CIBERATAQUES

LA CONCIENCIA YA NO ES UNA OPCIÓN

CIBERATAQUES
LA CONCIENCIA YA NO ES UNA OPCIÓN

RESUMEN EJECUTIVO

El crecimiento exponencial de los ataques cibernéticos contra particulares y organizaciones, cuya causa original se puede deber a un error humano, ha eliminado definitivamente cualquier duda sobre cuál es el eslabón débil de la cadena defensiva de las organizaciones.

LA TENDENCIA DE LOS CIBERATAQUES CRECE DE FORMA CONTINUA Y RÁPIDA.

LA CIBERSEGURIDAD ES UN PROBLEMA TRANSVERSAL QUE ATAÑE A TODO EL SISTEMA DEL PAÍS Y QUE AFECTA INDISTINTAMENTE A PERSONAS Y CLASES DE ORGANIZACIONES DE TODO TIPO

El factor humano, aún más vulnerable por el efecto pandémico, es hoy el **vector primario** utilizado por los **delincuentes informáticos** para infiltrarse en las organizaciones, con estrategias ofensivas cada vez más sofisticadas.
Son precisamente los usuarios, con comportamientos que no se adecuan a la complejidad del reto, los que abren sin saberlo la puerta a los atacantes.

La tendencia ya era muy evidente antes de la pandemia. Si se analizan desde 2020 los diversos informes sobre el estado de la ciberseguridad, tanto en Italia como en todo el mundo, el cuadro que emerge es que el **crecimiento de los ataques cibernéticos** parece **imparable** y que, entre las diversas técnicas de ataque utilizadas, las que se caracterizan por un mayor crecimiento se basan principalmente en el factor humano. Una confirmación más de que la gran mayoría de los ciberataques tienen un componente humano, atribuible a una acción incorrecta de un usuario.

La entrada en el escenario económico y social de la pandemia del coronavirus no ha hecho más que agravar esta situación, que ha aumentado el número de ataques. En los últimos años, la acción de los ciberdelincuentes se ha centrado cada vez más en las personas que, ante el fenómeno pandémico y sus principales consecuencias, como el uso masivo del trabajo inteligente, se han revelado mucho más vulnerables de lo que quizás las organizaciones podrían haber imaginado.

La **crónica** está **repleta** de **ciberataques** que han llegado a buen término y que han afectado a organizaciones de todos los sectores y de todos los tamaños. Marcas prestigiosas y otras menos conocidas han visto sus actividades productivas bloqueadas y su reputación comprometida. Incluso la vieja frase que tanto han citado muchas pymes, «No somos atractivos para un pirata informático», ha quedado desmentida por los hechos.

Se trata de una auténtica **guerra cibernética**. Una guerra asimétrica que ve a los **atacantes** en una **posición** de **indudable ventaja**, sobre todo porque la primera línea de defensa está formada por civiles desarmados que, en la mayor parte de los casos, ni siquiera se dan cuenta de que les están atacando.

En los últimos años, las **capacidades de defensa** desde un punto de vista tecnológico han aumentado, sin duda, pero la eficacia de estas inversiones se ve constantemente frustrada, de acuerdo con la teoría del **eslabón débil**, según la cual la **«fuerza global de una cadena viene determinada por el eslabón más débil».** Cuando el eslabón débil, como en este caso, son los usuarios que interactúan con las tecnologías digitales y con la red Internet, resulta evidente que las inversiones tecnológicas dejan de ser suficientes para detener los ataques.

La única manera de recrear una simetría entre los atacantes y los defensores es invertir en la **«primera línea de defensa»**, es decir, en los **usuarios digitales**. Es necesario que cada organización elabore **programas eficaces** e innovadores de concienciación sobre ciberseguridad. Sin embargo, solo se podrá ganar la guerra si estas inversiones demuestran toda su eficacia en el plano formativo, con programas capaces de incidir concretamente en los comportamientos de las personas.

En los últimos años, se han impulsado las inversiones en esta área, a menudo insuficientes, más por el requisito de lograr un grado mínimo de cumplimiento normativo que por la necesidad de alcanzar objetivos eficaces de protección contra los ataques cibernéticos.

Por otra parte, las principales normativas y los marcos que hacen referencias explícitas a la seguridad informática (por ejemplo, el RGPD, NIST, la Directiva NIS, AGID, etc.) han puesto de relieve la cuestión de la formación de los usuarios finales, pero han dejado un amplio espacio de interpretación a las organizaciones a la hora de determinar lo necesario para poder cumplir estas prescripciones.

Un espacio tan amplio que las iniciativas desarrolladas han demostrado ser ciertamente funcionales con respecto a la necesidad de cumplir con las regulaciones, pero absolutamente ineficaces en lo que se refiere al objetivo real: **aumentar la protección de las personas** y las **organizaciones** contra el riesgo cibernético.

EL RIESGO CIBERNÉTICO ES UNO DE LOS RIESGOS EMPRESARIALES MÁS IMPORTANTES A LOS QUE SE ENFRENTARÁN LAS ORGANIZACIONES EN LOS PRÓXIMOS AÑOS.

LOS CIBERATAQUES SE SIRVEN CADA VEZ MÁS DEL COMPONENTE HUMANO, EL VERDADERO ESLABÓN DÉBIL DE LA CADENA DEFENSIVA.

Por estas razones, es fundamental iniciar **programas de concienciación sobre ciberseguridad eficaces** e **innovadores**, capaces de **influir** en el **comportamiento de las personas** y de **convertir a los usuarios** en la primera línea de defensa de las organizaciones.

ESTA ES, DESDE EL PRINCIPIO, LA MISIÓN ESPECÍFICA DE CYBER GURU: CREAR UNA PLATAFORMA DE CONCIENCIACIÓN SOBRE CIBERSEGURIDAD CAPAZ DE AYUDAR A SUS CLIENTES A FORTALECER EL ESLABÓN MÁS DÉBIL DE LA CADENA DE CIBERSEGURIDAD.

LA PLATAFORMA CYBER GURU SE HA DESARROLLADO Y APLICADO CONSTANTEMENTE UTILIZANDO LAS TECNOLOGÍAS, LOS PROCESOS DE PRODUCCIÓN Y LAS METODOLOGÍAS PEDAGÓGICAS MÁS AVANZADAS PARA GARANTIZAR LA MÁXIMA IMPLICACIÓN DE LOS USUARIOS Y EL LOGRO DEL OBJETIVO PRINCIPAL DE UN PROGRAMA DE CONCIENCIACIÓN SOBRE SEGURIDAD: LA PROTECCIÓN CONTRA LOS RIESGOS CIBERNÉTICOS.

1. EL ESCENARIO

1.1 LA TRANSFORMACIÓN DIGITAL Y SUS TRAMPAS

RESUMEN

Podemos decir que 2021 ha estructurado la disrupción social y económica desencadenada por la pandemia en el año anterior para convertirla en una situación de alarma crónica en todos los frentes.

La transformación digital forzada ocurrida en 2020 y gestionada **con urgencia** se ha convertido en una **realidad consolidada** con la que la colectividad debe lidiar, para bien o para mal. Una de las consecuencias más obvias ha sido el crecimiento de los ciberataques, que se ha sumado a la ola del año anterior al continuar explotando las vulnerabilidades psicológicas y también la brecha entre el proceso acelerado de digitalización y la conciencia de los usuarios sobre las amenazas cibernéticas, a los que aún les queda camino que recorrer.

ESTOS DOS ÚLTIMOS AÑOS QUE HEMOS VIVIDO SERÁN, SIN DUDA, RECORDADOS EN LOS LIBROS DE HISTORIA COMO LOS AÑOS DE LA **PANDEMIA DE LA COVID-19** Y DE TODAS LAS TRANSFORMACIONES TRASCENDENTALES QUE LA COLECTIVIDAD HA VIVIDO TRAS ESTE EVENTO.

EN PRIMER LUGAR, ESTÁ EL **REPOSICIONAMIENTO** DE **NUESTRA VIDA** EN LA WEB. SI ANTES DE LA COVID-19 SOLO UNA PARTE DE ELLA SE COMPARABA DIARIAMENTE CON LA RED, HOY SE PUEDE DECIR QUE LA WEB GESTIONA LA MAYOR PARTE DE NUESTROS DÍAS.

Desde el trabajo, a la escuela, pasando por las relaciones, las compras y la información. En resumen, ya no se puede prescindir de ninguna faceta de la web. Esto ha supuesto una oportunidad muy apetitosa para quienes hacen de la **estafa informática** su profesión y, por tanto, los **ataques de piratas informáticos** han pasado a ser una **realidad muy extendida** e igualmente peligrosa.

Tanto es así que **JP Morgan** los definió como **«el arma más peligrosa del mundo»** en su Consejo Internacional, celebrado en el pasado mes de diciembre, y Christine Lagarde los describió como «la mayor amenaza para la estabilidad financiera, junto con el cambio climático» en la conferencia anual de la Junta Europea de Riesgo Sistémico (JERS). Afirmaciones que suscitan gran alarma y que, por desgracia, los datos confirman.

Según el **Informe Clusit** 2022 sobre **Seguridad Cibernética**, en los últimos 4 años, el promedio mensual de ataques graves en el mundo ha aumentado de 130 a 171, lo que resulta en un crecimiento dramático de las pérdidas, que han pasado de 1 billón de dólares en 2020 a 6 billones en 2021, con una tasa de empeoramiento anual de 2 dígitos y un valor de 4 veces el PIB italiano.

Una escalada debida principalmente al **uso masivo** del **trabajo inteligente** que, por la emergencia, se ha convertido, en muchas situaciones, en una nueva modalidad de trabajo, pero también a la adopción cada vez más frecuente de la enseñanza a distancia y de métodos de formación en línea, y al recurso a plataformas de colaboración social y de entretenimiento digital, que no es menospreciable.

Un signo indiscutible de esta rápida transformación también se puede ver en el **crecimiento** de **las compras en línea** que, según los datos del informe de Salesforce Shopping Index, para el primer trimestre de 2021, ha experimentado un **aumento global del** 58 % interanual en comparación con el 17 % del primer trimestre de 2020.

RECORDEMOS QUE EN EL **COMERCIO EN LÍNEA** ENTRAN EN JUEGO MÉTODOS DE PAGO COMO LAS TARJETAS DE CRÉDITO, CUYOS DATOS SON ESPECIALMENTE APETECIBLES PARA LOS **CIBERDELINCUENTES**. COMO CONFIRMACIÓN DE LA MAYOR DIGITALIZACIÓN DE LA SOCIEDAD, NO PODEMOS OBVIAR EL CONSTANTE AUMENTO EN EL USO DE BANDA. EN LOS PRIMEROS MESES DE LA PANDEMIA, MUCHOS OPERADORES DE SERVICIOS DE RED REGISTRARON AUMENTOS TAN IMPORTANTES COMO PARA TEMER ESCENARIOS APOCALÍPTICOS SOBRE EL MANTENIMIENTO DE INTERNET.

Italia es la protagonista, con un aumento del 78 %, porcentaje que la posiciona en el primer lugar en Europa y en el cuarto en el mundo, después de Canadá, Holanda y Reino Unido. Un **salto tecnológico** que sin duda ha representado y representa una gran oportunidad en el camino de la innovación, pero que, por otro lado, puede conllevar aterrizajes bruscos, si no traumáticos.

El punto es que todo esto ha sucedido sin el crecimiento correspondiente de la **cultura digital** y, por tanto, sin que los usuarios sean verdaderamente capaces de poder disfrutar de las tecnologías digitales y de la red Internet de manera segura. Una falta de conciencia de las amenazas del mundo digital que aún no se ha cubierto y que, por tanto, continúa brindando grandes oportunidades a las organizaciones delictivas cibernéticas.

1.2 **LOS ATAQUES CIBERNÉTICOS:** LAS «GRIETAS» PSICOLÓGICAS Y TECNOLÓGICAS

RESUMEN

La **situación particular** generada por la **pandemia** es el origen del **crecimiento** de los **ataques cibernéticos** que comenzó en 2020 y continuó fortaleciéndose en 2021. Desde este punto de vista, es necesario tener en cuenta tanto las **vulnerabilidades tecnológicas**, relacionadas con el trabajo inteligente, el aumento de todas las actividades en línea y el uso de nuevas herramientas digitales, como los códigos QR, como las de **carácter psicológico**, relacionadas con los **continuos estados** de **emergencia** y la condición de distanciamiento social. Dos «grietas» importantes en las que el crimen se ha infiltrado fácilmente, dando lugar a ataques que han tenido un efecto disruptivo en muchas organizaciones. La crónica se ha llenado de casos emblemáticos relativos a organizaciones de todo tipo y de todos los tamaños que han visto cómo ha disminuido su capacidad de operar por períodos más o menos largos, con todas las consecuencias, económicas y de imagen, que un parón de este tipo puede conllevar.

LA **PANDEMIA** DE LA **COVID-19** HA TENIDO UN **EFECTO DISRUPTIVO** NO SOLO EN EL PLANO ECONÓMICO Y SOCIAL, SINO TAMBIÉN EN LA **ACELERACIÓN** DE LOS **ATAQUES CIBERNÉTICOS** CLASIFICADOS COMO GRAVES.

Una tendencia ya fuertemente registrada en 2020 y que en 2021 ha experimentado un fuerte aumento. El informe Clusit, presentado a principios de año, habla de casos graves al alza y de una Europa cada vez más en el centro de los ataques de los ciberdelincuentes: +22 % frente al 16 % de 2020 y el 11 % de 2019.

Al aumento cuantitativo se suma el cualitativo, porque los **daños** son mucho más **graves** para las **empresas afectadas**. En general, en el cuatrienio 2018-2021 el número de ataques graves analizados por Clusit indica un aumento del 32 % y entre las categorías más afectadas se encuentran el sector gubernamental (15 %) seguido de las TIC y múltiples objetivos.

Según los datos sobre la **gravedad de los ataques**, los de nivel crítico fueron el 32 %, de nivel alto, el 47 %, de nivel medio, el 19 %, y de nivel bajo, solo el 2 %.
En general, por tanto, la gravedad crítica y alta de los ataques alcanzó el 80 %, mientras que el año anterior era del 56 %.

Además, un estudio reciente de IBM Security, el **«Cost of a Data Breach Report 2021»**, reveló que los ataques a la seguridad informática han ocasionado, en el año recién terminado, los costes más altos por violaciones de datos de los 17 años de historia del informe, con una media de 4,24 millones de dólares por incidente. Si la tendencia continúa así, las perspectivas no serán precisamente de color de rosa.

LOS PRINCIPALES **IMPULSORES DE** LA ACELERACIÓN DE LOS **ATAQUES CIBERNÉTICOS** SIGUEN DEBIÉNDOSE A LAS TRANSFORMACIONES INDUCIDAS POR LA PANDEMIA. UNO DE TIPO **PSICOLÓGICO** RELACIONADO CON EL EFECTO SOBRE LA PSIQUE HUMANA DE LA SITUACIÓN DE EMERGENCIA, EL OTRO DE TIPO **TECNOLÓGICO** ATRIBUIBLE AL USO MASIVO DE FORMAS DE TELETRABAJO Y AL MAYOR USO DE LA RED PARA LAS ACTIVIDADES COTIDIANAS.

El **nivel psicológico** ha generado estados de ansiedad y miedo típicos de las emergencias, con la **pérdida** de los **puntos de referencia** tradicionales, la búsqueda obsesiva de noticias e información y la dificultad de discernir entre la información verdadera y falsa, una dificultad que también se ve acuciada por las técnicas avanzadas de creación de **noticias falsas**.

Aprovechando estos estados de ansiedad mucho más extendidos en la población que en el período previo a la COVID-19, se han multiplicado las **campañas** de **«phishing»** que han tenido como objeto los distintos temas de la COVID-19: las diferentes variantes del virus, el Certificado COVID Digital de la UE y toda la información, a menudo alarmista, que ha girado en torno a la pandemia.

Además, el usuario se ha encontrado entonces más aislado y ha sido más propenso a perder sus puntos de referencia habituales dentro de la empresa u organización, difíciles de encontrar solo con el uso de herramientas de colaboración social.
Por otro lado, en el contexto específico generado por la pandemia, muchas veces los espacios del hogar han sido y son compartidos con otros familiares que funcionan de la misma manera, tanto por motivos profesionales como didácticos, de forma que se han creado así condiciones críticas desde el punto de vista de la seguridad informática.

COMPARTIR DISPOSITIVOS, LA RED, PERO TAMBIÉN ACTUAR INCONSCIENTEMENTE DEBIDO A FENÓMENOS INDUCIDOS POR LA DISTRACCIÓN, SE CONVIERTEN EN ELEMENTOS QUE JUEGAN EN BENEFICIO DE LA DELINCUENCIA.

Teniendo en cuenta que el **eslabón débil** es siempre el **comportamiento de las personas,** en una situación de alarma sanitaria generalizada, la atención a los comportamientos correctos que deben mantenerse en línea se ha penalizado, lo que ha abierto las puertas a los **delincuentes cibernéticos** que, como refinados conocedores de la psique humana, saben colarse por las **grietas emocionales**.

A todo esto se ha añadido el **nivel tecnológico**: el trabajo inteligente se basa en una arquitectura compleja que a menudo emplea dispositivos privados del usuario, menos seguros por definición y equipados dotados de configuraciones de «hardware».
También en este caso, sin embargo, es el factor humano el que más preocupa porque la brecha que existe entre la **velocidad** del **proceso** de **transformación digital** y la de **adaptación** de las **personas** a esta nueva dimensión socioeconómica sigue jugando, incluso hoy, a favor de la ciberdelincuencia.

Basta pensar en los **riesgos surgidos** con el aumento masivo del uso de **códigos QR**, que cada vez se utilizan más para resolver problemas relacionados con las restricciones pandémicas o para proporcionar servicios más innovadores y eficaces.

Una herramienta que, como toda tecnología, puede facilitar mucho la vida cotidiana, pero que, sin embargo, debe «manejarse» con cuidado, porque puede **esconder trampas peligrosas**, como **«malware»** o **sitios fraudulentos**. El hecho de que la mayoría de los usuarios no estén bien informados sobre las implicaciones opacas de los códigos QR, y de las herramientas digitales en general, facilita el trabajo a los piratas informáticos, que siempre están buscando nuevas formas de acceder a su delito favorito.

1.3 **LA GUERRA:** NO SOLO EN EL FRENTE, SINO TAMBIÉN EN EL CIBERESPACIO

RESUMEN

Para complicar una situación ya de por sí dramática, se ha sumado, a principios de este año, también la **guerra** en **Ucrania**, que ha abierto **más escenarios** en el frente de la **seguridad informática**. Además de la guerra tradicional, la que se hace disparando armas, se está combatiendo en otra **guerra**, la **cibernética**, hecha con otro tipo de armas y que tiene grandes repercusiones globalmente. Pero los efectos aún no son cuantificables y probablemente se verán dentro de unos meses, tal vez años.

Según los **controles** de **CheckPoint**, los ataques al sector gubernamental y militar desde el inicio de las hostilidades ya han aumentado en todo el mundo en un 21 %.
Una señal indudable de que el conflicto rusoucraniano es a todos los efectos un conflicto global que no solo se reduce al espacio geográfico de los dos países protagonistas.

En este escenario, ningún país europeo puede estar tranquilo, dadas las múltiples voces institucionales que recientemente han lanzado un **grito de alarma** sobre la vulnerabilidad cibernética de sus países, señalando la guerra cibernética como uno de los mayores riesgos en los que podemos vernos involucrados.

Los casos de ataques de piratas informáticos que aprovechan los **temores** de la **guerra** en curso son cada vez más frecuentes. Las primeras víctimas de los piratas informáticos fueron las empresas manufactureras europeas, que fueron víctimas de esta guerra y fueron blanco de una campaña de «phishing» por correo electrónico con el asunto **«Supplier Survey: Effect of supply chain from the Ucraine/Russia conflict»**. En el correo electrónico, los piratas informáticos, con una falsa apariencia, instaron a los destinatarios a completar un formulario adjunto, que obviamente contenía «malware», para informar de cualquier retraso y planes de apoyo.

Un terreno fértil que explota los miedos causados por la guerra y los fuertes impactos en el abastecimiento. Por no hablar de las diversas oleadas de spam y «phishing», en las que los **ciberdelincuentes**, haciéndose pasar por **agencias humanitarias** o **instituciones ucranianas**, han hecho circular en Europa y en Estados Unidos campañas benéficas y de recaudación de fondos con el único objetivo de robar dinero.

Pero estos pocos ejemplos de los que hemos hablado no son ciertamente todos los de una situación dinámica y en continuo movimiento que podría comportar la disrupción del escenario geopolítico y financiero, y de los equilibrios económicos, cosa que sin duda tendrá consecuencias para la seguridad informática, pero cuyos efectos probablemente se verán dentro de unos meses, tal vez años.

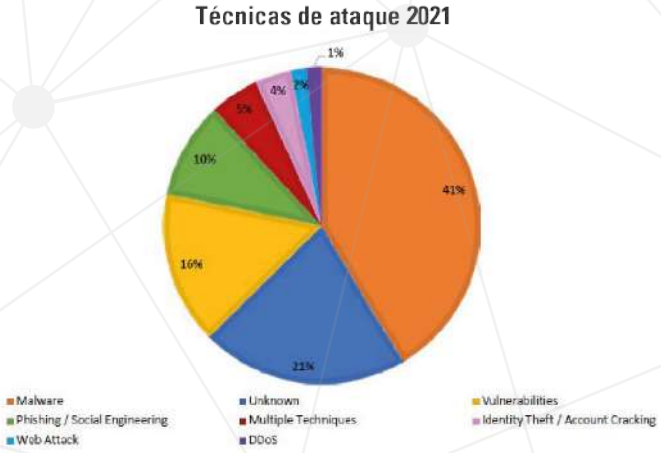
LA **AGENCIA** PARA LA **CIBERSEGURIDAD NACIONAL** EN ITALIA HA ECHADO LEÑA AL FUEGO ADVIRTIENDO A LAS EMPRESAS DE LA **URGENCIA** DE «PROCEDER A UN ANÁLISIS DEL RIESGO DERIVADO DE LAS **SOLUCIONES** DE **SEGURIDAD INFORMÁTICA** UTILIZADAS Y CONSIDERAR LA APLICACIÓN DE ESTRATEGIAS DE DIVERSIFICACIÓN APROPIADAS EN LO QUE RESPECTA, EN PARTICULAR A ANTIVIRUS, APLICACIONES WEB, "FIREWALLS", LA PROTECCIÓN DEL CORREO ELECTRÓNICO, LA PROTECCIÓN DE LOS SERVICIOS EN LA NUBE Y LOS SERVICIOS DE SEGURIDAD GESTIONADOS».

1.4 MÁS ALLÁ DEL «PHISHING» Y DEL «MALWARE»

RESUMEN

Si bien casi toda la atención sigue recayendo en los fenómenos del «malware» y, obviamente, del «phishing», ya hemos comentado cómo se han disparado literalmente en el último año las demás formas de ataque relacionadas con las distintas «grietas» o vulnerabilidades que los delincuentes logran aprovechar para causar daños u obtener datos o dinero de particulares y empresas. Entre ellas, ocupa un lugar de honor, sin duda, la relacionada con la **inteligencia artificial** y el **IoT**, el **Internet de las cosas**.

LO QUE SURGE AL ANALIZAR LAS NUEVAS FORMAS DE ATAQUE EN 2021, ES QUE LOS **DELINCUENTES** CIBERNÉTICOS SON CADA VEZ MÁS **SOFISTICADOS** Y CAPACES DE CONECTARSE CON EL CRIMEN ORGANIZADO. COMO RESULTADO, LAS **AMENAZAS** SE HAN VUELTO CADA VEZ MÁS SUTILES Y DIFÍCILES DE DETECTAR Y SE CENTRAN CADA VEZ MÁS EN EXPLOTAR LOS PUNTOS DE ENTRADA CONSIDERADOS MÁS DÉBILES, INCLUIDAS LAS PERSONAS.



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

El **informe Clusit** 2021 revela que más de la mitad de los objetivos afectados han sido víctimas de «malware» y de sus vulnerabilidades. En esencia, los ciberdelincuentes se han basado principalmente en la **eficacia** del **«malware»**, que ahora se produce industrialmente con un coste cada vez menor, y en la explotación de cualquier eslabón débil que pueda suponer una oportunidad para sus objetivos.

En este sentido, el **rápido desarrollo** de las **tecnologías digitales** y las aplicaciones que utilizan inteligencia artificial, sin duda una oportunidad importante para toda la humanidad, no puede pasar desapercibido. De hecho, si hasta hace unos años hubiéramos visto a nuestro mejor amigo hablando con la nevera, habríamos pensado en llamar a un médico o en recomendarle un largo período de vacaciones, mientras que hoy ya nos parece lo más normal del mundo. Sí, porque nuestras acciones diarias dependen cada vez más de herramientas de inteligencia artificial que reemplazan a las personas, no solo a la hora de actuar, sino también de pensar. A veces es difícil saber dónde acaba una y empieza la otra.

«SMART CITY», «SMART BUILDING», «SMART OFFICE», «SMART HOME», «SMART DEVICE» Y «SMART WEARABLES»: EL FUTURO DE LA HUMANIDAD OCCIDENTAL PARECE ENCAMINADO IRREVERSIBLEMENTE HACIA EL MÁXIMO RENDIMIENTO CON EL MÍNIMO ESFUERZO.

Hablamos de una revolución que afecta a las personas en su dimensión individual y también en la profesional. Y es que la adopción de sistemas IoT también está creciendo continuamente en las organizaciones, en especial en la automatización de edificios, en el sector automovilístico y en la atención sanitaria.

Es un **proceso** en **constante evolución** que allana el camino a una infinidad de aplicaciones posibles y que, especialmente cuando la red 5G se extienda ampliamente, gestionará la mayor parte de las facetas de nuestras vidas. Una perspectiva fascinante para muchos, pero que también implica grandes riesgos.

Sin entrar en las implicaciones que todo esto puede tener para el funcionamiento de nuestra mente, sin duda hay que subrayar el **riesgo** de la **seguridad**, que es **proporcional** al **uso** de la conexión a Internet. También porque los dispositivos inteligentes a menudo, especialmente en comparación con los ordenadores y los teléfonos inteligentes, han evolucionado mucho menos desde el punto de vista de las defensas tecnológicas y podrían usarse como una especie de caballo de Troya para infiltrarse en las redes. En resumen, las presas perfectas para los ciberdelincuentes.

En los últimos cinco años, los **ataques cibernéticos** relacionados con el IoT se **han multiplicado por 70**, ya que la mayoría (alrededor del 76 %) de las diversas herramientas se comunican con la red a través de canales no cifrados, por lo que resultan vulnerables para dicha de los piratas informáticos.

BASTA DECIR QUE ESTOS SISTEMAS DE INTELIGENCIA ARTIFICIAL A MENUDO SE INTEGRAN CON SISTEMAS DE COMERCIO ELECTRÓNICO Y, EN CONSECUENCIA, CON MEDIOS DE PAGO, COMO TARJETAS DE CRÉDITO O PORTAFOLIOS DIGITALES. UNA OPORTUNIDAD MUY APETECIBLE PARA LOS ESTAFADORES QUE VAN EN BUSCA DE GANANCIAS.

Según un estudio realizado por **Kaspersky**, el 89 % de los propietarios de dispositivos IoT tienen dudas sobre su seguridad en la red. Entre las preocupaciones más comunes, está la de ser **espiado** por ciberdelincuentes a través de **cámaras** y **micrófonos**, o recibir una solicitud de rescate después del bloqueo de uno de los dispositivos, o infectar toda la red doméstica.

Preocupaciones absolutamente fundadas tanto para los entornos en los que se vive como en los que se trabaja, también porque la difusión del IoT experimenta un crecimiento irreversible.
Según algunos analistas, para 2025 se prevé la presencia de más de 30 000 millones de conexiones de IoT en todo el mundo. Con estos números, cada persona y trabajador tendrá a disposición una media de 4 dispositivos interconectados. Por tanto, conocer las herramientas para defenderse de estos riesgos es de vital importancia.

LA SENSIBILIZACIÓN Y LA FORMACIÓN ADECUADA SOBRE LOS RIESGOS DIGITALES SIGUEN SIENDO LAS DOS ARMAS MÁS EFICACES.

1.5 **EN LA NUEVA ERA DIGITAL, LA SEGURIDAD NO ES UNA OPCIÓN**

RESUMEN

Ya se ha hecho evidente que la vida «de antes», la cual muchos añoran, tal vez no vuelva nunca más y los efectos que la pandemia ha causado pasarán a ser estructurales. La confianza que expresamos el año pasado sobre el final de la emergencia probablemente deba reducirse. De hecho, nos hemos dado cuenta de que la **emergencia** en todas sus formas se está convirtiendo en la **nueva normalidad** y que tendremos que **adaptarnos** lo más **rápidamente** posible a las transformaciones sociales y laborales que la crisis sanitaria nos ha impuesto. Por esta razón, es necesario actuar con decisión sobre el **factor humano**, el verdadero eslabón débil del sistema defensivo, con programas formativos eficaces de concienciación sobre ciberseguridad, una medida ya ineludible para la **seguridad** de las **personas** y de las **organizaciones**.

EL **«SMART WORKING»** ESTÁ ASUMIENDO UNA CONNOTACIÓN **ESTRUCTURAL**, ASÍ COMO EL COMERCIO ELECTRÓNICO, LA ENSEÑANZA A DISTANCIA Y LAS DISTINTAS PLATAFORMAS FORMATIVAS, Y LOS SERVICIOS AL CIUDADANO POR PARTE DE LA ADMINISTRACIÓN PÚBLICA Y DE LAS SOCIEDADES QUE PRESTAN SERVICIOS PÚBLICOS.

SI, POR UN LADO, LA **TRANSFORMACIÓN DIGITAL** REPRESENTA UNA GRAN OPORTUNIDAD PARA LA **INNOVACIÓN** Y LA **MODERNIZACIÓN**, POR OTRO LADO, CONLLEVA INEVITABLEMENTE LIDIAR CON UN **MAYOR RIESGO** PARA LA **SEGURIDAD**.

Para empeorar las cosas, los nuevos modos de ataque, como hemos visto, son cada vez más sofisticados, y la ingeniería social es cada vez más refinada y, a menudo, los ciberdelincuentes ya no actúan de forma autónoma, sino que se conectan con otros «compañeros» o incluso con la delincuencia organizada, lo que tiene efectos muy perjudiciales, especialmente para las empresas.

En resumen, si el futuro de nuestras vidas y empresas no puede prescindir de lo digital, la **gestión** de **datos**, su **uso correcto** y su **protección** estarán cada vez más en el centro de cualquier inversión empresarial.

Una tendencia que, afortunadamente, ha sido aceptada por **Europa** y que se ha traducido en el compromiso de apoyar a los **Estados miembros** en su transición a la **digitalización**. En este escenario, es importante ser conscientes de que no todos los países de la Unión Europea tienen el mismo nivel de digitalización, tal y como se desprende de la edición 2021 del índice de digitalización de la economía y la sociedad (Desi).

En los países con un menor nivel de digitalización, la población de entre 16 y 74 años posee competencias digitales básicas y solo el 22 % tiene competencias digitales superiores a las básicas.

Según el informe, Italia, entre los países de Europa con un bajo nivel de digitalización, «se enfrenta a importantes deficiencias en las competencias digitales básicas y avanzadas que corren el riesgo de traducirse en la exclusión digital de una parte significativa de la población y de limitar la capacidad de innovación de las empresas».

Por tanto, será determinante dónde se invertirán los 48 100 millones que, en el caso específico, el gobierno italiano ha decidido destinar a este sector a través del **PNRR** (Plan Nacional de Recuperación y Resiliencia), en el cual la **ciberseguridad** ocupa un lugar central y estratégico.

Hasta ahora, los estudios publicados sobre la transición digital indican que la evolución del tratamiento de los datos y de su seguridad será la carta ganadora para lograr la recuperación económica. En resumen, la innovación digital, además de ser muy atractiva, es esencial para el negocio del futuro, pero con su desarrollo también crece su lado oscuro, es decir, el riesgo de ataques cibernéticos.

Solo hay una forma de protegerse: una adecuada formación empresarial que permita a todos los empleados llegar preparados al encuentro con la nueva digitalización, evitando clics erróneos e irreversibles.

Para ello, es necesario actuar con decisión sobre el factor humano, el verdadero eslabón débil del sistema defensivo. La actuación sobre el factor humano y, en consecuencia, los programas de formación en concienciación sobre ciberseguridad, deben considerarse una medida de seguridad necesaria.

Muchas organizaciones a lo largo del tiempo han **activado** estos **programas** con el único objetivo de demostrar el cumplimiento de las diversas normativas que incluyen, en sus estándares, la **formación** del **personal**; en muchos casos esto ha supuesto poca atención a la verdadera eficacia de los **recorridos formativos**. Sin embargo, los dos últimos años nos han demostrado de manera inequívoca que esta actitud es perdedora y que en el futuro tendremos que preocuparnos sobre todo por su eficacia.

Los programas deberán ser capaces de transformar concretamente las actitudes y los comportamientos de los usuarios frente a la amenaza cibernética.

POR TANTO, AL OPTAR POR LA VÍA DE LA CONCIENCIACIÓN SOBRE CIBERSEGURIDAD, LAS ORGANIZACIONES DEBERÁN TENER EN CUENTA ALGUNAS VARIABLES FUNDAMENTALES COMO LA EFICACIA, LAS METODOLOGÍAS DIDÁCTICAS UTILIZADAS, LAS TÉCNICAS DE IMPLICACIÓN EMPLEADAS, LAS TÉCNICAS DE ACTUALIZACIÓN EN LOS DISTINTOS NIVELES DE CONCIENCIACIÓN Y TAMBIÉN LOS LENGUAJES MULTIMEDIA USADOS.

2. LA FORMACIÓN

2.1 UNA MEDIDA DE SEGURIDAD NECESARIA

RESUMEN

Todas las organizaciones que quieran beneficiarse de este imparable proceso de transformación digital deben invertir en el factor humano con programas de formación avanzados y eficaces capaces de transformar concretamente los comportamientos de los usuarios, adaptándolos al nivel de la amenaza que nunca deja de crecer ni de desarrollarse. Estamos ante un reto asimétrico en el que los atacantes llevan indudablemente ventaja. Para devolverle la simetría al problema, es necesario aprovechar el factor humano que, en ciberseguridad, desempeña un papel decisivo.

EL DESARROLLO DE LA SOCIEDAD DIGITAL, CON SUS RIESGOS, OBLIGA A TODAS LAS ORGANIZACIONES A INVERTIR DE MANERA SUSTANCIAL EN EL FACTOR HUMANO, ESPECIALMENTE EN EL NIVEL DE CONCIENCIACIÓN DE LAS PERSONAS. UNA INVERSIÓN QUE HA PASADO A SER NECESARIA PARA CERRAR LA BRECHA CULTURAL QUE LOS EFECTOS PANDÉMICOS Y LA RÁPIDA TRANSFORMACIÓN DIGITAL HAN AGUDIZADO.

El **problema** no solo afecta a las personas menos acostumbradas al uso de las tecnologías digitales, sino también a las **nuevas generaciones** y a los llamados **«millennials»**.
Las nuevas generaciones, a pesar de tener una propensión natural al uso de las tecnologías, a menudo adoptan una postura digital similar a la de los «usuarios inconscientes», al no saber reconocer los riesgos cibernéticos que están detrás de sus acciones.

Nos hemos acostumbrado en los últimos años a ver la **ciberseguridad** como un tema **tecnológico** que solo afectaba a un nicho de especialistas. Detrás de esto está la creencia de que en algún lugar de nuestra organización, siempre hay alguien que se ocupa de la seguridad cibernética y que con eso basta. Cuando nos enfrentamos a un ciberataque, tendemos a pensar que el problema solo le corresponde a ese equipo de especialistas.

Además, la ciberseguridad siempre se ha percibido como algo que atañe exclusivamente a la dimensión profesional de nuestra existencia, como algo que no nos afecta directamente. El prejuicio siempre ha sido el mismo: **«¿Por qué un pirata informático iba a interesarse en mi persona».** En los últimos años, nos hemos tomado todo esto con cierta «ligereza»: una convicción que ha afectado no solo al comportamiento de los usuarios, sino también, y esto es aún más preocupante, al de las funciones directivas. Hoy está claro que la ciberseguridad es, en cambio, un problema transversal que afecta a todo el mundo y que afecta por igual a personas y organizaciones de todo tipo.

Un **desafío asimétrico** en el que los atacantes están en una posición de indudable ventaja, también porque, la primera línea de defensa la componen personas «indefensas» que no son conscientes de las amenazas ni de las contramedidas necesarias. En algunos casos, los usuarios reciben ataques sin darse cuenta. Siguiendo la teoría del eslabón débil, según la cual la fuerza global de una cadena depende de su eslabón más débil, podemos afirmar que la eficacia de estas inversiones se ve hoy extremadamente reducida por la debilidad del factor humano.

CON LOS AÑOS, LAS ORGANIZACIONES SE HAN PREOCUPADO SOBRE TODO DE DESARROLLAR CAPACIDADES DEFENSIVAS TECNOLÓGICAS Y, SIN DUDA, ESTAS DEFENSAS HAN AUMENTADO.

La presencia en el campo de un eslabón tan vulnerable, como el que representan los **usuarios** que **interactúan** con las **tecnologías digitales** y con la red Internet, nos permite hacernos una idea de lo desequilibrada que está la situación, en la que los atacantes cuentan con ventaja.

Para poder devolver la simetría a la situación, ya que, de lo contrario, el resultado no cambiará, es necesario que los usuarios sean **conscientes**, y luego, en consecuencia, maduren sus actitudes y adapten sus comportamientos a los riesgos cibernéticos.
Un proceso continuo que no solo requiere adquirir conocimientos teóricos, sino también **entrenar** algunas cualidades defensivas de las personas, como la **percepción** del **peligro** y la **prontitud**.

Un proceso que, si, por un lado, debe verse como una medida de seguridad necesaria, por otro lado, debe diseñarse y manejarse según los criterios típicos de la formación orientada al desarrollo de los recursos humanos. Para aumentar la conciencia de las personas, se necesitan **programas de capacitación avanzados**, basados en metodologías innovadoras de capacitación continua, entrenamiento y participación.
Plataformas de formación que minimicen el impacto en las funciones de gestión de la formación y la ciberseguridad. Solo de esta manera será posible mantenerse al día con la evolución constante de las estrategias de ataque, que son cada vez más sofisticadas y, sobre todo, capaces de adaptarse a los cambios constantes de los escenarios. También hay que tener en cuenta la necesidad de guiar el **aprendizaje cognitivo** de manera adecuada, sin sobrecargar el sistema cognitivo del alumno que, no lo olvidemos, es una persona extremadamente ocupada y solo puede dedicar a la formación «parte» de su atención.

EN CIBERSEGURIDAD, ¡EL FACTOR HUMANO DESEMPEÑA UN PAPEL DECISIVO!

2.2 EL PAPEL DE LA FORMACIÓN

RESUMEN

La única manera de reforzar las capacidades defensivas de las organizaciones frente a la **ciberdelincuencia** consiste en **invertir significativa** y constantemente en la «primera línea de defensa», es decir, en las **personas**. Por tanto, será necesario involucrar a toda la fuerza laboral en un **recorrido formativoque** permita a todo el mundo usar de forma cada vez más consciente las tecnologías digitales, las herramientas sociales y los recursos presentes en la web.

Un camino de crecimiento que permita adquirir un nivel de conocimiento compartido y que estimule algunas cualidades defensivas de las personas, como la **atención**, la **prontitud** y la **reactividad**.

Tratemos de imaginar una ciudad medieval fortificada preparándose para resistir un asedio. Piensa en un puñado de soldados empeñados en reforzar incesantemente las defensas perimetrales de la ciudad, mientras la mayor parte de los habitantes sigue entrando y saliendo de las fortificaciones dejando las puertas abiertas, y entre ellos, algunos incluso cavando túneles desde el interior hacia el exterior, para garantizarse vías de acceso privilegiadas hacia algunas zonas de la campiña circundante.

El mero hecho de imaginarlo parece absurdo, porque los habitantes de las ciudades medievales eran perfectamente conscientes del riesgo individual y colectivo que tal comportamiento produciría.
A menos de que fuese un conspirador a sueldo del enemigo, a ningún ciudadano se le habría ocurrido siquiera debilitar el sistema defensivo de su ciudad con un comportamiento «de riesgo».

En cambio, en la **realidad digital**, abundan este tipo de comportamientos, y ocurren en un clima de total **inconsciencia**, sin una percepción real del **nivel** de **riesgo** determinado por estos comportamientos.

DE ESTE MARCO SE DESPRENDE LA CERTEZA DE QUE LA ÚNICA MANERA DE RECREAR UNA SIMETRÍA EN LA ETERNA LUCHA ENTRE ATACANTES Y DEFENSORES CONSISTE EN INVERTIR SIGNIFICATIVA Y CONSTANTEMENTE EN LA PRIMERA LÍNEA DE DEFENSA, ES DECIR, EN LAS PERSONAS, LOS USUARIOS DE LAS TECNOLOGÍAS DIGITALES.

Ya hemos destacado cómo el factor humano se puede encontrar en la mayoría de los ataques, incluso en los aparentemente más tecnológicos. Los vectores de activación más comunes pueden deberse a comportamientos por parte de los usuarios relacionados con:

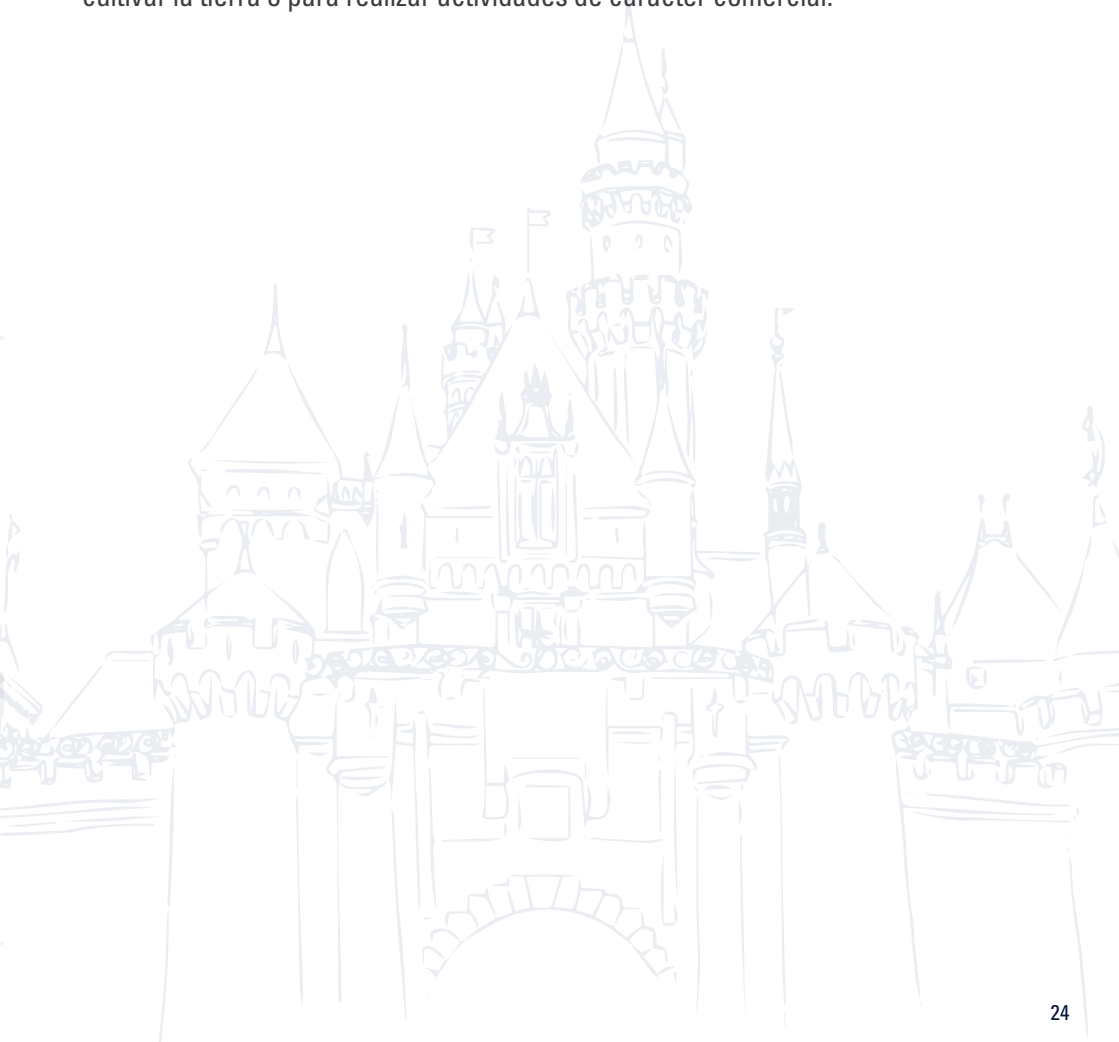
- **LA GESTIÓN DE LOS DISPOSITIVOS DIGITALES;**
- **LA INTERACCIÓN CON LA MENSAJERÍA, DESDE EL CORREO ELECTRÓNICO;**
- **EL USO DE CREDENCIALES DE ACCESO Y, EN PARTICULAR, DE CONTRASEÑAS;**
- **LA POCA ATENCIÓN AL VALOR DE LA PRIVACIDAD Y DE LA INFORMACIÓN CRÍTICA;**
- **LA ACTITUD CON LA QUE SE NAVEGA POR LA RED INTERNET Y CON LA QUE SE ABORDAN LOS RECURSOS DE LA WEB.**

Para contrarrestar eficazmente los riesgos cibernéticos, cada organización, pública o privada, tendrá que involucrar a toda la plantilla, independientemente del papel desempeñado y de las habilidades, en un recorrido formativo que permita a todo el mundo usar de forma cada vez más consciente las tecnologías digitales, las herramientas sociales y los recursos presentes en la web.

Un **camino** de **crecimiento** que permita adquirir un nivel de **conocimiento compartido** y que estimule algunas cualidades defensivas de las personas, como la **atención**, la **prontitud** y la **reactividad**.

La **conciencia** del **riesgo** lleva a reaccionar de manera más adecuada ante los peligros conocidos, pero también a tener una **actitud defensiva correcta** ante **amenazas potenciales** aún desconocidas, una actitud que en el mundo cibernético es absolutamente necesaria por la **rápida evolución** de las técnicas de ataque.

La conciencia también es necesaria para evitar que una actitud extremadamente defensiva frente a una percepción irracional del riesgo produzca comportamientos que afecten negativamente a la productividad del individuo y de la organización. También en las ciudades medievales era necesario salir de las fortificaciones para cultivar la tierra o para realizar actividades de carácter comercial.



2.3 **METODOLOGÍA EFICAZ**

RESUMEN

Un programa de formación que tiene como objetivo transformar los comportamientos individuales debe basarse en una metodología eficaz, que muestre resultados tangibles en los procesos de aprendizaje.

Una metodología que no se centre exclusivamente en el aspecto memorista, sino que sea capaz de integrar en el proceso formativo también recorridos de carácter experiencial e inductivo. Esta mezcla de componentes permitirá desarrollar no solo el conocimiento, sino también la percepción del riesgo y la preparación, creando una generación de usuarios conscientes, capaces de interactuar correctamente en la esfera digital, tanto en su dimensión personal como en su dimensión profesional.

UN PROGRAMA FORMATIVO DE CONCIENCIACIÓN SOBRE CIBERSEGURIDAD DEBE TENER COMO BASE UNA **METODOLOGÍA EFICAZ**, ORIENTADA A UN **RESULTADO PARTICULARMENTE DESAFIANTE** COMO EL DE TRANSFORMAR LOS COMPORTAMIENTOS DE LAS PERSONAS. LA CONSECUCIÓN DE ESTE RESULTADO ESTÁ ESTRICTAMENTE RELACIONADA CON LA CAPACIDAD PARA ACTUAR DE MANERA EFICAZ EN LOS PROCESOS DE APRENDIZAJE, TANTO EN LOS DE CARÁCTER MÁS ESTRICTAMENTE DIDÁCTICO, COMO EN LOS RELACIONADOS CON LA ACTITUD DE FONDO EN LO QUE SE REFIERE A LA CIBERSEGURIDAD, AMBOS TIPOS NECESARIOS PARA LOGRAR QUE EL CAMBIO DEL COMPORTAMIENTO SEA DURADERO.

La formación debe contribuir a desarrollar la **correcta percepción** del **riesgo** cibernético, **realineando** la **esfera racional** con la **emocional**, porque hoy en día en la mayoría de los casos la dimensión objetiva y la subjetiva no están equilibradas. En lo que respecta a los usuarios digitales, en general el **riesgo cibernético se subestima profundamente,** o, por el contrario, precisamente por no comprender correctamente el fenómeno, se pueden generar actitudes de bloqueo a la hora de enfrentarse a los ineludibles procesos de la transformación digital.

Un **usuario consciente** es un usuario que tiene una comprensión clara de las amenazas de la red y una percepción correcta del riesgo cibernético, y que, por tanto, ha adoptado una actitud digital adecuada. Un usuario consciente es también aquel que puede comprender cómo el tema de la conciencia afecta tanto a su dimensión privada como a su dimensión profesional, además de desarrollar la capacidad de mantener ambas dimensiones lo más separadas posible, porque hoy en día estas dos dimensiones a menudo tienden a superponerse.

Una **metodología eficaz** debe evitar los errores que en los últimos años han impedido que las iniciativas de concienciación sobre ciberseguridad generen el clima de participación necesario, una condición fundamental para lograr resultados tangibles si se quiere reducir el riesgo. Errores a menudo inherentes a los métodos de formación tradicionales y que, en este contexto específico, al tratarse de una materia considerada particularmente difícil, pueden tener aún más relevancia.

Entre las **percepciones erróneas,** las más comunes sobre el tema de la concienciación sobre ciberseguridad son:

- LA CONCIENCIACIÓN SOBRE LA CIBERSEGURIDAD ES UNA DISCIPLINA TÉCNICA QUE TIENE EL PROPÓSITO ILUSORIO DE TRANSFORMAR A LOS USUARIOS EN ESPECIALISTAS DE LA INDUSTRIA O EN UNA ESPECIE DE SHERLOCK HOLMES MODERNO CAPAZ DE LLEVAR A CABO INVESTIGACIONES SOFISTICADAS;

- LA CONCIENCIACIÓN SOBRE LA CIBERSEGURIDAD AFECTA EXCLUSIVAMENTE A LA DIMENSIÓN PROFESIONAL DEL INDIVIDUO Y, POR TANTO, A SU PAPEL DENTRO DE LA ORGANIZACIÓN;

- LA CONCIENCIACIÓN SOBRE LA CIBERSEGURIDAD TIENE COMO ÚNICO OBJETIVO PROTEGER A LA ORGANIZACIÓN EN LOS PROCESOS DE AUDITORÍA VINCULADOS A NORMATIVAS OSCURAS Y TIENE UNA IMPLICACIÓN IMPOSITIVA;

- LA CONCIENCIACIÓN SOBRE LA CIBERSEGURIDAD ES UNA FORMACIÓN IMPUESTA QUE NO PRODUCE RESULTADOS ÚTILES NI PARA EL INDIVIDUO NI PARA LA ORGANIZACIÓN;

- LA CONCIENCIACIÓN SOBRE LA CIBERSEGURIDAD TRATA ARGUMENTOS TEÓRICOS QUE NO GUARDAN NINGUNA CORRESPONDENCIA PRÁCTICA EN LA DIMENSIÓN PRIVADA NI EN LA PROFESIONAL DEL INDIVIDUO.

La **concienciación sobre la ciberseguridad** es, en cambio, una disciplina transversal, de carácter divulgativo, que permite desarrollar la competencia necesaria para actuar de manera segura en la esfera digital, tanto en la esfera privada, protegiéndonos a nosotros mismos y a nuestra red social, como en la profesional, protegiendo nuestro papel y nuestras responsabilidades corporativas, nuestra organización y todo el ecosistema del que la organización forma parte (clientes, proveedores, socios, etc.).

Para obtener resultados concretos, los programas de concienciación sobre la ciberseguridad no pueden limitarse a proporcionar nociones, sino que deben articularse en caminos de carácter experiencial e inductivo, siguiendo los enfoques **«learning by doing»** y **«learning by example»**.

Uniendo enfoques formativos de carácter didáctico, a otros de carácter experiencial e inductivo, se obtiene una significativa mezcla capaz de actuar positivamente sobre el conocimiento, sobre la percepción del peligro y sobre la prontitud, condicionando actitudes y comportamientos.

Aunque es bastante fácil imaginar una **formación didáctica**, cuesta más pensar en una formación experiencial e inductiva. En el caso del aprendizaje experiencial, el usuario deberá experimentar situaciones típicas de un ataque, como el caso de un ataque de «phishing», convirtiéndose en el objetivo de simulaciones capaces de reproducir la experiencia real. Por su parte, la formación inductiva deberá llevarse a cabo en situaciones reales, a través de una narrativa eficaz que produzca un proceso de identificación, hasta el punto de sentir la amenaza con una concreción mayor a la acostumbrada.

2.4 **FORMACIÓN CONTINUA**

RESUMEN

Dadas las características y el contexto específico de la temática, un programa formativo, para ser eficaz, debe desarrollarse según un modelo de formación continua, el cual podríamos definir metafóricamente como de tipo «homeopático», caracterizado por microintervenciones repartidas a lo largo del tiempo. Una formación capaz de actuar no solo en el plano cognitivo, sino también en el plano perceptivo, para permitir al usuario desarrollar una verdadera actitud a la hora de reconocer las amenazas de la dimensión digital, algo parecido a lo que sucede con las amenazas de la vida real.

EN EL CONTEXTO HISTÓRICO ACTUAL, UN PROGRAMA DE CONCIENCIACIÓN SOBRE CIBERSEGURIDAD, PARA SER EFICAZ, DEBE DESARROLLARSE SEGÚN UN MODELO DE FORMACIÓN CONTINUA, ALINEADO CON EL PROCESO DE TRANSFORMACIÓN DIGITAL Y DE EVOLUCIÓN DE LOS ATAQUES CIBERNÉTICOS, QUE PROCEDE SIN SOLUCIÓN DE CONTINUIDAD.

Para sustentar un modelo de formación continua, sin afectar negativamente de manera manifiesta la productividad del individuo y de los equipos de trabajo, será fundamental realizar microintervenciones organizadas periódicamente.

El principio básico es que las organizaciones deben acostumbrar a su plantilla a dedicar regularmente una parte de su tiempo (aunque compatible con sus actividades y con la necesidad de no sobrecargar el sistema cognitivo) a prevenir aquello que hoy es el riesgo más importante para su seguridad individual y, en consecuencia, para la seguridad de toda la organización.

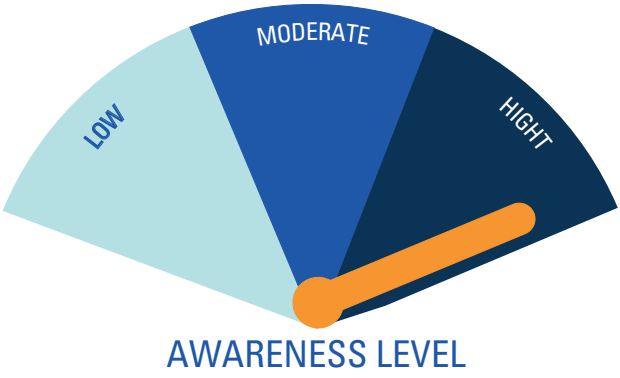
POR TANTO, ES ESENCIAL TOMAR REALMENTE CONCIENCIA DEL NIVEL DE RIESGO. PORQUE EL RIESGO CIBERNÉTICO PUEDE, POR UN LADO, HACER QUE LA VIDA DE UNA PERSONA SE CONVIERTA EN UNA VERDADERA PESADILLA Y, POR OTRO LADO, PONER EN ENTREDICHO LA PROPIA SUPERVIVENCIA DE LA ORGANIZACIÓN.

Hoy en día, la ciberseguridad ya no es un tema tecnológico, sino un serio problema empresarial y, por tanto, el riesgo cibernético también debe interpretarse de manera diferente que en años anteriores.

¿CUÁL ES LA RELACIÓN ENTRE FORMACIÓN CONTINUA Y FORMACIÓN EFICAZ?

¿Por qué un modelo de formación continua debería ser más eficaz que un modelo de formación caracterizado por enfoques más «concentrados», más intensos y, por tanto, más fáciles de organizar, gestionar y supervisar?
Antes de responder a esta pregunta, es necesario dar una premisa: en esta profundización no se tiene en cuenta la formación en el aula, porque se considera menos eficaz en el ámbito profesional y porque los eventos que se han producido desde 2020 han demostrado, de hecho, que, para abordar esta clase de problemas, solo nos queda la opción de la formación a distancia, en todas sus diversas formas.

Volviendo a las dos preguntas anteriores, es fundamental subrayar nuevamente el objetivo real y concreto de la formación en el ámbito de la concienciación sobre la ciberseguridad: **generar conciencia sobre** las **amenazas cibernéticas** para transformar el comportamiento de todas las personas, especialmente de quienes que no tienen ningún conocimiento o especialización en el ámbito cibernético, considerado desde siempre como un ámbito tecnológico.



Para transformar los comportamientos de los usuarios digitales, adaptándolos al nivel actual y futuro de las amenazas, no es suficiente actuar con un modelo didáctico, sino que es necesario incidir también desde el punto de vista perceptivo.

El usuario debe adoptar cultivar una **actitud capaz de reconocer los peligros**, desarrollando un nivel decente de resiliencia, para que este tipo de instinto pueda adaptarse constantemente a la evolución continua de las estrategias de ataque.
En el plano digital, por tanto, debemos ayudar a los usuarios a desarrollar ese nivel de percepción del peligro, que en la vida cotidiana nos libra de muchas amenazas que nos rodean.

Por estas razones, una **formación intensiva** y **concentrada** solo tendrá un efecto efímero y será eficaz en el corto plazo, ya que, por su propia naturaleza, tenderá a evaporarse inevitablemente a lo largo del tiempo.
En cambio, utilizar un enfoque «homeopático», con pequeñas intervenciones repartidas a lo largo del tiempo, te permite mantener la dimensión perceptiva en un nivel adecuado y también actualizar la dimensión memorista, manteniéndola siempre a la altura de los desarrollos del tema. Puesto que las amenazas cibernéticas cambian constantemente, adoptando formas cada vez más sofisticadas, que las diferencian de su forma original, es crucial continuar inoculando pequeñas dosis de «vacuna» en las personas, para hacerlas inmunes a sus múltiples formas.

PERO, ¿QUÉ CANTIDAD DE TIEMPO ES ACEPTABLE DEDICAR A ESTE TIPO DE FORMACIÓN?

¿CUÁL ES EL PUNTO DE EQUILIBRIO ENTRE EL RESULTADO OBTENIDO Y EL IMPACTO PRODUCIDO?

La experiencia adquirida nos ha demostrado cómo una dedicación de 20 a 30 minutos al mes, con una modularidad que permite dividir este compromiso en sesiones formativas autoconsistentes que no superan los 10 minutos, es compatible con cualquier tipo de exigencia laboral, eliminando cualquier potencial bloqueo debido a una sobrecarga de tipo cognitivo.

Muchos cursos intensivos y concentrados, como el de seguridad laboral (ley 81/2008) o los cursos relacionados con la introducción del RGPD (Reglamento General de Protección de Datos), han producido a lo largo de los años una especie de rechazo por parte de todos los empleados: un error que debe evitarse por todos los medios.
En el siguiente párrafo veremos cómo un modelo de formación continua, incluso de bajo impacto en la plantilla, debe servirse de técnicas que hagan al usuario implicarse, para que se sienta motivado a participar en favor de la calidad de los contenidos recibidos de y los beneficios obtenidos.

2.5 **INTERVENCIÓN FORMATIVA**

RESUMEN

Un **curso eficaz** debe ser extremadamente **atractivo** y, por tanto, no percibido según una mera lógica «impositiva». La intervención depende mucho de los idiomas y formatos, pero también de la capacidad de transmitir el beneficio individual que obtiene el participante, una suerte de retorno importante asociado a su compromiso. Esto no quiere decir que una formación de este tipo no pueda ser obligatoria, pero los requisitos obligatorios nunca deben usarse como excusa para no usar criterios eficaces de «compromiso».

UN PROGRAMA QUE BUSQUE SER EFICAZ DEBE SER ATRACTIVO PARA EL PARTICIPANTE, Y GENERAR EN ÉL UN NIVEL SUFICIENTE DE «ENGAGEMENT». PARA INVOLUCRAR AL USUARIO EN UN TEMA APARENTEMENTE «HOSTIL», ERRÓNEAMENTE CONSIDERADO COMO EXCLUSIVO DEL PERSONAL ESPECIALIZADO, ES NECESARIO SUPERAR EL PREJUICIO INSTINTIVO DE QUIEN, NO SIENDO TÉCNICO, NO LOGRA ENCONTRARLE UNA JUSTIFICACIÓN.

Lo primero que hay que tener en cuenta es el lenguaje y las formas expresivas empleadas. Estamos acostumbrados a pensar que la formación empresarial debe caracterizarse por la «pesadez» de los contenidos y las formas de expresión.

Basándonos en los cánones de la formación tradicional, correríamos el riesgo, sobre una temática cuyo objeto son las amenazas cibernéticas y las consecuencias que estas pueden generar, de caer en el alarmismo y en el tecnicismo, y de inducir una situación de rechazo.

PARA ALCANZAR EL OBJETIVO DE LA CONCIENCIACIÓN SOBRE LA CIBERSEGURIDAD, EL **LENGUAJE UTILIZADO** DEBE SER **ALTAMENTE DIVULGATIVO**, Y **COMPRENSIBLE** PARA TODO EL MUNDO. UN LENGUAJE QUE EXPLIQUE CON CLARIDAD QUE NO SE TRATA DE UNA MATERIA DE CARÁCTER TÉCNICO, SINO DE UNA **MATERIA** QUE **AFECTA A LA VIDA COTIDIANA** Y A TODA PERSONA QUE INTERACTÚE CON LA ESFERA DIGITAL.

Todo efecto barrera preventivo debe derrumbarse desde el principio, para dejar paso a una clara percepción de la utilidad de la intervención formativa y de la posibilidad de poder disfrutar plenamente de ella, independientemente de las propias competencias.

Las formas expresivas deben inspirarse inevitablemente en los principios del aprendizaje multimedia y caracterizarse por una gran interactividad. El aspecto moderno y atractivo nunca deberá «sobrecargarse» con un uso excesivo de animaciones, que deben guardar el equilibrio con el elemento humano. La función de «coaching», por tanto, seguirá interpretándola el elemento humano para favorecer el proceso de identificación basado en el canon docente/alumno.

La concienciación sobre la ciberseguridad es una inversión en el factor humano y esta connotación también debe reflejarse en el programa formativo. La interactividad asume una relevancia concreta en la lógica de una alternancia continua entre breves contenidos formativos y pruebas de aprendizaje que sirven para reforzar la comprensión del contenido, siguiendo la lógica de la exención universitaria, más que la lógica del examen final. Otra forma de implicación tiene que ver con el beneficio que se obtiene de una formación, de lo que podemos llamar la «palanca individual».

Es fundamental que el participante comprenda desde las primeras lecciones que el beneficio principal de la concienciación sobre la ciberseguridad es para el individuo y su red social, antes que para su organización. Esta convicción mitigará el carácter impositivo de la propia formación y la idea de que solo se requiere para proteger a la organización de posibles consecuencias.

Solo al percibir este tipo de beneficio, la participación será total y el estímulo para mantener actualizado el nivel de conciencia sobre los ataques cibernéticos será automático. Esta sensación de implicación espontánea se percibirá aún más si el proceso de identificación se potencia con la referencia continua a casos y situaciones reales, en los que es fácil reconocerse.

A menudo, a la hora de iniciar un recorrido de este tipo, la pregunta que más se plantean los responsables internos es si esta formación debe catalogarse como obligatoria o si debe centrarse sobre todo en la implicación de las personas. Honestamente, no hay una respuesta única a esta pregunta, porque cada organización tiene sus propias dinámicas.

Es indudable que el máximo de eficacia se obtiene combinando estos dos tipos de palancas: la de la obligatoriedad y la de la implicación.

SI ES CIERTO QUE LA OBLIGATORIEDAD DE UN PROGRAMA DE FORMACIÓN SE PUEDE PERCIBIR NEGATIVAMENTE COMO UNA IMPOSICIÓN, TAMBIÉN ES CIERTO, Y LA EXPERIENCIA ADQUIRIDA LO CONFIRMA, QUE LA NO OBLIGATORIEDAD SE PUEDE CONSIDERAR SINÓNIMO DE «POCO IMPORTANTE». POR ESTA RAZÓN, LA MÁXIMA EFICACIA SE OBTIENE CUANDO LA OBLIGACIÓN Y LA PARTICIPACIÓN COEXISTEN DE MANERA EQUILIBRADA.

2.6 **LUDIFICACIÓN**

RESUMEN

El juego es quizás el más poderoso de los elementos que generan implicación en la formación empresarial. Las formas de ludificación individual, con el otorgamiento de reconocimientos virtuales y grupales, y con el desarrollo de una sana competencia entre diferentes equipos, fortalecen los procesos de aprendizaje y también repercuten positivamente en el juego en equipo.

YA SE SABE, Y DESDE HACE MUCHO TIEMPO, QUE EL JUEGO ES UNA HERRAMIENTA QUE FACILITA LOS PROCESOS DE APRENDIZAJE, ASÍ COMO HAY EVIDENCIA DE QUE LAS TÉCNICAS DE LUDIFICACIÓN APLICADAS A LA FORMACIÓN EMPRESARIAL INCREMENTAN LA EFICACIA DE LA FORMACIÓN, AL AFECTAR POSITIVAMENTE A LA PARTICIPACIÓN DESDE UN PUNTO DE VISTA CUANTITATIVO Y DESDE UN PUNTO DE VISTA CUALITATIVO. ESTO ES AÚN MÁS VÁLIDO CUANDO HABLAMOS DE FORMACIÓN A DISTANCIA.

Las **técnicas** de **ludificación**, al añadir elementos motivacionales, refuerzan el nivel de implicación en el recorrido formativo, algo que, como hemos visto, representa un paso fundamental para obtener un resultado eficaz.

La ludificación puede actuar en el **plano individual**, gracias a elementos de gratificación virtuales, como la adquisición de insignias, medallas, copas, etc., que marcan todos los pasos importantes del recorrido formativo y premian el compromiso del participante. La ludificación también puede actuar en el plano grupal, **aprovechando** así el sentido de pertenencia y el juego en equipo.

Pertenecer a un equipo y, en este sentido, activar el mecanismo de sana competencia con otros equipos, genera niveles elevados de implicación y una mayor capacidad para desarrollar procesos de comunicación interna generalizados.

LAS TÉCNICAS DE LUDIFICACIÓN Y, POR TANTO, LA CAPACIDAD DE CONVERTIR EL NIVEL DE USO DEL RECORRIDO FORMATIVO EN UNA PUNTUACIÓN, AYUDAN TANTO A LOS PARTICIPANTES COMO A LOS SUPERVISORES A CONOCER DE INMEDIATO LOS PROGRESOS ALCANZADOS EN EL APRENDIZAJE, Y PROPORCIONA ELEMENTOS CONCRETOS PARA EFECTUAR LA EVALUACIÓN DE LOS RESULTADOS.

2.7 **COMPROMISO**

RESUMEN

El nivel de compromiso dentro de la organización y la atención de la alta dirección son factores decisivos, especialmente en comparación con una iniciativa que se caracteriza por su transversalidad y por la criticidad del tema tratado.

EN EL ÁMBITO DE LA FORMACIÓN EMPRESARIAL, LA EFICACIA SE VE CLARAMENTE FAVORECIDA TAMBIÉN POR EL NIVEL DE COMPROMISO Y DE IMPLICACIÓN DE LAS ESTRUCTURAS EMPRESARIALES.
LA ATENCIÓN DE LA ALTA DIRECCIÓN SOBRE UNA INICIATIVA TAN TRANSVERSAL SE CONVIERTE EN UN FACTOR CRÍTICO DE ÉXITO DE LA PROPIA INICIATIVA.

Ya hemos señalado que el riesgo cibernético es, de hecho, un riesgo empresarial, al igual que otros, por lo que es obvio que reducir la amenaza de este riesgo debe ser un objetivo de toda la organización y no solo de los departamentos de TI/SEC.

La implicación de las estructuras de RR. HH., de la Comunicación Interna, con la activación de todos los canales de comunicación, como por ejemplo la Intranet, es fundamental para favorecer el éxito de la iniciativa y para que siga adelante con el tiempo.

LA EXPERIENCIA HA DEMOSTRADO QUE, CUANDO EL COMPROMISO ALCANZA AL LLAMADO «C-LEVEL», LAS BARRERAS QUE FRENAN LA PARTICIPACIÓN Y LA IMPLICACIÓN SE DERRUMBAN Y LA EFICACIA DE LA FORMACIÓN AUMENTA CONSIDERABLEMENTE.

3. CYBER GURU
3.1 **LA PLATAFORMA DE SEGURIDAD**

RESUMEN

Cyber Guru es la primera línea de soluciones de concienciación sobre ciberseguridad diseñada para aumentar el nivel de seguridad de las personas y las organizaciones. Una plataforma capaz de actuar eficazmente sobre el factor humano gracias a una metodología innovadora que mejora los procesos de aprendizaje.

LA PLATAFORMA CYBER GURU, DISEÑADA EN ITALIA, SE BASA EN METODOLOGÍAS DE FORMACIÓN QUE SON EL FRUTO DE UN TRABAJO MULTIDISCIPLINAR, QUE, CON EL TIEMPO, SE HA BENEFICIADO TAMBIÉN DE LA COLABORACIÓN DEL DEPARTAMENTO DE CIENCIAS DE LA FORMACIÓN DE LA UNIVERSIDAD DE ROMA TRE.

Todas las soluciones de la plataforma Cyber Guru permiten lograr dos objetivos principales:

- **AUMENTAR LA CONCIENCIACIÓN (AWARENESS) DE LAS PERSONAS RESPECTO A LOS RIESGOS QUE SE CORREN CUANDO SE INTERACTÚA CON LAS TECNOLOGÍAS DIGITALES Y CON LA WEB;**
- **INFLUIR EN EL COMPORTAMIENTO DE LAS PERSONAS PARA ADAPTARLO A LAS NECESIDADES DE PROTECCIÓN DE LAS ORGANIZACIONES Y A LOS RETOS QUE PLANTEA LA EVOLUCIÓN DE LA CIBERDELINCUENCIA.**

Para alcanzar estos objetivos, el diseño y desarrollo de las plataformas ha seguido unas líneas metodológicas precisas, que tienen en cuenta la necesidad de actuar de forma eficaz sobre los procesos de aprendizaje.

LA METODOLOGÍA SE ARTICULA EN 3 NIVELES DE FORMACIÓN:

FORMACIÓN DIDÁCTICA

APRENDIZAJE EXPERIENCIAL

FORMACIÓN INDUCTIVA

ADEMÁS, LA METODOLOGÍA, QUE ES LA BASE DE CYBER GURU, TIENE EN CUENTA OTROS DOS ASPECTOS DETERMINANTES:

- Un proceso de formación continua, constituido por microintervenciones efectuadas con constancia y regularidad.
- La participación del usuario en este proceso, dejando claro al propio usuario que el objetivo principal del proceso es su protección, como individuo insertado en un contexto social cada vez más interconectado.

TODO ESTO SIRVE PARA DESARROLLAR, CONSTANTE Y PROGRESIVAMENTE, TRES CARACTERÍSTICAS QUE INFLUYEN EN LOS COMPORTAMIENTOS HUMANOS CUANDO LAS PERSONAS SE VEN AMENAZADAS, GENERANDO LA CAPACIDAD DE REACCIONAR CORRECTAMENTE PARA PROTEGERNOS A NOSOTROS MISMOS Y A NUESTRA ORGANIZACIÓN:

CONOCIMIENTO
ACCIÓN RACIONAL

PERCEPCIÓN
ACCIÓN INSTINTIVA

PRONTITUD
ACCIÓN INMEDIATA

3.2 CYBER GURU AWARENESS

RESUMEN

Cyber Guru Awareness es un innovador sistema integrado de «e-learning» que permite involucrar a toda la organización en un recorrido de formación basado en una metodología de formación continua y en la aplicación de técnicas de juego a todo el recorrido formativo.

Cyber Guru Awareness se ha diseñado para que toda la organización participe en un itinerario de aprendizaje educativo y estimulante que se caracteriza por su enfoque de «desarrollo constante y gradual» y algunas características únicas:

- MÓDULOS FORMATIVOS AUTOCONSISTENTES DE ACTIVACIÓN MENSUAL;
- COMPROMISO MÍNIMO SEMANAL, COMPATIBLE CON CUALQUIER FUNCIÓN;
- MICROLECCIONES EN VÍDEO EN FORMATO MULTIMEDIA;
- USO DE ACTORES PROFESIONALES CON FUNCIONES DE «COACH»;
- LENGUAJE ALTAMENTE DIVULGATIVO;
- ENFOQUE INTERACTIVO CON ALTERNANCIA CONTINUA ENTRE MICROLECCIONES Y PRUEBAS;
- TEST DE EVALUACIÓN DE RESPUESTA MÚLTIPLE;
- METODOLOGÍA DE LUDIFICACIÓN, CON ORGANIZACIÓN EN EQUIPOS;
- PLATAFORMA MULTILINGÜE;
- CONTENIDOS ADICIONALES Y CONSTANTEMENTE ACTUALIZADOS.

El **recorrido formativo** de **Cyber Guru Awareness** consta de **módulos de formación autoconsistentes**, cada uno dedicado a un tema específico, con activación mensual para un periodo de 12, 24 o 36 **meses**.
Cada módulo consta a su vez de **3 breves lecciones en vídeo** de **5 minutos cada una**, todas ellas asociadas a un **test** de aprendizaje con **preguntas** de **opción múltiple.**
La lección en vídeo, con el **actor «coach»** es el elemento básico del recorrido formativo, ya que permite implicar activamente al usuario en este itinerario de la mano de la ludificación.

Los mecanismos de gamificación se han estructurado para alcanzar el máximo nivel de implicación tanto del individuo como de la organización, favoreciendo la activación de procesos de comunicación interna, siguiendo también una lógica de **«team building».**

LA LUDIFICACIÓN SE ESTRUCTURA:

- **DE FORMA INDIVIDUAL,** CON LA ASIGNACIÓN DE MEDALLAS Y COPAS VIRTUALES QUE PREMIAN LA PARTICIPACIÓN DEL USUARIO, INCLUSO DESDE EL PUNTO DE VISTA CUALITATIVO;
- **DE FORMA AGREGADA,** CON UNA ORGANIZACIÓN EN EQUIPO QUE PERMITE GENERAR UNA SANA COMPETENCIA ENTRE DIFERENTES EQUIPOS, UN MECANISMO PARTICULARMENTE MOTIVADOR QUE APROVECHA LAS LÓGICAS DE PERTENENCIA.

Cyber Guru Awareness, con el fin de aumentar la participación del usuario, sin dar trabajo a quien dirige la formación, pone a disposición la función automática Student Caring, que se ocupa de estimular la participación, a través de notificaciones puntuales.

3.3 CYBER GURU PHISHING

RESUMEN

Cyber Guru Phishing es una innovadora plataforma de entrenamiento antiphishing, basada en una metodología de aprendizaje experiencial. El objetivo de Cyber Guru Phishing es maximizar la eficacia formativa frente al riesgo de «phishing»: percepción del peligro, prontitud para reaccionar ante el ataque y conocimiento de la amenaza.

CYBER GURU PHISHING SE HA DISEÑADO PARA QUE LA PLANTILLA ENTRENE CÓMO RESISTIR ATAQUES DE «PHISHING», A TRAVÉS DE CAMPAÑAS DE ATAQUES SIMULADOS, QUE SE PERSONALIZAN SEGÚN EL PERFIL DE COMPORTAMIENTO DE CADA USUARIO, GRACIAS A UN PROCESO AUTOMÁTICO Y ADAPTATIVO, GUIADO POR EL USO DE TÉCNICAS DE INTELIGENCIA ARTIFICIAL.

Gracias a su enfoque adaptativo, Cyber Guru Phishing puede considerarse un verdadero «entrenador personal» en la función antiphishing.

Las campañas de simulación reproducen la experiencia real y las estrategias de ataque adoptadas por los ciberdelincuentes. Los algoritmos de aprendizaje utilizados por la plataforma son capaces de seleccionar plantillas de ataque basándose en un criterio de máxima eficacia formativa.

En cada campaña, el motor adaptativo elige las nuevas plantillas en función del perfil de usuario, aumentando, por ejemplo, el nivel de dificultad de los ataques, para los usuarios clasificados como «fuertes».

La plataforma sigue el siguiente esquema de funcionamiento:

1. CON CADA CAMPAÑA, LA PLATAFORMA SELECCIONA AUTOMÁTICAMENTE LAS PLANTILLAS DE ATAQUE Y LAS PONE A DISPOSICIÓN PARA SU APROBACIÓN.

2. LA PLATAFORMA DISTRIBUYE LOS ATAQUES SEGÚN UN ESQUEMA PERSONALIZADO Y CON UN MECANISMO QUE EVITA EL FENÓMENO DEL BOCA A BOCA.

3. TODO AQUEL QUE CAE EN EL ENGAÑO SE EXPONE A UN ENTRENAMIENTO ESPECIALIZADO SEGÚN EL ATAQUE SUFRIDO, ALGO QUE REFUERZA EL MÉTODO DE APRENDIZAJE EXPERIENCIAL.

4. LOS EFECTOS DE CADA CAMPAÑA PERMITEN VALORAR LOS INDICADORES DE RIESGO MONITORIZADOS POR LA PLATAFORMA, PARA DETERMINAR LA PREPARACIÓN Y LA DISTRIBUCIÓN DE LA SIGUIENTE CAMPAÑA.

5. ADEMÁS DE LA CLASIFICACIÓN DE LOS USUARIOS EN «DÉBILES», «INTERMEDIOS» Y «FUERTES», LA PLATAFORMA PERMITE VALORAR TAMBIÉN LA CATEGORÍA DEFINIDA DE LOS «DEFENSORES» ES DECIR, DE AQUELLOS QUE, ADEMÁS DE NO CAER EN EL ENGAÑO, RECONOCEN EL ATAQUE Y LO SEÑALAN.

6. TODOS LOS INDICADORES SIRVEN PARA ALIMENTAR LA FUNCIÓN DE INFORMES EN TIEMPO REAL, QUE SE EMPLEAN A TRAVÉS DE UN CUADRO DE MANDOS AVANZADO.

Los informes no se limitan a exponer la tasa de clics de una campaña, sino que ponen a disposición informes e indicadores que dibujan un mapa claro del riesgo y la eficacia real del recorrido emprendido.

El aprendizaje experiencial, alcanzado a través de Cyber Guru Phishing, demuestra ser particularmente efectivo para reducir el riesgo de «phishing», al aumentar constantemente el nivel de resistencia a los ataques cibernéticos de toda la organización y reducir con igual regularidad el número de usuarios clasificados como «débiles».

Esta metodología de aprendizaje está respaldada por las características de la plataforma, especialmente por su nivel de automatización, que minimiza el impacto en los equipos de ciberseguridad.

3.4 CYBER GURU CHANNEL

RESUMEN

Cyber Guru Channel es un curso de formación en vídeo basado en una metodología inductiva, realizado con técnicas de producción avanzadas, típicas de las series de televisión, y con una narrativa atractiva, diseñado para sumergir al usuario en situaciones reales que reproducen las consecuencias de un ataque cibernético generado por un comportamiento humano erróneo.

La metodología inductiva implementada por Cyber Guru Channel se basa en la inmersión del usuario en una situación real y en un proceso de autoidentificación con la ciberamenaza, que adopta una forma concreta y, por tanto, posible.

El usuario toma conciencia a través de una narración, que actúa, primero, sobre la percepción del peligro y, posteriormente, sobre el elemento memorista, en vez de a través de una noción.

El elemento memorista se «infiere» de la propia narrativa y se refuerza con el material de profundización puesto a disposición del usuario.

Los vídeos de la plataforma de Cyber Guru Channel se han realizado con técnicas de producción avanzadas y con una narrativa particularmente atractiva.

En este recorrido en particular, en el que la participación en una historia es la clave para comprender el tema, el usuario cuenta también, dentro de la plataforma, con el apoyo del material necesario disponible para profundizar, que proporciona las bases teóricas para aumentar su propio nivel de conciencia sobre la amenaza presentada en la historia.

CYBER GURU CHANNEL INCLUYE:

- **MÁS FORMATOS DE VÍDEO CON DISTINTAS HISTORIAS;**
- **DOCUMENTACIÓN DE PROFUNDIZACIÓN PARA CADA EPISODIO;**

- **INTEGRACIÓN CON EL MECANISMO DE GAMIFICACIÓN.**
- **FUNCIONES DE STUDENT CARING, PARA MOTIVAR LA PARTICIPACIÓN;**
- **INFORMES AVANZADOS SOBRE EL NIVEL DE APROVECHAMIENTO**

El nivel de compromiso generado por Cyber Guru Channel es muy alto y, por ello, resulta una base fundamental para otros cursos de formación destinados a concienciar sobre la ciberseguridad y para actividades de comunicación interna destinadas a difundir la cultura de la ciberseguridad en la organización.

Los vídeos formativos, integrados en la plataforma Cyber Guru, se enriquecen con los componentes de control del acceso, interacción y supervisión de la plataforma.


Cyber
Guru

WWW.CYBERGURU.IT