Cómo estructuro una charla de ciberseguridad para que realmente impacte

No se trata de asustar a la gente. Se trata de que salgan pensando diferente.

Meta descripción: Descubre cómo estructurar una charla de ciberseguridad que conecte de verdad con cualquier audiencia, desde jóvenes hasta empresarios. (152 caracteres)

Hay una imagen que tengo muy grabada. Primer día en Córdoba, tres charlas seguidas en un instituto, yo con poco más de una experiencia previa en Lanzarote y un guión en la cabeza que rezaba para no olvidar. Entré con el estómago encogido. Salí con algo que no esperaba: la sensación de que había pasado algo real en esa sala. Los chavales hacían preguntas, se formaban debates espontáneos, algunos se quedaron después con dudas concretas. No fue perfecto, pero funcionó. Y desde entonces llevo pensando en por qué funcionó.

Este artículo es para centros educativos, institutos, escuelas de negocio y empresas que se preguntan qué diferencia a una charla de ciberseguridad que realmente deja huella de una que simplemente rellena un hueco en el calendario.

El problema real de las charlas de ciberseguridad

La mayoría de ponencias de ciberseguridad cometen el mismo error: hablan *sobre* los riesgos en lugar de hacer que la audiencia los *sienta*. Presentan estadísticas, mencionan conceptos como phishing o ransomware, muestran algún titular alarmante y terminan con una lista de consejos que nadie va a aplicar la semana siguiente.

El resultado es predecible. La gente asiente, aplaude por educación y dos días después sigue usando "123456" como contraseña.

El problema no es la ciberseguridad. Es cómo se cuenta.

Después de seis charlas en ciudades como Lanzarote, Córdoba y Toledo, y de haber participado en más de diez actividades relacionadas con emprendimiento y ciberseguridad —talleres, incubadoras, ponencias para empresarios—, he llegado a una conclusión clara: la audiencia no necesita más información, necesita un cambio de perspectiva. Y ese cambio solo ocurre cuando la charla se diseña para provocarlo, no para rellenarlo.

El primer paso es conocer a quién tienes delante

No es lo mismo hablar a un grupo de adolescentes en un FP que a un panel de empresarios con veinte años de negocio a sus espaldas. Y he tenido la suerte —o el reto— de haber hecho ambas cosas.

Con los jóvenes, el desafío principal es la vergüenza. No la ignorancia, sino la vergüenza de participar, de levantar la mano, de admitir que no saben algo. En cuanto consigues romper esa barrera —normalmente con una pregunta directa, sin juzgar, que les invite a opinar— la sala cambia completamente. Se vuelven curiosos, se sorprenden, preguntan cosas que ningún adulto preguntaría porque los adultos ya "deberían saberlo".

Con los empresarios ocurre lo contrario. Están acostumbrados a hablar, a debatir, a cuestionar. Las preguntas son más técnicas y más concretas. He tenido empresarios preguntarme qué pueden hacer si ya han pagado un rescate por un ataque de ransomware. Esa pregunta no tiene una respuesta bonita, pero sí tiene una respuesta honesta. Y eso es exactamente lo que esperan: que no les vendas humo.

El primer trabajo antes de diseñar cualquier charla es hacerse esa pregunta incómoda: ¿qué sabe esta audiencia, qué le preocupa y qué no sabe que debería preocuparle?

La estructura que a mí me funciona

No existe una fórmula universal, pero sí hay una lógica que se repite en mis mejores charlas.

Empiezo por mí. No por los datos ni por las amenazas. Primero me presento, cuento de dónde vengo, qué hace la empresa en la que trabajo, por qué estoy ahí ese día. Esos primeros dos minutos son los más importantes de toda la charla porque determinan si la gente decide escucharte o no. Nadie escucha a alguien en quien no confía.

Después, el anzuelo. Un caso real. Siempre. No un caso inventado, no una estadística genérica. Un caso concreto, con nombres cambiados si hace falta, pero con detalles reales que hagan pensar "esto le podría pasar a alguien que conozco". La ingeniería social —esa capacidad que tienen los atacantes de manipular la psicología humana para obtener lo que quieren— es mucho más fácil de entender cuando la ves aplicada a una situación cotidiana que cuando te la explican en abstracto.

Luego, el concepto. Una vez que la audiencia ya está enganchada emocionalmente, introduzco los términos técnicos. Phishing, OSINT, ransomware, ingeniería social. Pero explicados desde el ejemplo, no al revés. Primero el "esto pasó", después el "esto se llama así y funciona de esta manera". El orden importa más de lo que parece.

Y entonces, la práctica. En las charlas de Córdoba hacíamos un ejercicio en directo: crear una contraseña segura siguiendo unos criterios concretos, y luego evaluábamos entre todos cuáles eran las más robustas. Suena simple, pero el efecto es poderoso. La gente no olvida lo que hace; sí olvida lo que escucha.

El cierre, reflexivo y sin catastrofismo. Mi frase de referencia al terminar casi siempre gira en torno a la misma idea: el primer paso para mejorar tu ciberseguridad es aprender a dudar de todo lo que ves en el mundo online. No te pido que desconfíes de las personas, te pido que desarrolles un criterio propio antes de hacer clic, de compartir, de pagar. Eso no es paranoia. Es cultura digital.

Lo que he aprendido que nadie te dice

La improvisación no es lo contrario de la preparación. Es su consecuencia. Cuando dominas el tema, puedes salirte del guión porque el guión ya está dentro de ti. Las mejores

intervenciones que he tenido no fueron las más planificadas al milímetro, sino las que surgieron de una pregunta inesperada que me llevó a un terreno no previsto y en el que aun así me sentía seguro.

El feedback duele, pero es el mejor recurso que tienes. Me han dicho que repito demasiado ciertos términos. Me han pedido más herramientas concretas y prácticas. Esas críticas, leídas con honestidad, son las que definen la siguiente versión de tu charla.

Y hay algo que me frustra del panorama actual de la divulgación en ciberseguridad, especialmente en entornos educativos: seguimos queriendo prohibir la tecnología en lugar de enseñar a usarla bien. Quitarle el móvil a un adolescente no le enseña nada sobre cómo funciona el mundo digital en el que va a vivir. Darle herramientas para entenderlo, sí.

Por qué esto importa si estás pensando en contratar una charla

Si representas a un centro educativo, a una empresa o a una organización que está valorando invertir en formación sobre ciberseguridad, la pregunta correcta no es "¿cuánto cuesta?" sino "¿qué va a cambiar en mi equipo o en mis alumnos después de esta charla?"

Una buena charla de ciberseguridad no es un trámite. No es el PowerPoint que hay que pasar para cumplir con el protocolo. Es una oportunidad real de instalar un criterio nuevo en personas que toman decisiones digitales todos los días: jóvenes que comparten datos sin pensarlo, empleados que abren adjuntos sin verificar, directivos que no tienen un plan ante un incidente.

El impacto no se mide en aplausos. Se mide en si alguien, tres semanas después, duda antes de hacer clic en un enlace sospechoso.

Reflexión final

Llevas tiempo pensando en la ciberseguridad como algo técnico, como algo de informáticos o de empresas grandes. Pero cada vez que un adolescente publica su ubicación en tiempo real, cada vez que una pyme no tiene copias de seguridad, cada vez que alguien paga con su tarjeta en una red WiFi pública sin pensarlo, la ciberseguridad deja de ser un tema técnico y se convierte en algo muy humano.

Por eso las charlas importan. Por eso el cómo se cuentan las cosas importa todavía más.

Isaac Ruiz Romero.