# CIENXCIEN

**Episodio 15. La ciberseguridad no se instala: se entrena**

Con Mariano González, Irene Álvarez y Carmen Bacaicoa

*[Sintonía de entrada]*

“Luego, qué es lo que decimos en seguridad, el eslabón más débil. El eslabón más débil para nosotros es siempre el que está situado entre la silla y el teclado.”

**Ana**

“Nosotros.”

**Irene**

“Nosotros, el usuario.”

*[Sintonía de entrada con indicativo: “Esto es CIENxCIEN, el podcast del Banco de España”]*

**Ana**

Ver para creer. Hasta hace muy poco estábamos muy seguros de que si lo veíamos con nuestros propios ojos tenía que ser real.

El mundo de cine iba un poco más allá y siempre ha desarrollado y aprovechado avances tecnológicos que nos permitiesen ver lo que otros imaginaban. Habilidades heroicas, personajes fantásticos, batallas espaciales... Ahora con la inteligencia artificial podemos disfrutar de un joven Indiana Jones a sus 81 años o de Agatha Christie dando un curso de escritura en la BBC 50 años después de su muerte.

Se llama *deepfake* a los vídeos, imágenes o audios generados por inteligencia artificial que hacen que un contenido parezca completamente real, aunque no lo sea. Es como si alguien pudiera poner en tu boca palabras que no has dicho, hacer que parezca que estás en un lugar en el que nunca estuviste o, incluso, imitar tu voz con total precisión.

¿Te imaginas? Podrías incluso pensar que este podcast lo presenta Ana Comellas y en realidad ser otra la persona que ocupa su lugar.

Que haya un titiritero que haga que ella diga cosas que él quiere que tú escuches.

¿Y entonces cómo podemos distinguir lo real de lo falso? ¿Están en juego la privacidad y seguridad de cada uno de nosotros si confiamos en alguien que no es quien parece ser? ¿Qué medidas podemos tomar para evitar ser víctimas de un fraude? En definitiva ¿por qué es tan importante la ciberseguridad?

Para responder a estas y otras muchas preguntas tenemos la suerte de que nos acompañe Mariano González que cuando no juega a ser presentador es el CISO, el responsable de seguridad de la información del Banco de España, Irene Álvarez, especialista en la gestión de riesgos del Banco, y Carmen Bacaicoa, especialista en concientización de seguridad. Ellos son 100% confianza en el Banco de España y pertenecen a la Unidad de Riesgos y Seguridad de la Información. Bienvenidos.

Mariano, ¿es más habitual el *deepfake* de lo que pensamos? ¿Qué usos se le están dando?

**Mariano**

Pues la verdad que cuando hablamos de inteligencia artificial y *deepfake* nos creemos que somos bastante modernos, pero para nada somos tan modernos. Ya en 2012 en el festival Coachella se consiguió resucitar virtualmente a un rapero, a Tupac Saruk, Evidentemente en aquel momento la tecnología no era tan precisa como es ahora, pero tenemos un resultado bastante mucho más profesional y mucho más creíble en 2024 en la gala de celebración de los premios WMA donde otro rapero, Eminem, consiguió actuar, vivo, con su holograma o alter ego virtual.

Si nos vamos a otro terreno, como más el juego, es bastante habitual utilizar *deepfake* en los videojuegos relacionados con deportes porque los hacemos mucho más cercanos a las personas y mucho más vendibles cuando ponemos esas caras de esos personajes famosos que están jugando, ya sea fútbol o baloncesto o cualquier deporte.

Y por otro lado también tiene un uso bastante interesante, que me gusta especialmente, que es el de la divulgación histórica y básicamente, si Carlos III nos cuenta su historia en su viva voz y en su imagen es mucho más fácil que aprendamos historia.

Pero como cualquier tecnología no todo es positivo, no todos los usos son legítimos.

A nivel ciberseguridad hablamos mucho de que la inteligencia artificial se utiliza para el fraude y, en nuestro caso, algo que nos preocupa bastante es el fraude del CEO.

**Ana**

Y hecho hubo un caso muy sonado el de la consultora Arup que bueno no fue solamente el jefe fue todo un consejo de administración, ¿nos lo cuentas?

**Mariano**

Sí, este caso fue bastante curioso porque los atacantes empezaron con un simple correo electrónico. El empleado, que estaba bastante concienciado, evidentemente lo rechazó, pero los ciberatacantes dijeron “vamos a ir a un paso más allá” y, como bien dices, lo llamaron a una reunión y en esa reunión había tres personas de su confianza total en la empresa. Una de esas personas era el director financiero. ¿Qué pasa? Que si llega el director financiero y te invita a hacer una transferencia y hay otras personas de tu organización que están dando fe de lo que está pasando allí es real, si parece real como fue el caso, pues esa persona finalmente realizó las transferencias.

¿Qué pasó? 15 transferencias, 25 millones de dólares de pérdida financiera, que sinceramente es un pico.

Otros usos que se le que se le dan al *deepfake* sobre todo, o también recientemente, en el ámbito de la desinformación en medio de la escalada militar en la guerra Rusia y Ucrania, se publicó un vídeo apócrifo haciéndose pasar por Vlodomir Zelensky en el que él mismo instaba a sus, a su ejército a rendirse contra la ocupación la ocupación rusa, con lo cual pues si alguien se lo creyó, pudo tener determinadas consecuencias.

Y si nos movemos un poco más en el terreno del corazón, un poquito de salseo, también se están reportando muchos casos en los que alguien entra a una aplicación de citas, conoce a otra persona, esa persona resulta que es famosa y de principio a lo mejor no se lo cree, pero si te llama esa persona con la voz de esa persona famosa, con la cara de esa persona famosa, pues hay quien entra al fraude. Sospechosamente esa gente, en un momento determinado, tienen una enfermedad de un familiar y te piden dinero o quieren viajar para estar contigo, para pasar unos días contigo y te piden dinero.

Y puedes pensar ¿por qué la gente cae en eso? Porque tenemos mucho ego y al final el ego es algo que siempre incidimos en la ingeniería social: el atacante busca el ego de las personas ¿porque yo no voy a enamorar a una persona famosa? Por supuesto.

Parece una tontería, pero el trabajo muchas veces el trabajo que hacemos nosotros en las labores de concienciación que luego comentará Carmen, hay que trabajar mucho el ego. El ego puede ser una de las principales vías de entrada para atacar a una organización. Porque te crees importante, porque te crees guapo o te crees guapa… cualquier cosa se puede utilizar para atacar a una organización, y sobre todo relacionado con el ego, es clave.

**Ana**

Bueno y cuántos egos tenemos en el mundo ¿es muy habitual este tipo de fraudes?

**Mariano**

La gente muchas veces no denuncia este tipo de ataques. Por otro lado, a veces, cuando hablas con la policía o con las Fuerzas y Cuerpos de Seguridad del Estado, lo que te transmiten es que muchas veces no sabes si hay inteligencia artificial detrás de un ataque,

Lo que sí sabemos es que los datos que publica el Ministerio de Interior en su página web, si comparamos la primera parte del año 2024 con la primera parte del 2025, si bien los delitos tradicionales están bajando en torno al 2%, los ciberdelitos están subiendo cerca del 3,4% ¿Quiere decir que esto sea por el objeto de la inteligencia artificial? No lo sabemos, pero sí sabemos que la inteligencia artificial de alguna forma democratiza el acceso a las herramientas de fraude hacia para los malhechores.

Pero no me gustaría terminar esto como un mensaje negativo. La inteligencia artificial por supuesto es una tecnología, y como cualquier tecnología, nunca jamás la tecnología va a ser una amenaza, o la tecnología va a ser un riesgo. Lo que es una amenaza es el uso fraudulento que se puede hacer de la misma, y estoy totalmente convencido que si utilizamos la inteligencia artificial de forma que cumplamos con la normativa, y también de forma responsable, nos va a ayudar a hacer un mundo, un mundo mejor.

**Ana**

Carmen y ¿cómo podemos protegernos, no ya de este mundo mejor, sino de este tipo de fraudes?

**Carmen**

Bueno pues, como bien has dicho cuando nos has presentado, nosotros trabajamos en la unidad de riesgos y seguridad de la información entonces nuestro trabajo se focaliza mucho en la protección de la información y aquí sí que me gustaría recalcar la importancia de nuestra información, de nuestras contraseñas, de nuestros de nuestros datos bancarios, de nuestras fotos, de nuestra ubicación… Todos estos datos para los ciberdelincuentes son muy muy valiosos y tenemos que aprender a protegerlos.

Entonces ¿cómo podemos proteger nuestra información, nuestros datos personales, bancarios, etcétera? Bueno, pues manteniendo una buena higiene digital.

La higiene digital es un conjunto de hábitos, de buenos hábitos, de medidas, que nosotros adoptamos para proteger la información y nuestros dispositivos en un entorno digital. Medidas concretas, pues podemos empezar con las contraseñas. Estamos hablando de intentar crear contraseñas de al menos de 12 caracteres, que combinen letras mayúsculas con minúsculas, símbolos, números, etcétera. No, claro, aquí me puedes decir…

**Ana**

Lo estoy pensando, a gritos, te lo estoy diciendo: llega un momento que eso es inmanejable.

**Carmen**

Claro porque tenemos decenas de cuentas de distintos servicios y además es que las buenas prácticas dicen que por cada servicio tienes que tener una contraseña distinta. Entonces, claro, cómo podemos memorizar nosotros esa cantidad de datos, de contraseñas. Bueno, pues para eso tenemos unas herramientas, que son los gestores de contraseñas, que nos ayudan a guardar de manera segura todas esas contraseñas.

Otra medida que es muy interesante que tenemos que aplicar en la medida de lo posible, porque no siempre es posible, es el uso del doble factor de autenticación.

**Ana**

Es esta vez ¿no? que te piden como un código adicional.

**Carmen**

Eso es, suele ser un código que te llega por SMS a tu teléfono móvil y entonces, como el ciber delincuente pues no tiene acceso a ese segundo código de verificación, pues no podría realizar la operación, una transferencia o no podría acceder a la cuenta.

Más medidas. Pues también es muy importante la revisión de los permisos que damos a las aplicaciones que tenemos instaladas en los dispositivos.

¿A qué me refiero con esto? Una aplicación de linterna para funcionar no necesita acceder a mis contactos, como mucho necesitará acceso a la cámara para activar el flash y para iluminar. Entonces, tenemos que ser conscientes de estas cosas y si vemos en este caso tendríamos que sospechar de esa aplicación.

Y más medidas, pues yo ya acabaría pues con el tema de la instalación de antivirus en todos nuestros dispositivos y, muy importante, la actualización no sólo de lo que es el sistema operativo sino también de todas las aplicaciones que tengamos instaladas.

**Ana**

Pero ahora mismo ya en casa no estamos solos. Muchos de nosotros teletrabajamos, mantenemos reuniones a lo mejor con otros miembros de la familia, tenemos dispositivos digitales a nuestro alrededor que también están presentes mientras teletrabajamos. ¿Cómo influye la ciberseguridad que tengamos en nuestra casa en la ciberseguridad de la empresa?

**Carmen**

Pues efectivamente, hoy en día con el auge que tenemos del teletrabajo sí que es cierto que esa frontera entre lo personal y lo profesional sí que se ha diluido. Al final nuestras casas han pasado a ser como una extensión de la oficina y aparece un concepto que es el de oficina ampliada.

Podemos empezar con el tema de compartir contraseñas. Esto sí que es cierto que se va un poco de este contexto de teletrabajo, pero sí que uno de los principales errores que cometemos es que utilizamos las mismas contraseñas para el mundo laboral que para el mundo personal.

Otro de los riesgos que vemos es el tema de compartir espacios con personas, con nuestras parejas, con nuestros hijos, con nuestros compañeros de piso. Tampoco se trata de estar sospechando de que mi compañero de piso me está me está espiando. No, para nada es eso. Pero sí que tenemos que ser conscientes de que si estamos manteniendo una reunión en la que tratamos información sensible, pues si tenemos a personas que no tienen por qué estar escuchando esa información, sí que pudiera producirse una fuga de una fuga de información.

Y otro tema interesante que también lo has comentado es el uso de, pues eso, que hoy en día también está el auge de los dispositivos inteligentes. No convivimos sólo con personas en casa, sino que convivimos con unos dispositivos que están diseñados para escuchar constantemente y para activarse cuando detectan una palabra clave.

Entonces, bueno podría llegar a ocurrir que ese dispositivo grave fragmentos de esa reunión. Entonces, para evitar esto, lo que tenemos que hacer es apagar estos dispositivos, mantenerlos lo más alejados posible de esos espacios en los que yo estoy trabajando y también hacer una revisión de qué permisos les estamos dando a estos dispositivos, a qué es a lo que pueden acceder.

**Ana**

Irene, y siendo conscientes de esto, también de las nuevas formas de trabajo, ¿qué es lo que hacemos en el Banco para ser ciberseguros?

**Irene**

Pues ya veis que a nivel personal hay muchas cosas que hacer, pues a nivel corporativo también hay unas cuantas.

Lo primero con lo que contamos son unas herramientas de seguridad que nos defienden y personal, experto, que tiene el conocimiento para evitar cualquier ataque, o lo que intentamos, pero también contamos con normativa y con procedimientos que nos ayudan a seguir gestionando la seguridad de manera eficiente.

Y últimamente, una cosa que está adquiriendo mucha relevancia es los productos de terceros, Cada vez adquirimos más productos de terceros y se

está viendo que la seguridad peligra por ahí. Los cibercriminales han visto que es muchísimo más fácil atacar a un proveedor pequeño que a una empresa grande.

Un caso súper conocido fue el de SolarWinds, que lo que hicieron los cibercriminales fue infiltrarse en desarrollo de software. Había un software que se llamaba Orion, que era de monitorización y de gestión de la infraestructura IT, y bueno se infiltraron en el software, claro de una manera que el software parecía legítimo, pero llevaba ese código ahí imbuido y pues fue descargado por gobiernos, por empresas y estuvo allí latente nueve meses, espiando y sin ser detectado,

Luego, qué es lo que decimos en seguridad, el eslabón más débil. El eslabón más débil para nosotros es siempre el que está situado entre la silla y el teclado.

**Ana**

Nosotros.

**Irene**

Nosotros, el usuario.

**Ana**

El ego del usuario.

**Irene**

El ego del usuario que cree que controla todo perfectamente y pues lo que digo, al final tú le metes muchísimas herramientas, mucha gente ahí trabajando para que todo esté seguro y de repente llega un mail con un contenido malicioso y el empleado le da clic y adiós muy buenas todo, a la seguridad que habíamos puesto nosotros. Entonces, prestamos especial atención a la concienciación de nuestros empleados.

Pues aquí estábamos hablando de concienciación en el hogar, pues nosotros tenemos unas campañas de concienciación. Por un lado, tenemos ejercicios de phishing. Los ejercicios de phishing es lanzar emails trampa, de manera así que a ver cómo actúan nuestros empleados. Con eso, pues también detectamos quiénes son los que nos pueden provocar mayores riesgos y a la vez les concienciamos y les hacemos entender los riesgos que supone dar a un clic sin pensar.

Y luego lo que hacemos, que además suele gustar mucho, son unas jornadas en familia donde no sólo hacemos que el empleado sea consciente, sino que lo trasladamos también al ámbito familiar. Como comentaba Carmen, esa parte también es muy importante. Hacemos esa mezcla de concienciar al

empleado y a su familia. Hacemos unas jornadas que incluyen adultos y menores, con talleres, juegos, de manera muy lúdica y entretenida.

**Ana**

Irene, si pienso en un asalto al Banco de España, nos viene a todos a la cabeza 'La casa de papel'. Alguien que viene, que quiere entrar a la Cámara del Oro y llevárselo. Pero realmente es una frase que ya empieza a circular, que los datos son el nuevo oro. Quizá ese asalto al Banco de España no se produzca por la parte física, sino por la parte digital. ¿Qué hacemos contra eso? ¿Cómo nos preparamos?

**Irene**

Es muy difícil. Los que estamos en seguridad siempre tenemos que estar protegiendo continuamente todos los agujeros por donde pueden entrar. Ellos solo tienen que buscar un agujero y colarse. Es complicado realmente.

Al igual que para otras cosas físicas se hacen simulacros, nosotros hacemos ejercicios de simulacros. Por ejemplo, hacemos un ejercicio que se llama *Red Team*.

Volviéndonos a la serie, que tanto éxito tiene, y para que nos entendamos mejor. Es como si el Profesor se reúne con su equipo, se trae a Berlín, a Tokio, a Nairobi, nos juntamos. Esos son el *Red Team*. Vamos a preparar el ataque al Banco.

En este caso el objetivo no es el oro, no es el dinero, son los sistemas del Banco y quizá unos documentos. ¿Qué hace este equipo? Igual que en la serie, se junta varios meses, planea el ataque empezando por conocer al Banco.

En el caso de seguridad física serían los planos, los puntos ciegos de las cámaras, la rutina de los guardias. En nuestro caso sería ver qué sistemas informáticos usan, qué empleados hay por ahí que nos puedan servir para un ataque de ingeniería social, qué vulnerabilidades públicas tienen los sistemas del Banco de España.

Siguen pensando cómo vamos a entrar. En la serie sería, ¿vamos a entrar a través de la alcantarilla o a través del sistema de ventilación o por la puerta principal? En este caso vamos a ver si hacemos un lanzamiento de un phishing a este empleado que le va a dar clic o bien vamos a aprovechar una vulnerabilidad y vamos a ir saltando de sistema en sistema.

Y encima una cosa muy relevante en este ejercicio es que, obviamente para que sea exitoso y que no haya trampa, el equipo de defensor, la gente de seguridad, no sabe que se va a hacer este simulacro. La gente de seguridad es lo que llamamos el *blue team*.

Entonces imaginemos que ya están dentro, han conseguido entrar, a veces se consigue, otras veces no se consigue, eso depende del ejercicio. Ya están ahí con sus monos rojos, su máscara de Dalí.

El profesor se quita su máscara de Dalí. Esto ha sido un simulacro. Aquí tenéis un informe de seguridad.-¿Qué funciona? ¿Qué no funciona? Esta puerta la tienes mal cerrada, tienes que reforzar aquí. Este sistema tiene aquí esta vulnerabilidad. Hemos entrado por aquí. Una serie de pautas que al final el mensaje es hemos llegado hasta aquí y toca reforzar la seguridad y seguir aprendiendo.

**Ana**

Mariano, ¿y por qué es tan importante la seguridad, en este caso la ciberseguridad, del Banco de España?

**Mariano**

Si me permites darte un titular, te diría que protegiendo la ciberseguridad del Banco y protegiendo al sistema financiero, protegemos a la ciudadanía.

antes se protegía, simplificando mucho, salvaguardando el efectivo y salvaguardando el oro, ya digo simplificando mucho. Ahora ya no solo hay que salvaguardar o proteger esos dos temas, sino hay que proteger los datos, hay que proteger los sistemas informáticos que dan esa estabilidad al sistema financiero. En ese caso, en esa parte externa, trabajan nuestros compañeros de Supervisión y de Sistema de pago, que se encargan de hacer esa supervisión a las entidades financieras y a los medios de pago en relación con su riesgo tecnológico o su ciberresiliencia.

Y finalmente, en cuanto a la parte externa, también formamos parte de grupos de coordinación y de intercambio de información en caso de crisis sistémica.

Y luego la parte interna, que es la que trabajamos nosotros en el día a día dentro de la Unidad de Riesgos y Seguridad de la Información, garantizamos la ciberresiliencia de los activos del Banco, de los sistemas que dan soporte a nuestro negocio y, por supuesto, también a los sistemas que dan soporte a las infraestructuras de mercado que, como bien sabes, somos proveedores de servicios para todo el Eurosistema.

Y, por supuesto, no solo de las aplicaciones, sino que también garantizamos la confidencialidad y la integridad y la disponibilidad de los activos de información que dan soporte a todo el negocio del Banco, que no es poco.

**Ana**

Muy bien, pues si os parece me quedo con tres ideas.

La primera que siempre pensamos que la ciberseguridad es un tema técnico y ya vemos que es un tema de egos, que es un tema más de personas que de máquina.

Que tenemos que ser muy conscientes de los ciberriesgos sin tenerles miedo, igual que sabemos que en la calle hay muchos peligros y, sin embargo, no

dejamos de salir, simplemente salimos con precaución, pues en el mundo digital tenemos que seguir, por supuesto, utilizándolo, pero siendo conscientes

Y que las empresas, la inversión en ciberseguridad no solo tiene que ser en sus propios sistemas, sino también invertir en esa parte de que sus empleados sean ciberseguros.

Y terminamos ya el podcast con la pregunta de rigor de esta temporada que es, ¿qué hacen dos informáticos como vosotros, Irene, Mariano, en un sitio como el Banco de España?

**Irene**

Bueno, pues yo estaba en el sector privado y también en un banco donde, al final, el nombre de Banco de España se oía con mucho, como el regulador y entonces siempre te quedas con la, bueno, ¿qué pasa si pruebo a entrar? Y aparte también, mi familia incluso, también se oía mucho ese prestigio del Banco de España. Es una cosa que, la verdad, que como que ya desde bien pronto, pues como que había oído siempre hablar con mucho prestigio del Banco de España y, al final, cuando oyes hablar tanto de algo, pues te animas a ver qué pasa si entro aquí, ¿no? Y, bueno...

**Ana**

Aquí estás.

**Irene**

Aquí estoy, aquí estoy. Muy contenta.

**Ana**

Mariano.

**Mariano**

En mi caso, la verdad que inicié mi carrera profesional en una consultora muy orientada al sector público y siempre tuve el gusanillo de qué puedo aportar yo al servicio público. Cuando estaba trabajando, yo en este caso estaba trabajando en otro momento en una telco y vi que se publicaban las plazas de expertos en tecnología de la información aquí en el Banco y decidí que era un buen momento.

Unido a que la vocación de servicio público me viene desde chiquitillo, desde educación, desde casa y que también, como decía Irene, el Banco de España me parece un sitio importante e interesante donde poder seguir aprendiendo y poder seguir desarrollándome profesionalmente, pues todo eso se unió y casi siete años que llevo ya trabajando aquí y muy contento.

**Ana**

Y, en tu caso, Carmen, teleco, una ingeniera de telecomunicaciones en el Banco de España.

**Carmen**

Si, eso es, soy teleco pero siempre me he dedicado al mundo de la informática. Yo conocí el Banco hace muchos años, en 2008, fue mi primer trabajo y empecé en una empresa externa, en una tecnológica. En 2013, salieron unas plazas de técnico de sistemas de información y me animaron a presentarme, me presenté y aprobé.

Luego seguí donde estaba, en el mismo proyecto en el que estaba y en 2018, si hace ya siete años, decidí dar un cambio a mi vida profesional y me embarqué en este mundo de los riesgos y de la seguridad de la información y aquí estoy siete años después, la verdad que muy contenta con unos compañeros que habéis visto que son muy top y aprendiendo mucho de ellos todos los días y nada más.

**Ana**

Pues muchas gracias, Carmen, gracias, Irene, Mariano, muchas gracias a los tres por hacernos también conscientes de toda esa seguridad que no se ve pero que tan importante es en nuestra vida personal y también profesional.

**Mariano**

Muchísimas gracias, Ana por invitarnos a la Unidad de Riesgos y Seguridad de la Información a este podcast que sabemos que es muy importante para el banco y para nosotros también es muy importante que se vea todo el trabajo que hacemos.

**Ana**

Pues para eso estamos; nos volveremos a ver, no me cabe duda.

*[Sintonía de salida]*

**Ana**

Soy Ana Comellas y todo lo que escuchas en este podcast es 100% Banco de España. Ya sabes que puedes escuchar todos los episodios en nuestra web, www.bde.es/podcast, donde encontrarás además información adicional a este episodio tan educativo.

También los puedes escuchar en YouTube Podcast, en Spotify o en tu plataforma de podcast favorita. En nuestra web, además de encontrar toda la información y servicios que ofrecemos a la ciudadanía, podrás encontrar los enlaces del Portal del Cliente Bancario y de Finanzas para Todos.

Muchas gracias por escucharnos.

*[Sintonía de salida]*