentro del Área de TI se hacen implementaciones de motores de inteligencia artificial internos, que no tengan salida a Internet, para cuestiones meramente de TI. Después podrían implementar la parte de código y la revisión de ese código.

Reporta que están en la fase de pruebas que les ayuden, por ejemplo, a resolver problemas fácilmente y mejorar la atención de las necesidades del negocio.

El encargado de Seguridad Informática Sr. Araya Martínez regresa a los conceptos del *Red Team* y del *Blue Team*, que corresponden básicamente a los equipos de ataque y los equipos de defensa y representan la dualidad existente en el área de la ciberseguridad. Lo mismo sucede con la inteligencia artificial, es decir, las herramientas que vienen a sustituir o mejorar las soluciones relacionadas con ciberseguridad, detectan el ataque generado por la propia IA.

Así como los atacantes utilizan la IA para perpetuar sus ataques, las soluciones o los proveedores están poniéndose en línea para identificar los ataques que vienen de la inteligencia artificial.

Es un trabajo constante, es y seguirá incorporado en las mejoras de todas las soluciones y así como los atacantes utilizan la IA, también las soluciones que adquiere Popular Valores y los procesos realizados vienen para detectar estos ataques.

Reporta que se está en la parte de pruebas, hay dos ambientes, especifica a la IA en la nube; informa que se trabaja desde la definición de directrices, políticas y controles para evitar que los colaboradores puedan subir información confidencial a otras IA. Desde el año pasado se tiene un acompañamiento, no solo técnico, también de concientización para evitar que prevalezca solo el control técnico y que todos los usuarios estén conscientes que podrían comprometer datos sensibles de la organización.

Afirma, para finalizar, que hacen pruebas con inteligencia artificial, pero a nivel local, de manera que no se exponga la información.

La vocal Sra. Morales Jiménez comenta que todo tiene todo tiene una parte buena y una parte mala y la aplicación de la inteligencia artificial en los temas del negocios no está exenta de eso. Le parece que es muy importante, la información que se le brinde al cliente; esta, quizás,

siempre va atrás a los nuevos métodos utilizados por los criminales cibernéticos y destaca el hackeo de cuentas, el traslado de fondos y este tipo de situaciones que se vuelve relevante.

Repasa que hasta este momento han visto más la aplicación de estafas a nivel personal, desde temas bancarios y asociado a cuentas bancarias, más no en negocios bursátiles. Desconoce si ya hay algún antecedente en ese tema.

El auditor interno Sr. Cortés Hernández informa, desde esta Auditoría Interna que, a partir de finales del año pasado, se le da seguimiento y asesoría a la Administración en cuanto al uso y a las políticas en materia de inteligencia artificial.

Cree que la más apropiada para darle mayor amplitud al tema, sería la auditora de Tecnología de Información, la Sra. Shirley Calvo.

La auditora de Tecnología de Información Sra. Calvo Calderón confirma que, desde el año pasado, esta Auditoría Interna, a partir de estudios realizados sobre seguridad de la información, tenía la incertidumbre de qué estaba haciendo este Puesto de Bolsa y el Banco Popular en relación con la inteligencia artificial. De ahí nacieron algunas recomendaciones que brindaron sobre este tema.

Hace énfasis en que la IA ya está entre todos y precisa que se brindaron algunas recomendaciones para implementar y definir cuáles eran las políticas o las directrices que tendrían y así lo ha hecho la Administración. Confirma que esta se ha encaminado en definir las políticas y buscar una estrategia implementación.

La inteligencia artificial es un tema muy amplio, pero cada empresa u organización debe definir en dónde se aplicará porque ese sería el verdadero valor de la inteligencia artificial. Anota que, si no se tiene un gobierno de inteligencia artificial, pueden crearse iniciativas aisladas y no verán resultados.

A partir de la definición de la directriz de Popular Valores y basados en las propuestas del Banco Popular, decidieron que, inicialmente, adquirían licencias de Copilot.

Recuerda que Copilot está integrado a la plataforma de Office de Microsoft y, por tanto, era mucho más sencillo adquirir la licencia y contar con un ambiente controlado para el uso de esa plataforma.

Además, no solo se ha capacitado al personal de la Auditoría Interna, sino a otras áreas, específicamente en cómo Copilot puede ayudar como un coagente o como un *co-worker* para ser más eficientes en el trabajo.

Por ejemplo, en la Auditoría Interna ya han realizado algunas pruebas, recibieron capacitaciones y han utilizado la plataforma para consultar de forma más rápida y sencilla sobre normativa, políticas, incluso, para el análisis de los estados financieros y comenta que una tarea que requería varias horas ahora puede realizarse en mucho menos tiempo.

Así, un auditor, quien debe realizar alrededor de cinco informes al año, ahora tendrá la oportunidad de elaborar siete u ocho informes, según la implementación de esas herramientas.

Comenta que en un estudio podían tardar más tiempo y ahora están minimizando los periodos, además, están ofreciendo resultados más amplios.

Añade que han tenido reuniones con el Área de Tecnología de Información para tener un agente Copitot de estudio más automatizado y así lograr notificaciones en tiempo real del sistema de legitimación de capitales.

Reporta que están trabajando en algunas iniciativas, que posiblemente más adelante las compartirán, y tendrán algún apoyo que podría ser interno o externo de Tecnología de Información para incorporar la inteligencia artificial en las tareas diarias que realizan y cómo darles seguimiento a incidentes de seguridad, incidentes de la estructura tecnológica o de legitimación de capitales cuando se presenta una transacción que no está dentro de los lineamientos establecidos.

Están avanzando en la elaboración de los lineamientos, según las directrices que la Administración les va brindando y asegura que el objetivo es ofrecer un acompañamiento y una asesoría conforme obtengan esa estrategia de inteligencia artificial.

El presidente Sr. Espinoza Guido agradece la exposición y los comentarios y le pide al Sr. Jose Navarro exponer su reflexión final.

El representante de la empresa Sofistic Cybersecurity Sr. Navarro Hudson manifiesta que la inteligencia artificial no es un insumo ni bueno ni malo, siempre dependerá del uso que se le dé y si el uso es correcto, puede ser una herramienta muy buena para automatizar procesos y eso, incluso, permitirá ahorrar mucho tiempo y dinero.

Aconseja que cuando utilicen inteligencia artificial licenciada, como el caso del Copilot, no introduzcan datos de clientes o, al menos, datos identificables de clientes. Recomienda anonimizar los datos de los clientes antes de subirlos.

Explica que anonimizar es asignarle un nombre ficticio y que solo algunos sepan a qué se hace referencia. Por ejemplo, llamar a un cliente Júpiter, es decir, con el nombre de un planeta y si algo llega a suceder y la información se filtra, solo se nombró a Júpiter, un nombre que no identifica a alguna persona y así nadie sabría realmente de quién se está hablando.

Espera que la capacitación les haya sido de mucho provecho y haya sido de su agrado.

El presidente Sr. Espinoza Guido agradece la presentación del Sr. José Navarro Hudson y a la empresa Sofistic Cybersecurity por haber colaborado con este proceso de capacitación para la Junta Directiva.

Se despide de los expositores y de los invitados a esta capacitación.

Al ser las **diecisiete horas con quince minutos**, finalizan su participación virtual el Sr. José Navarro Hudson y la Sra. Karina Roque, representantes de la empresa Sofistic Cybersecurity. De igual manera, se retira el encargado de Seguridad Informática Sr. Rolando Araya Martínez.

Acto seguido, se plantea el acuerdo:

Dar por recibida la capacitación titulada AI y Ciberseguridad: Un enfoque actual, expuesta por el representante de la empresa Sofistic Cybersecurity Sr. José Alberto Navarro Hudson.

Esta exposición se presenta como parte del Plan de Capacitación 2026 de la Junta Directiva de Popular Valores Puesto de Bolsa, S. A.

Todos los directores manifiestan estar de acuerdo con la propuesta.

Al respecto, la Junta Directiva acuerda por unanimidad:

> **"Dar por recibida la capacitación titulada *AI y Ciberseguridad: Un enfoque actual,* expuesta por el representante de la empresa Sofistic Cybersecurity Sr. José Alberto Navarro Hudson.**
>
> **Esta exposición se presenta como parte del Plan de Capacitación 2026 de la Junta Directiva de Popular Valores Puesto de Bolsa, S. A.".**
> (Ref.: oficio PVSA-282-2026)
>
> **ACUERDO FIRME.**

La tesorera Sra. Campbell McCarthy pregunta si la adopción de este tipo de iniciativas de inteligencia artificial se está *trackeando* de alguna forma, es decir, conocerán avances en algunos de los informes que reciben. De lo contrario, sí le gustaría que puedan tomar un acuerdo para darle seguimiento cada cuatrimestre o cada semestre y de ese modo conocer el avance de la adopción de esas herramientas. Considera que constituyen un elemento de ventaja competitiva para el ahorro de tiempos.

El presidente Sr. Espinoza Guido propone dar un poco más de vuelta a la petición y solicitarle a la Administración y a la Auditoría Interna la elaboración de un inventario de los programas que están utilizando la inteligencia artificial y pedirle a la Administración que presente si hay alguna iniciativa conglomeral que esté unificando estas herramientas como política.

Recalca que es un banco público y tiene sus características en términos reglamentarios.

La tesorera Sra. Campbell McCarthy menciona que está de acuerdo, pues de ese modo pueden conocer el punto de partida y así definir cuáles aspectos se han aprobado, a cuál política responde y hasta dónde podían avanzar. El fin es tener una visión más amplia y cree que los miembros de la Junta Directiva Nacional posiblemente conozcan más datos y por eso le gustaría saber qué hay al respecto y qué deben impulsar en esta Sociedad.

Al estar en el marco de todo un Conglomerado deben fundamentarse en las directrices conglomerales e insiste en recibir más información para conocer el avance del tema.

La vicepresidenta Sra. González Mora considera muy interesante la observación de la Sra. Kimberly Campbell McCarthy y añade que por ser un tema conglomeral, deben exponerlo primero en el Comité Corporativo de Tecnología de Información y luego subirlo a la Junta Directiva Nacional para que gire instrucciones, ya que el uso de las herramientas debe ser autorizado a nivel conglomeral.

Aclara que ese proceso no impide que las sociedades avancen con análisis y otras acciones, pero si hubiese una política conglomeral y ese es el objetivo, deben seguir todas las etapas de manera ordenada. Enfatiza en que esa es la forma correcta de abordar este tema.

El auditor interno Sr. Cortés Hernández coincide con la vicepresidenta Sra. Shirley González Mora e indica que desde la Auditoría Interna están preparando un documento de asesoría dirigido a la Administración de Popular Valores y a la Junta Directiva sobre esta temática.

Adicionalmente, recuerda que ya hay un acuerdo basado en la recomendación de la Auditoría Externa.

En cuanto al proceso de auditoría continua, recalca que están trabajando en un proyecto de inteligencia artificial, ya fue incluido en los informes trimestrales de la Auditoría Interna, pero con todo gusto atenderán lo que esta Junta Directiva considere apropiado.

El presidente Sr. Espinoza Guido solicita que el Sr. Ricardo Azofeifa comente el panorama de este tema en el Banco Popular, específicamente sobre los avances al respecto en términos de reglamentación, autorizaciones y otros aspectos, pues en materia legislativa aún no hay muchos avances.

El director jurídico corporativo Sr. Azofeifa Castillo menciona que el Comité Ejecutivo tomó un acuerdo para revisar, a la luz del marco normativo, el uso de tecnología de inteligencia artificial en el ámbito de Conglomerado, tanto en asuntos que impacten el Código de Ética, como para hacer un procedimiento propio sobre el tema.

En su dependencia, estuvieron revisando la normativa existente y, si bien existe, no es suficiente, entonces, se acordó analizar el tema en conjunto con la Dirección Corporativa de Riesgo y la Dirección de Tecnología, porque más allá de las normas, hay temas que escapan de la parte legal y se vinculan con la seguridad de la información, la tecnología y el riesgo.

Así las cosas, una vez que esas mejores prácticas estén determinadas por las áreas competentes, su Dirección se encargará de darle forma para que dicha regulación pase a esa Comisión. Primero, debe aprobarlo el Comité Ejecutivo, después la Comisión Técnica de Asuntos Jurídicos y, finalmente, a la Junta Directiva Nacional.

La gerente general Sra. Ulate Murillo comenta que, en el nivel conglomeral, ya se tienen directrices sobre seguridad de la información e inteligencia artificial. Esos documentos fueron aprobados en las reuniones del equipo del Comité Ejecutivo.

Ahí se consideró que, para utilizar las herramientas de inteligencia artificial, debe tratarse de Copilot, que es interno de la plataforma Microsoft y de donde no sale la información cargada. Además, se tienen otras e directrices para avanzar en las políticas.

Se está trabajando, como bien lo indicó el Sr. Azofeifa Castillo, y se ha solicitado a los diferentes equipos avanzar en otros aspectos, pero sí está la seguridad de la información.

El presidente Sr. Espinoza Guido manifiesta que, siendo así, parece que está bastante acotado el uso de instrumentos o herramientas, sin embargo, le pareció escuchar que la Auditoría está yendo un poco más allá. Si está equivocado, solicita que lo corrija, porque se ahí debería levantarse una alerta.

El auditor interno Sr. Cortés Hernández explica que están utilizando Copilot y el año pasado cuando solicitaron la definición de directrices políticas, era en función de eso, pues no se querían apartar de ningún contexto de Conglomerado.

El otro tema que están desarrollando se vincula con la herramienta TeamMate Analytics, pero siempre en un contexto de Popular Valores, sin usar o cargar información en la nube, sobre lo cual se han cuidado de sobremanera, y eventualmente, estarán en un proceso de consulta con la firma que da mantenimiento en esa herramienta, apenas se está iniciando y está en función de las directrices.

El presidente Sr. Espinoza Guido recapitula y confirma que ya hay un lineamiento y una directriz corporativa que autoriza a las diferentes unidades de negocio a implementar Copilot para ciertas labores. Adicionalmente, está la inercia normal de los negocios que ejecuta Popular Valores, lo cual está en esa dinámica, entonces, percibe de parte de esta Junta Directiva su interés en que esta definición conceptual normativa interna se defina lo más pronto posible.

Pregunta si hay algún interés en tomar un acuerdo dirigido a dicho Órgano en ese sentido, porque remitirlo a otra instancia no es conveniente, en virtud de que es un tema tomado por la Gerencia General Corporativa, como debe ser.

Le cede la palabra y solicita ir concretando, porque este tema no estaba agendado.

El subgerente general de Operaciones Sr. Mora Mora agrega que el objetivo del Comité Ejecutivo es dictar una política en el uso de la inteligencia artificial en el nivel conglomeral.

La vicepresidenta Sra. González Mora trae a colación que cuando se han referido a Copilot, han considerado que es una herramienta de Microsoft con capas de seguridad y debidamente autorizada por esa firma, sobre todo cuando se tiene licenciamiento. Es una herramienta que tiene la seguridad de por sí y, por esa razón, probablemente fue autorizada corporativamente sin la existencia de políticas.

Le parece que tomar un acuerdo desde acá, ante la ausencia de esas políticas y reglamentación que se está creando desde el Banco, no sería conveniente, entonces, tal vez el presidente y su persona podrían informarse un poco para dar un lineamiento claro, correcto, y no incurrir en errores o en la creación de vulnerabilidades que eventualmente podrían afectar a la Subsidiaria y que podrían apartarse de lo planeado por la Gerencia General.

Insta a actuar con prudencia, aunque es muy importante y no quisiera que se limiten en la investigación sobre la búsqueda de alternativas y demás. La idea es no tomar un acuerdo hoy en este seno, porque prefiere ubicarse mejor.

El presidente Sr. Espinoza Guido concuerda y por eso hizo la pregunta; el tema es válido, está muy vivo, es importante, tampoco es que no se estén haciendo nada, pues ya está la iniciativa trazada por parte de la Administración del Banco.

Le indica a la vicepresidenta que en una próxima sesión de Junta Directiva se aborde una intervención sobre cuál es el estado actual de la elaboración de la política para que se documente no solamente en esta Subsidiaria, sino para todas las demás y así dejar plasmado el interés manifiesto.

Agradece por la discusión, por plantear el tema y comenta que se presentará la información de vuelta apenas se tenga.

ARTÍCULO 5

Todos los directores manifiestan estar de acuerdo con la propuesta.

Al respecto, la Junta Directiva acuerda por unanimidad:

> **"1. Dar por conocida la presentación del estudio de *Factibilidad técnica para la migración del dominio de Popular Valores al Banco Popular,* realizado por el Departamento de Tecnología de Información y el Administrador de Proyectos de Popular Valores.**
>
> **La exposición incorporó una evaluación preliminar de la factibilidad técnica para la migración de la infraestructura, aplicaciones y servicios actualmente operativos en el dominio *popularvalores.com* hacia el dominio *bp.fi.cr*. Esta evaluación de factibilidad se generó a partir de reuniones con compañeros del Banco Popular.**
>
> **Como punto importante se destacó que la migración es técnicamente viable en términos generales, dado que la infraestructura, los sistemas operativos, las bases de datos y los servicios en nube muestran una alta compatibilidad con el entorno destino.**
>
> **No obstante, su ejecución segura depende de una gestión controlada por fases y un ambiente paralelo, así como la validación previa de las dependencias críticas, especialmente en temas relacionados con servicios bursátiles y regulatorios, certificados e integraciones externas, continuidad operativa, seguridad, trazabilidad y cumplimiento.**
>
> **Todos estos aspectos estarán considerándose a partir de un cronograma coordinado y validado por el Banco Popular y Popular Valores.**
>
> **Finalmente, la exposición fue presentada por el gestor de proyectos Sr. Pablo Barrantes Rivera y el jefe de Tecnología de Información Sr. José Castro Lee.**
>
> **2. A raíz de la presentación del estudio de *Factibilidad técnica para la migración del dominio de Popular Valores al Banco Popular*, se solicita a la Administración del Puesto de Bolsa mantener informada a esta Junta Directiva de Popular Valores sobre el avance en la hoja de ruta para el conocimiento del traslado del dominio *popularvalores.com* hacia el dominio *bp.fi.cr*, según lo que se establezca a nivel interno y en coordinación con las dependencias correspondientes del Banco Popular.**

Dichos avances serán incorporados en los informes trimestrales de gestión de Tecnología de Información".
(Ref.: oficio PVSA-283-2026)

ACUERDO FIRME.

Lo declarado CONFIDENCIAL en este artículo, así como la documentación de soporte, obedece a que el tema discutido contiene información o se relaciona con asuntos ***de gestión de riesgo,*** *de conformidad con lo establecido en el artículo 24 de la Constitución Política, artículo 30 párrafo final de la Ley Orgánica del Sistema Bancario Nacional y el artículo 273 de la Ley General de la Administración Pública, en relación con las disposiciones de la Ley de Información No Divulgada, Ley No. 7975 y la Ley de Protección de la Persona frente al tratamiento de sus datos personales, Ley No. 8968.*

ARTÍCULO 6

Todos los directores manifiestan estar de acuerdo con la propuesta.

Al respecto la Junta Directiva acuerda por unanimidad:

"Dar por conocido el Informe CIA-009-PVAL*: Análisis del portafolio de inversiones en TI (Informe de portafolio de proyectos*) de Popular Valores Puesto de Bolsa, S. A., con corte a marzo de 2026.

Dentro de este informe se incorporan los siguientes considerandos:

I. Que, según la Calendarización de Informes Anuales, la actividad CIA-009 establece que el Departamento de Tecnología de Información debe presentar un Análisis de Portafolio de Inversiones en TI (Informe de portafolio de proyectos).

II. Que el estado de las iniciativas de optimización de los procesos, con corte a marzo de 2026, para Popular Valores tiene un avance en el cronograma general del 29%, con un cumplimiento del 91% de las actividades programadas.

III. Que se presentan los beneficios y recursos consumidos de las iniciativas del portafolio al cierre de marzo de 2026.

Finalmente, este informe fue expuesto por el gestor de proyectos Sr. Pablo Barrantes Rivera".
(Ref.: acuerdo CCTI-BP-09-ACD-95-2026-Art-6)

ACUERDO FIRME.

Lo declarado CONFIDENCIAL en este artículo, así como la documentación de soporte, obedece a que el tema discutido contiene información o se relaciona con asuntos ***estratégicos y de gestión de riesgo,*** *de conformidad con lo establecido en el artículo 24 de la Constitución Política, artículo 30 párrafo final de la Ley Orgánica del Sistema Bancario Nacional y el artículo 273 de la Ley General de la Administración Pública, en relación con las disposiciones de la Ley de Información No Divulgada, Ley No. 7975 y la Ley de Protección de la Persona frente al tratamiento de sus datos personales, Ley No. 8968.*

ARTÍCULO 7

Todos los directores manifiestan estar de acuerdo con la propuesta.

Al respecto, la Junta Directiva acuerda por unanimidad:

"Dar por conocido el *Informe mensual sobre el contexto económico bursátil local e internacional,* con corte a mayo 2026, expuesto por el gerente de Negocios Sr. Carlos Rivera Ramírez en atención al SIG-064-PVAL del Sistema de Información Gerencial de esta Junta Directiva de Popular Valores".
(Ref.: oficios PVSA-284-2026 y PVGN-135-2026)

ACUERDO FIRME.

Lo declarado CONFIDENCIAL en este artículo, así como la documentación de soporte, obedece a que el tema discutido contiene información o se relaciona con asuntos ***estratégicos y de auditoría****, de conformidad con lo establecido en el artículo 24 de la Constitución Política, artículo 30 párrafo final de la Ley Orgánica del Sistema Bancario Nacional y el artículo 273 de la Ley General de la Administración Pública,*

en relación con las disposiciones de la Ley de Información No Divulgada, Ley No. 7975 y la Ley de Protección de la Persona frente al tratamiento de sus datos personales, Ley No. 8968.

ARTÍCULO 8

4.1.4.- La Sra. Mónica Ulate Murillo, gerente general, remite para conocimiento, el Cronograma de Formulación PAO y Presupuesto 2027 de Popular Valores Puesto de Bolsa, S. A. (Ref.: oficio PVSA-269-2026).

La gerente general Sra. Ulate Murillo hace notar que este oficio es informativo, como en otras oportunidades, la idea es comentarle a la Junta Directiva que están iniciando con el proceso de planeación 2027 para la formulación del PAO, el presupuesto y para la coordinación desde ya de las sesiones en julio.

Recuerda que, en dicho mes, además de todos los informes de cierre de trimestre a junio, tienen las sesiones con los planes para el 2027. Entonces, les comenta que desde ya se están iniciando el proceso, ya se remitieron los oficios a las diferentes áreas para que envíen los requerimientos a mediados de junio, incluida la Auditoría Interna, Tecnología de Información, que tiene el Plan de Tecnología de Información que es conocido por esta Junta Directiva; menciona también el Plan de Sostenibilidad.

Trae a colación los indicadores que el Banco facilite, como los datos del tipo de cambio, la inflación, etc., estarían considerándose para el próximo año principalmente. La idea es presentarle a la Gerencia General Corporativa las proyecciones para el 2027 para su validación de acuerdo con el procedimiento corporativo que se tiene en los primeros días de julio. La Gerencia General del Puesto de Bolsa, representada en su persona, estará coordinando para tener esa reunión.

Reitera que en julio solicitarán tres sesiones, el objetivo es que en la primera y segunda sesión de julio se presente lo que corresponde a los diferentes planes, el Plan de Negocios, de Tecnología de Información, de Capacitación y de Sostenibilidad, así como el PAO y los cuadros del presupuesto.

La idea es tener el presupuesto final y el PAO para la tercera sesión de julio que sería el día 31. A partir de esa aprobación se remitirían al Banco para cumplir con las fechas solicitadas a partir de los procedimientos. Avisa que a principios de agosto debe remitirse para que se haga la consolidación que el Banco requiere.

Tienen tiempo hasta el cierre de setiembre para enviarlo a la Contraloría General de la República, sin embargo, la idea es incluir el presupuesto en los sistemas de la Contraloría en los primeros 15 días de ese mes.

Finaliza y queda atenta a comentarios o dudas.

El presidente Sr. Espinoza Guido observa que como siempre, lo hacen con bastante tiempo, para no tener que apresurarse al final.

Lee la propuesta de acuerdo: *Dar por conocido el Cronograma de Formulación del Plan Anual Operativo (PAO) y del Presupuesto 2027 de Popular Valores Puesto de Bolsa, S. A.*

Todos los directores manifiestan estar de acuerdo con la propuesta.

Al respecto, la Junta Directiva acuerda por unanimidad:

> **"Dar por conocido el Cronograma de Formulación del Plan Anual Operativo (PAO) y del Presupuesto 2027 de Popular Valores Puesto de Bolsa, S. A.".**
> (Ref.: oficio PVSA-269-2026)
>
> **ACUERDO FIRME.**

ARTÍCULO 9

Todos los directores manifiestan estar de acuerdo con la propuesta.

Al respecto, la Junta Directiva acuerda por unanimidad:

> **"Dar por conocida la información sobre la situación de los Fondos de Liquidez Mixtos de Popular SAFI generada a raíz de la intervención de la Financiera Desyfin, hasta el actual proceso concursal.**

Dentro del informe se incorpora la retroalimentación sobre los clientes de este Puesto de Bolsa que poseen inversiones en dichos fondos.

Finalmente, lo anterior se presenta en atención al inciso 2) del acuerdo JDPV-770-Acd-358-2024-Art-9".
(Ref.: oficio PVSA-274-2026)

ACUERDO FIRME.

Lo declarado CONFIDENCIAL en este artículo, así como la documentación de soporte, obedece a que el tema discutido contiene información o se relaciona con asuntos ***de auditoría****, de conformidad con lo establecido en el artículo 24 de la Constitución Política, artículo 30 párrafo final de la Ley Orgánica del Sistema Bancario Nacional y el artículo 273 de la Ley General de la Administración Pública, en relación con las disposiciones de la Ley de Información No Divulgada, Ley No. 7975 y la Ley de Protección de la Persona frente al tratamiento de sus datos personales, Ley No. 8968.*

ARTÍCULO 10

Todos los directores manifiestan estar de acuerdo con la propuesta.

Al respecto, la Junta Directiva acuerda por unanimidad:

"Dar por conocido el Informe Integral de Riesgos del Conglomerado Financiero Banco Popular y de Desarrollo Comunal, correspondiente a marzo de 2026 y expuesto por el representante de la Dirección Corporativa de Riesgo Sr. Johan Rojas Fonseca.

Dentro del informe se destacan las siguientes conclusiones para este Puesto de Bolsa:

- Popular Valores cumple en su totalidad con los requerimientos de capital para la cobertura de riesgos y los límites establecidos en el Reglamento de Gestión de Riesgo, aprobado por el Conassif el 27 de febrero del 2009.

- Para el mes de marzo se cumple con los indicadores del Perfil de Riesgo Institucional aprobado por esta Junta Directiva mediante su acuerdo JDPV-779-Acd-077-2025-Art-15, además, con lo dispuesto en el Manual de Políticas para la Administración Integral de Riesgo de Popular Valores (POL4-GCC).

- Con respecto al seguimiento de los objetivos del PAO, en marzo de 2026 se registra un cumplimiento del 99,15%.

- La aplicación de controles, el seguimiento de los indicadores de riesgo y la gestión de los riesgos que realizan las diferentes áreas de Popular Valores es fundamental para mantener el Perfil Institucional en nivel de riesgo medio de acuerdo con lo aprobado por esta Junta Directiva de Popular Valores.

Finalmente, la presentación de este informe se realiza de conformidad con lo establecido en:

- El CIA-06 (*Informe Mensual Integral de Riesgo Corporativo*) de la Calendarización de Informes Anuales del Comité Corporativo de Riesgo.

- El SIG-050 (*Informe Mensual Integral de Riesgo Corporativo*) de la Estructura del Sistema de Información Gerencial de la Junta Directiva Nacional.

- El artículo 9, inciso d) y en el artículo 13, inciso b), del Acuerdo SUGEF 02-10, *Reglamento sobre Administración Integral de Riesgo*.

- El artículo 33, inciso b), del *Reglamento para la Organización y Funcionamiento de los Comités y Comisiones del Conglomerado Financiero del Banco Popular y de Desarrollo Comunal.*

- El SIG-055-PVAL (*Informe Mensual Integral de Riesgo*) del Sistema de Información Gerencial de esta Junta Directiva de Popular Valores Puesto de Bolsa, S. A.**".**
(Ref.: acuerdo JDN-6307-Acd-400-2026-Art-14)

ACUERDO FIRME.

El presidente Sr. Espinoza Guido pide extender la presente sesión.

Todos los directores manifiestan estar de acuerdo con la propuesta.

Al respecto, la Junta Directiva acuerda por unanimidad:

> **"En virtud de que esta sesión ordinaria n.° 821 incorpora información muy importante y temas muy valiosos para Popular Valores, Puesto de Bolsa, S. A., se extenderá hasta finalizar la presente agenda. Por consiguiente, se solicita a la Secretaría General que considere el pago del tiempo extra para la funcionaria Sra. Anna Halina Molina Strugala por el tiempo en el que se extienda la sesión".**
>
> **ACUERDO FIRME.**

Lo declarado CONFIDENCIAL en este artículo, así como la documentación de soporte, obedece a que el tema discutido contiene información o se relaciona con asuntos ***de gestión de riesgo,*** *, de conformidad con lo establecido en el artículo 24 de la Constitución Política, artículo 30 párrafo final de la Ley Orgánica del Sistema Bancario Nacional y el artículo 273 de la Ley General de la Administración Pública, en relación con las disposiciones de la Ley de Información No Divulgada, Ley No. 7975 y la Ley de Protección de la Persona frente al tratamiento de sus datos personales, Ley No. 8968.*

ARTÍCULO 11

Todos los directores manifiestan estar de acuerdo con la propuesta.

Al respecto, la Junta Directiva acuerda por unanimidad:

> **"Dar por conocido el oficio PVAI-051-2026, remitido por el auditor interno Sr. Carlos Cortés Hernández, mediante el cual informa que la Auditoría Interna de Popular Valores Puesto de Bolsa, S. A. está sometiéndose a una evaluación de calidad para el período 2025.**
>
> **Por lo anterior, se les solicita a los miembros de esta Junta Directiva y Fiscalía, quienes estuvieron en funciones durante el año 2025, que completen la encuesta correspondiente y cuyo plazo es el 12 de junio de este 2026".**
>
> **ACUERDO FIRME.**

Lo declarado CONFIDENCIAL en este artículo, así como la documentación de soporte, obedece a que el tema discutido contiene información o se relaciona con asuntos ***de auditoría****, de conformidad con lo establecido en el artículo 24 de la Constitución Política, artículo 30 párrafo final de la Ley Orgánica del Sistema Bancario Nacional y el artículo 273 de la Ley General de la Administración Pública, en relación con las disposiciones de la Ley de Información No Divulgada, Ley No. 7975 y la Ley de Protección de la Persona frente al tratamiento de sus datos personales, Ley No. 8968.*

ARTÍCULO 12

4.3.2.- El Sr. Carlos Cortés Hernández, auditor interno, somete a consideración, la solicitud de vacaciones por un espacio 9 días, comprendidas del viernes 26 de junio al miércoles 8 de julio 2026 (Ref.: Oficio PVAI-057-2026)

El presidente Sr. Espinoza Guido cita el enunciado de este punto y plantea el acuerdo:

1. Aprobar la solicitud de disfrute de 9 días hábiles de vacaciones para el auditor interno de Popular Valores Sr. Carlos Cortés Hernández, del viernes 26 de junio al miércoles 8 de julio de 2026.

2. Nombrar a la Sra. Leonor Cordero Fuentes, contadora pública autorizada, cédula de identidad 302620105, vecina de Cartago, como auditora interna a. i., del viernes 26 de junio al miércoles 8 de julio de 2026.

3. Autorizar el pago por el recargo de funciones a la Sra. Leonor Cordero Fuentes como auditora interna a. i., del viernes 26 de junio al miércoles 8 de julio de 2026.

Lo antes indicado, según el Reglamento vigente en esta Sociedad, publicado en La Gaceta n.° 89 del 9 de mayo de 2008.

Todos los directores manifiestan estar de acuerdo con la propuesta.

Al respecto, la Junta Directiva acuerda por unanimidad:

> **"1. Aprobar la solicitud de disfrute de 9 días hábiles de vacaciones para el auditor interno de Popular Valores Sr. Carlos Cortés Hernández, del viernes 26 de junio al miércoles 8 de julio de 2026.**
>
> **2. Nombrar a la Sra. Leonor Cordero Fuentes, contadora pública autorizada, cédula de identidad 302620105, vecina de Cartago, como auditora interna a. i., del viernes 26 de junio al miércoles 8 de julio de 2026.**
>
> **3. Autorizar el pago por el recargo de funciones a la Sra. Leonor Cordero Fuentes como auditora interna a. i., del viernes 26 de junio al miércoles 8 de julio de 2026.**
>
> **Lo antes indicado, según el Reglamento vigente en esta Sociedad, publicado en La Gaceta n.° 89 del 9 de mayo de 2008".** (Ref.: oficio PVAI-057-2026)
>
> **ACUERDO FIRME.**

ARTÍCULO 13

Asuntos Varios.

El fiscal Sr. Oreamuno Herra recuerda que el 25 de este mes termina el plazo de presentación de la declaración jurada a la Contraloría General de la República; este tema fue informado y les quedan 4 días.

La vicepresidenta Sra. González Mora solicita que les hagan llegar el *link* de la autoevaluación de la Auditoría Interna por correo, para tenerlo a mano y que no se les olvide.

El auditor interno Sr. Cortés Hernández manifiesta que lo hará con todo gusto en cuanto finalice la sesión.

Por otra parte, en cuanto a lo comentado por el Sr. Oreamuno Herra, destaca la preocupación de la Contraloría General de la República por la baja participación e insta a presentar la declaración correspondiente.

El subgerente general de Operaciones Sr. Mora Mora recomienda no dejar la declaración para el último día, ya que pueden presentarse caídas del sistema y ser muy estresante. Los exhorta a realizar la declaración antes del vencimiento.

El presidente Sr. Espinoza Guido se despide y agradece la participación en la presente sesión.

Al ser las **DIECINUEVE HORAS CON CINCO MINUTOS**, finaliza la sesión.

Sr. Raúl Espinoza Guido
Presidente

Sr. Álvaro Ramírez Sancho
Secretario