COMPARECENCIA DEL SOCIO DIRECTOR DE S2 GRUPO, DON JOSÉ MIGUEL ROSELL TEJADA, EN LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES CELEBRADA EL DÍA 4 DE NOVIEMBRE DE 2013.

El señor **SOCIO DIRECTOR DE S2 GRUPO** (Rosell Tejada): Mientras tanto, ante todo muchas gracias por invitarme a compartir con ustedes lo que sé sobre este tema, que seguro que con el tiempo que llevan ustedes ya estudiando todo esto, mucha más información e incluso muchos más datos van a tener ustedes en algunos sentidos.

Yo voy a cambiar un poco el tercio respecto al anterior ponente. Soy técnico, soy ingeniero, no soy abogado, y por tanto no voy a hablar de leyes, voy a darles un punto de vista técnico de una empresa, como verán, que se dedica a trabajar en los temas de seguridad y ciberseguridad. Para lo cual, como técnico que soy, voy a hacer uso de los medios que tengo, que me han puesto ustedes a mi disposición, y voy a utilizar una presentación que me va a permitir enseñarles incluso algunas cosas que yo creo que son interesantes y que pueden ser de su interés.

Para empezar, quiero empezar con una idea que voy a repetir varias veces a lo largo de la ponencia: y es que yo creo que el tema sobre el que estamos hablando, la situación de riesgo de los jóvenes no es el problema, para mí es una consecuencia. El problema en realidad somos nosotros. El problema es que falta una cultura en la sociedad sobre temas de ciberseguridad, digamos que falta una cultura mínima básica. Y el problema por tanto, como bien digo o como creo, somos nosotros y no los menores.

En cualquier caso, permítanme que les dé dos *flashes* de quién soy y a quién represento. Como les decía, soy director general de una empresa de

seguridad, aparte de ser padre de dos niñas y de haberme, si me permiten la expresión, comido este problema durante los últimos seis o siete años en primera persona, y por tanto hablo como experto en la materia desde un punto de vista técnico y como padre de dos hijas que son usuarias intensivas de las redes sociales.

S2 Grupo es una empresa técnica especializada en temas de ciberseguridad; no tocamos la seguridad física, solo temas de seguridad desde el punto de vista informático o tecnológico. Somos una empresa de unas 115 personas que actualmente estamos trabajando en distintas áreas para nuestros clientes, fundamentalmente en tres líneas de negocio, para que sepan ustedes de qué es de lo que puedo saber y de qué no. Trabajamos en proyectos de consultoría y auditoría para clientes, sobre todo para cuentas de tamaño medio y grande, que son las que en este momento están desarrollando mucho trabajo en materia de ciberseguridad. Tenemos un centro de servicios que presta servicio a nuestros clientes en formato 24 x 7, vigilando sus negocios y sus redes. Y además estamos desarrollando desde hace ya varios años productos de tecnología nacional para implantar en los clientes en los que estamos trabajando.

Evidentemente, no solo por eso creo que estamos aquí. Realmente nosotros estamos aquí porque desde hace ya algunos años (por ejemplo, la semana pasada nos dio el distintivo de igualdad la ministra de Sanidad), al margen de haber hecho determinado tipo de cosas internas en materia de responsabilidad social, llevamos mucho tiempo trabajando (por una historia que luego les contaré) en temas de seguridad y menores. Y en los temas, digamos, sociales hemos invertido mucho tiempo y mucha imaginación, como luego verán, en ver qué es lo que podíamos nosotros hacer para intentar poner nuestro granito de arena a la hora de resolver este problema.

Por este motivo pienso que el tema de la ponencia, estudio sobre los riesgos derivados del uso de la red por parte de menores, es un tema que a

mí particularmente y a nuestra empresa nos es familiar; hemos trabajado mucho, como verán, en todo ello. Y me gustaría empezar con una frase del señor Churchill, de Winston Churchill, que siempre me ha llamado mucho la atención, que pronunció en un discurso en la Cámara de los Comunes en el año 1943, hablando de la reconstrucción de algunos edificios emblemáticos de Londres, y decía: "Nosotros damos forma a nuestros edificios y después nuestros edificios nos dan forma a nosotros". Es una frase que a la hora de hablar de la red y de lo que estamos viviendo ahora, de la sociedad en la que estamos viviendo ahora, es perfectamente válida. De hecho, nosotros en el año 1969 vimos el nacimiento de lo que fue en aquel momento ARPANET en unas universidades americanas, con la comunicación de cuatro ordenadores (estamos hablando del año 1969). Del año 1969 en adelante, la verdad es que la evolución fue muy lenta. Fueron pasando algunas cosas significativas; por ejemplo, William Gibson, en el año 1981 acuñó el término "ciberespacio" en una novela que se llamaba *Johnny Mnemonic*, muy interesante sobre todo para entender la evolución de Internet o del ciberespacio fundamentalmente.

En el año 1983 vivimos el nacimiento de verdad de Internet, cuando se cambió de tecnología de comunicaciones antigua a lo que hoy es TCP, con lo cual en el año 1983, el 1 de enero de 1983 es cuando se data realmente el nacimiento de Internet tal y como lo conocemos.

A partir de ahí en el año 1984, otra vez el señor William Gibson, en una novela bastante famosa de ciencia ficción que se llama *Neuromante*, fue donde popularizó el término "ciberespacio". En la década de los noventa hubo una fiebre generalizada por subir todos los servicios, todo a la red, que acabó con el estallido de la burbuja de las .com en el año 2000. Evidentemente, en el camino quedaron muchas cosas, quedó mucha infraestructura instalada, mucha infraestructura para navegar a alta

velocidad, y quedaron también empresas como Amazon, que no creo que necesiten ninguna presentación.

A partir de ahí, en el año 2004 se creó la primera gran red social, Facebook. Y a partir de 2004, yo creo que la historia ya la conocen ustedes: una locura de redes sociales, de medios, de contenidos en Internet, a través de LinkedIn, de Twitter, de YouTube, de Picasa, un montón de medios disponibles para todas las personas, incluidos los menores, que se han desarrollado en los últimos años.

Bien, al final de todo esto lo que tenemos es el concepto de ciberespacio que el señor Gibson acuñó de una forma, digamos, un poco etérea, que ha ido tomando forma con el nacimiento de Internet y con el desarrollo de las redes sociales. Hasta el punto de que en este momento, en el año 2013, lo hemos conectado todo a Internet, y cuando digo todo es todo, todo o casi todo; estamos en proceso de conexión de todo. En este momento hay quien dice también que si antaño la frontera de las redes eran las máquinas, en este momento hay quien dice que las personas somos el nuevo perímetro. Y el perímetro es lo más accesible, y por tanto lo más vulnerable en determinadas circunstancias.

Aquí quiero ponerles un pequeño ejemplo de un caso. Insisto, somos una empresa técnica, y como tal abordamos la auditoría de muchos equipos, de muchos elementos que tenemos en nuestras casas. Últimamente está de moda, con todos los temas de la eficiencia energética, poner unos cacharritos en casa que son unos cacharritos domóticos que se dedican a analizar el consumo energético y que nosotros desde un móvil podemos acceder a él y podemos ver el consumo energético de nuestra casa, con el fin de apagar una lavadora o lo que sea. Estos cacharros, que aparentemente son inocuos, realmente cuando analizas un poco la seguridad de los dispositivos, te das cuenta de que realmente lo que son es un agujero de seguridad de cara al acceso a las propias redes. No se han

preocupado en diseñar estos dispositivos teniendo en cuenta la seguridad de los mismos, con lo cual al final, claro, la gente te dice "¿y quién va a querer saber la información del consumo de mi casa?". Bueno, realmente la gente que piensa mal, el consumo de una casa yo lo puedo querer saber porque quiero saber cuando una persona está o no en casa, incluso patrones de salida de casa. O incluso, este aparatito que aparentemente es un aparato que me da información de mi consumo energético, realmente lo que acaba dándome es acceso a una red donde hay niños, donde hay personas, donde hay cámaras, donde hay dispositivos dentro de una red interna y mediante los cuales yo puedo obtener información de la familia, de la casa, etc.

Yo he analizado un poco toda la información que han tenido ustedes en las comparecencias anteriores, y me he quedado sobre todo (aparte de un montón de datos que no voy a repetir, y de hecho van a ver que no voy a entrar en estadísticas sobre el uso de la red por parte de menores, porque creo que ya tienen ustedes información suficiente) con dos datos: uno, una frase citada por el director general de la policía, Ignacio Cosidó, que dijo que básicamente ninguna tipología delictiva está creciendo al ritmo al que lo está haciendo la ciberdelincuencia, que además coincide con la introducción de la Estrategia Europea de Ciberseguridad, que viene a decir lo mismo. Y otro es el trabajo excepcional que está haciendo la policía (esto es capturado de hace un par de días) con 637.000 seguidores en el Twitter de la policía, y que incido no en el uso del canal (por lo menos en nuestra empresa tenemos varios canales de Twitter), sino en el cómo lo están haciendo. Es decir, cómo el uso de un canal como el que está utilizando la Policía Nacional, con poca inversión, con poco coste, puede tener la repercusión que está teniendo. Con lo cual incidiré después otra vez en el cómo más que en el qué, cómo vamos a hacer las cosas o cómo podemos hacer las cosas.

En definitiva, lo que en mi opinión es evidente es que tenemos un problema, un problema importante cuyo origen no está en los jóvenes, está en la sociedad. Y sobre esto, insisto, repetiré.

He dicho que no les voy a dar datos de los menores, y no lo voy a hacer. Lo que sí voy a darles es datos de la sociedad en general y algunos –desde aquí, yo soy incapaz de leer, pero creo recordar más o menos lo que pone–, en algún caso, en el primero (esto es de la Estrategia Europea de Ciberseguridad) dice que hay aproximadamente un millón de víctimas diarias de ciberdelitos; el 12% de los usuarios de Internet ha tenido alguna experiencia de fraude *online*; si tenemos 2.000 millones de usuarios, estamos hablando de 240 millones de personas que han sufrido el fraude *online* en los últimos años; el 74% de los usuarios cree que se ha incrementado el riesgo de ser víctima de un ciberdelito. En España –muy importante– el 71% de los ciudadanos no se siente informado (por ejemplo, en Europa es el 59% los que dicen que creen que no tienen información). Importante desde el punto de vista empresarial, y doy fe de ello, el 56,8% de las empresas declara haber tenido algún incidente relacionado con temas de ciberseguridad. Los incidentes de ciberseguridad aumentan en frecuencia y magnitud, y son cada vez más complejos y no tienen fronteras, Cada día hay 150.000 virus en circulación y 148.000 ordenadores son infectados; y según el Foro Económico Mundial, hay entre un 10% y un 20% de probabilidad de que se interrumpan sistemas críticos de información en los próximos diez años, con pérdidas que yo ya no sé si son 250.000 millones de dólares o cuánto es. Lo que quiero decir con esto es que sí, hay muchas cifras sobre los problemas que tienen los menores, y otro montón de ellas sobre los problemas que tenemos como sociedad los adultos y la sociedad en general.

Con lo cual, ¿cuál es la situación? Pues en mi opinión, la situación es que las niñas y los niños, efectivamente, tienen muchos problemas. Las

madres y los padres no se enteran de lo que está ocurriendo. Los adultos también tenemos muchos problemas. El cibecrimen mueve una cantidad de dinero alucinante. Un elevado número de niños ha sufrido acoso por Internet o ha tenido problemas con el uso de las redes sociales. Estamos incluso asistiendo a muertes en el mundo relacionadas con temas de ciberdelincuencia. El problema es que, encima, evoluciona a una velocidad de vértigo: no nos da tiempo a estar al día ni a los que nos dedicamos a esto, es que es casi imposible; y encima, hay una opinión generalizada de que el entorno legislativo no está a la altura de las necesidades, ni mucho menos. Y además tenemos muy pocas herramientas para luchar contra un problema cada vez mayor.

Y aquí quiero hacer mención de un problema, un ejemplo de tantos que podría poner, relacionado con nuestra empresa, que es de lo que puedo fundamentalmente hablar: nosotros somos una empresa de seguridad, tenemos un centro 24 x 7, y vigilamos la infraestructura de seguridad de nuestros clientes; clientes, algunos de ellos importantes, grandes y con manejo de información sensible. Hace poco, el último incidente que hemos tenido (que fue hace, no sé, seis o siete meses) fue un incidente grave; nosotros, cuando tenemos un incidente declaramos una situación de emergencia, formamos un gabinete de crisis, todo en el ciberespacio; y evidentemente, nuestro objetivo en este caso es intentar impedir que los atacantes consigan entrar en nuestros sistemas, porque entonces ponemos en peligro nuestro negocio y el de nuestros clientes. Bien, en este caso tuvimos un incidente que duró tres días. Yo recuerdo uno de los días a las 5 de la mañana sentado en el gabinete de crisis, mirando a mis compañeros que saben de seguridad un montón, con las manos así sin poder hacer absolutamente nada; sabíamos de dónde venía el ataque, es más, sabíamos quién era, porque si quién es un dato y un dato es una dirección IP, sabíamos quién era el que nos estaba atacando; y no podíamos hacer

absolutamente nada. ¿Qué pasó? Pues nada. No paso nada pues porque por suerte conseguimos impedir que estos señores entrasen en nuestros sistemas.

Lo que quiero decir con esto es que realmente no tenemos el equivalente a una ciberpatrulla. De hecho, esto lo denunciamos, sabemos quién es, y ha acabado en los juzgados y ha está siguiendo su proceso, cuatro meses más tarde del incidente. Pero realmente, ¿qué hubiese pasado si estos señores hubiesen conseguido entrar en mis sistemas? Pues hubiéramos tenido un problema, nosotros y nuestros clientes, muy gordo. Realmente estamos atados de pies y manos. No tenemos ni la capacidad de contrarrestar los ataques que nos están haciendo. Con lo cual lo único que podemos hacer es mirar. Y si entran, pues intentar responder.

Por lo tanto, ¿cómo definimos hoy la situación en que nos encontramos? Bueno, para empezar esta situación, desde nuestro punto de vista, y así lo dicen muchos estudios que hemos analizado, es una barrera para el desarrollo de la cibersociedad, es un problema importante con una frontera muy difusa. Yo no tengo claro que el problema sean los menores y que la solución esté en atacar, digamos, el problema que tienen los menores, sino el de la sociedad en su conjunto.

Es un problema que es cambiante, cambia a una velocidad alucinante. De hecho, en los últimos años la velocidad de cambio es cada vez mayor, y además puede llegar a limitar el desarrollo social, y limitarlo mucho; porque el uso de Internet, el uso de las tecnologías es en tanto en cuanto genera confianza; si no hay confianza, al final, evidentemente, la opción será dejar de utilizarlo. Y eso, para la sociedad o para la sociedad en la que nos movemos, yo creo que es sinceramente malo. Con lo cual, en este momento lo que estamos analizando es un problema del que solo podemos ver la punta del iceberg.

Y además, insisto otra vez en la idea: yo creo que el problema somos nosotros. Y además, pensemos en algo que no se está analizando aún, que yo no lo estoy viendo, pero que no les quepa duda de que va a llegar, y es el utilizar a los jóvenes no solo como un fin, el problema del joven, sino como un medio. Es decir, si yo quiero obtener información sensible de una persona, posiblemente, si esta persona está suficientemente concienciada yo no podré atacar directamente a esa persona, pero sí a su familia, y utilizar a los niños en este caso como un medio y no como un fin en sí mismo.

Además, yo creo que deberíamos predicar con el ejemplo, y sinceramente no lo hacemos. En materia de educación vial, que luego volveré a tocar un poco el tema, a los niños les decimos "no se debe conducir hablando por el móvil, circular sin cinturón, cruzar con el semáforo en rojo, saltarnos un stop", etc. Pero nosotros permanentemente pirateamos la Wii de los niños para no pagar los juegos, descargamos todo tipo de contenidos sin saber su procedencia, usamos contraseñas débiles, compartimos las contraseñas con todo hijo de vecino, nos conectamos en cualquier sitio para descargar cualquier información sin un mínimo de precaución, y abrimos cualquier adjunto que nos informa de que hemos ganado el premio de una lotería a la que no hemos jugado siquiera. Entonces, ¿qué les vamos a decir a los niños, qué les podemos transmitir a los niños? Yo creo que el problema lo tenemos nosotros. Y somos nosotros los que tenemos que conseguir, digamos, arreglarlo.

Entonces, antes de entrar en lo que yo les voy a hablar, que es nuestra experiencia y la solución que yo creo que tiene todo esto, me gustaría comentar algunos errores, alguno de los cuales ha salido en la ponencia anterior y que me gustaría comentar.

Desde luego, en esta situación, lo que no es una solución es, como hacen muchos padres, meter la cabeza bajo el ala o debajo de la arena, esto

no es la solución. Pero esta tampoco. Nosotros, en las conferencias que damos (que luego les contaré un poco cuál es nuestra experiencia en esa materia), tenemos padres que se levantan de la silla directamente para ir a arrancar el ADSL de casa y decir "ya está". Esto no es la solución. Claro, esa no es la solución; esta tampoco. Yo pongo un control parental y ya está, un antivirus y ya está: vamos, ni de casualidad. Permítanme recordarles que en los móviles los controles parentales no existen. Y cada vez los niños usan más el móvil para acceder a Internet y a las redes sociales, con lo cual, por mucho que pongamos el control parental en el PC de casa, de poco nos va a servir, de muy poco.

Poner el ordenador en el salón tampoco es la solución. El ordenador es lo de menos; el avance, la evolución de todo esto... el ordenador es un dispositivo por el que los niños... es un cacharro antiguo que ven los niños como un electrodoméstico. Los chavales no utilizan el ordenador para acceder a un montón de información, utilizan los dispositivos móviles.

Prohibir, tampoco, en mi opinión; porque por mucho que prohibamos, se van a casa del vecino o se van a casa del amigo y ya tienen todo lo que tienen en sus manos. Ponerle puertas al campo, en mi opinión, es absolutamente inútil. Por mucho que intentemos regular muchas cosas en España, la red es global, lo queramos o no. Podemos romper la red, podemos quitarla entera. Pero no podemos limitarlo con actuaciones en el entorno de nuestro país. Porque yo les pregunto, yo puedo limitar el contenido de juegos, por ejemplo, que hace la publicidad de las televisiones de aquí, de España: ¿y la televisión mexicana que se ve a través de Internet, con un horario distinto? ¿Qué hacemos con ella? Es difícil. Yo creo que aunque hagamos cosas localmente, la solución tiene que ser global, no puede ser local jamás.

Dicen por ahí: los niños son más vulnerables porque son inocentes. Yo lo siento pero discrepo: no son más vulnerables porque son inocentes.

Los mayores somos inocentes igual que los niños. El problema es que un problema en un niño tiene un mayor impacto, y cuando definimos la vulnerabilidad como la probabilidad de que una amenaza tenga éxito, el problema no es la probabilidad del suceso, es el impacto que sobre un joven tiene. En este caso las pruebas de ingeniería social (de hecho, nosotros hacemos auditorías con auditorías de ingeniería social que es el incidente más grave que tenemos en este momento en la sociedad); la ingeniería social funciona en el cien por cien de los casos, digo el cien por cien. O sea, si ustedes cogen una llave USB con un troyano y la dejan con un cartelito que pone "confidencial" en el ascensor de una multinacional, les garantizo que en el cien por cien de los casos esa llave USB acaba pinchada en la red de la multinacional. Y no se lo estoy diciendo porque lo creo, se lo estoy diciendo porque lo sé. En el cien por cien de los casos, ¿vale? Con lo cual, lo de que los niños son más vulnerables porque son inocentes, yo creo que eso no es cierto.

También he oído, y lo han dicho aquí, que los jóvenes son nativos digitales y saben todo sobre la tecnología. Sí que es cierto que saben, pero por el número de horas que llevan. Realmente lo que pasa no es que ellos hayan nacido con un teclado en la mano y sepan mucho más que nosotros, qué va; es que le dedican muchísimo más tiempo. Y aquí lo que creo yo es que hay un problema de dejación de funciones de madres y padres, educadoras y educadores. Hay un problema de dejación de funciones porque es complicado. Yo estoy de acuerdo, es muy complicado. Pero realmente el problema, vuelvo otra vez al principio, no es de los niños, el problema es de la sociedad: es una sociedad distinta, completamente distinta, y ya podemos hacer lo que queramos, que va a seguir siendo una sociedad distinta. Lo que tenemos que hacer es adaptarnos a esa sociedad distinta. Su sociedad es una cibersociedad y va a seguir siéndolo. Con lo cual, tenemos que ayudar a nuestros colegas, a nuestros padres y madres y

educadoras y educadores a que enseñen a los niños cómo usar esto en condiciones.

Bien, en este sentido, ¿qué es lo que podemos decirle, desde nuestro punto de vista, desde el punto de vista de una empresa que se dedica a trabajar en temas de seguridad? En el mundo empresarial todo esto, o buena parte de esto, está ya diseñado y existe. Hay modelos de gestión. Esto no es un proyecto, no podemos coger aquí y decir "vamos a hacer ahora un plan de choque para concienciar a niños o a jóvenes entre 13 y 16 años" y ya está. No es así. Porque mañana los riesgos van a ser diferentes, con lo cual esto es un proceso que, queramos o no, iniciamos el día que aceptamos meter en nuestras casas Internet, en los colegios Internet, en las empresas Internet; lo iniciamos y no tiene vuelta atrás, es muy difícil volver atrás. Con lo cual, lo que tenemos que diseñar es una solución que tenga en cuenta todo esto, que tenga en cuenta que tenemos que estar en un proceso continuo y que, si me permiten, desde un punto de vista ya técnico ingenieril, cuando nosotros nos enfrentamos a un problema de seguridad y decimos "vamos a diseñar un modelo de gestión de seguridad", ¿qué es lo que nos preguntamos? Primero, qué es lo que quiero proteger y cuál es mi objetivo de protección; qué es lo que le puede pasar a mi objetivo de protección; cuál es la probabilidad de que le pase eso; y si le pasa, qué impacto tiene sobre su vida, sobre su bien, sobre su persona; qué es lo que yo puedo hacer para evitarlo. Y sobre todo, desde qué puntos de vista, en qué ámbitos, ¿un ámbito legal, un ámbito lógico, técnico, un ámbito físico, desde qué ámbitos? Esto para nosotros, desde el punto de vista técnico, es la definición del objetivo de protección, el TOP, cuál es mi objetivo de protección; el análisis de la taxonomía de amenazas, que si ustedes cogen una taxonomía de amenazas de adultos y de jóvenes, son idénticas, idénticas. El adulto dice "me han suplantado la identidad"; y el chaval dice "me han robado el Tuenti". Pero es lo mismo, ¿vale? Con lo cual, al final,

aparte de la taxonomía de amenazas, que es igual, tenemos un problema de riesgo: los mecanismos de protección que tienen que cubrir el riesgo y los ámbitos de actuación (un ámbito legal, un ámbito técnico).

Voy a centrarme solo en dos, porque no tenemos más tiempo. Todos estos sistemas de gestión, la verdad es que están permanentemente orientados a la gestión del riesgo, hay veces que parece que compremos numeritos para tener más riesgo, como es el caso de este señor: esta foto, que la encontré por ahí, la verdad es que me dejó impactado. Pero es que en Internet, en el ciberespacio los menores y los mayores compramos numeritos para que nos toquen los problemas: navegamos por redes que no son seguras, descargamos contenidos que no sabemos de dónde vienen.

Claro, cuando hablamos de riesgo, como decía antes, tenemos que valorar por una parte el impacto y por otra parte la probabilidad. Y el riesgo es un producto de ambos. Nosotros podemos tener una amenaza sobre un adulto o sobre un menor. Posiblemente la probabilidad no sea muy distinta, la probabilidad de que algo ocurra no sea muy distinta; lo que cambia sustancialmente es el impacto. El impacto en un adulto puede ser una pérdida económica, un problema de reputación; en un niño, pues un problema físico, un problema de pornografía infantil. Con lo cual, el impacto es evidentemente distinto, y por tanto el riesgo también lo es. Pero la probabilidad prácticamente es igual. Incluso yo diría que como nosotros vamos, si me permiten la expresión, muchas veces muy de sobrados, a veces incluso es mayor la probabilidad de engañar a un adulto que de engañar a un niño. Depende en qué, ¿vale?

El otro punto que quería comentar es relativo a los mecanismos, qué es lo que nosotros podemos hacer para mitigar todo este riesgo. Tenemos unos cuantos mecanismos. Uno, el de disuasión: “cuidado con el perro”. Estos son extraordinariamente baratos y extraordinariamente eficientes. Es decir, una ley, por el mero hecho de promulgarse o de comunicarse, es un

mecanismo de disuasión. Evidentemente, sino hay leyes que permitan determinado tipo de comportamientos, la disuasión no existe, ¿de acuerdo?

Después tenemos los mecanismos de protección. Es decir, un antivirus, un control parental: son mecanismos de protección. Pero los mecanismos de protección no siempre tienen que funcionar.

Cuando los mecanismos de protección no funcionan tenemos que tener mecanismos de detección, ¿que detecten qué? Que detecten que un niño tenga un problema, que detecten que se hayan saltado las barreras del antivirus y del control parental.

Evidentemente, cuando la detección funciona, tenemos que tener mecanismos de respuesta que nos sirven para ayudar al menor o al chaval a ver qué es lo que hace con ese problema.

Y después, mecanismos de recuperación, que a lo que nos llevan es a recuperar la posición inicial de partida.

En este sentido, los mecanismos de disuasión, fundamentalmente yo ahí veo mecanismos legales, de definir legislación que permita tanto a Fuerzas y Cuerpos de Seguridad del Estado como a las empresas que nos dedicamos a todo esto luchar contra estos incidentes.

Desde el punto de vista de protección (yo creo que es el punto además en el que hay que incidir), tenemos que incidir sobre la concienciación; concienciación, la autorregulación, la concienciación sobre la sociedad entera, no solo sobre los menores, sino sobre la sociedad.

Desde el punto de vista de detección: se ha trabajado muchísimo en problemas de protección, o mecanismos de protección de tipo de control parental, antivirus, pero en mecanismos de detección que identifiquen riesgos a los que está sometido un menor, hay muy pocas herramientas.

Y por último, mecanismos de respuesta y recuperación: el director general de INTECO, en la ponencia que he leído yo que tuvo con ustedes, les dijo que en una estadística que han hecho solo el 1% de los niños

declara que acudiría a sus padres en caso de tener un problema con temas de ciberdelincuencia o con un problema en la red. Claro, si no van a los padres, ¿adónde van? Pues en este momento están yendo a amigos, están pidiendo ayuda a amigos. Pero realmente creo que nosotros tenemos centros en España, hay CERT cualificados, tanto públicos como privados, que pueden prestar ese tipo de ayuda a los chavales. Lo que necesitan los chavales es saber dónde acudir. Igual que todos sabemos que hay un 112 que en el caso de ver un accidente podemos llamar al 112 y tenemos ayuda, no existe un ciber-112 o el equivalente al 112 en el ciberespacio. Igual que la sociedad física tiene una centro de emergencias, la sociedad virtual, la cibersociedad necesita también un centro de emergencias, un centro donde los chavales puedan pedir socorro, algo tan sencillo como eso.

En este sentido, ¿cuál es nuestra experiencia, qué es lo que hemos hecho nosotros? Pues como les decía, desde hace ya unos años (ya ahora les explicaré un poco la historia) hemos trabajado mucho, no en el qué, porque lo tenemos clarísimo desde hace mucho tiempo, a lo mejor estamos equivocados, pero el qué es que tenemos que concienciar en general a la sociedad, hemos trabajado mucho en el cómo, cómo hacerlo para que sea efectivo. Iniciativas de concienciación hay muchísimas; charlas, yo he ido a muchísimas, a dar muchísimas charlas (en mi opinión, hay muchas de ellas que no sirven absolutamente para nada), y además, dependiendo de quién sea el público objetivo, si son padres o son niños, el tipo de charla tiene que ser diferente, y en eso hemos trabajado.

Esto es un poco la línea de tiempo del trabajo de nuestra compañía en temas relacionados con el de la ponencia: empezamos en el año 2007 con la publicación de un blog que se llama Security Art Work en el ámbito técnico; es un ámbito técnico, que ahora les daré dos datos sobre el blog. En el año 2008 tuvimos un incidente en el que participamos como peritos de parte en un caso de pornografía infantil. En aquel momento eso nos

marcó mucho, porque evidentemente no son casos agradables. A partir de ese momento decidimos que lo que íbamos a hacer nosotros en materia social es invertir en la formación a nuestros hijos y a los hijos de nuestros amigos, de nuestros clientes, de nuestros colegas, y empezamos con un proyecto que se llamó ProtegITs a finales de 2009 y principios de 2010. El proyecto tuvo tanto éxito que al final lo convertimos en una iniciativa en la que estamos trabajando y en la que estamos colaborando con empresas dando concienciación en materia de ciberseguridad a empleados y a familias, incluidos los hijos de los empleados. El proyecto pasó a llamarse ProtegITs, y junto con Hijos Digitales, que es un blog que diseñamos para tener información asíncrona, no in situ, es en lo que estamos trabajando ahora. Algún informe que les contaré sobre el tema de los juegos, que además me ha hecho gracia que hagan antes esa apreciación, porque como consecuencia de las clases que nosotros hemos estado dando, uno de los problemas principales que detectamos fue precisamente el uso que los niños hacían de los juegos *online*. E hicimos un informe, y ahora comentaré un poquito sobre él.

Y ahora, en 2013, estamos pasando muchos de los contenidos, de la forma que les voy a contar ahora, que es una forma curiosa y un tanto original, los estamos pasando a una plataforma *online*.

Les decía que Security Art Work, que es una plataforma técnica que tiene solo dos datos, un millón de páginas vistas a lo largo de su historia, desde abril de 2007, pero en este momento tiene 5.218 seguidores. Es información fundamentalmente técnica, para compartir conocimiento de seguridad en ámbitos técnicos.

Hijos Digitales es un blog que se creó en mayo de 2011 orientado fundamentalmente a niños y padres. El lenguaje de este blog es nada técnico, es totalmente llano, para que lo entienda todo el mundo. Toca muchos temas relacionados con seguridad y temas relacionados con

tecnología, con un enfoque de seguridad. Con mucho menos periodo de vida tiene casi 900.000 páginas vistas, y en este momento unos 1.500 seguidores en Twitter. Tiene mucho éxito, hasta el punto de que... Nos ha sorprendido, además, mucho, porque es un blog relativamente joven. Pero la gente tiene muchísima necesidad de este tipo de contenidos. Es un blog que publica una entrada diaria, como decía, en un lenguaje muy llano. Tuvo un día que fue el TOP, que fue el caso de una persona, un colaborador del blog que publicó el caso del ciberacoso a su hija. Lo curioso de este caso no fue el hecho, sino la solución que le dio; fue una solución imaginativa. Yo les invito a que lo lean porque es curiosísimo. O sea, la solución que le dio estaba basada... Esto fue un caso de acoso a través de WhatsApp, y en un momento determinado tenía muchos problemas, es muy largo, pero no voy a extenderme, y entonces se dio cuenta de que la solución no podía venir a través de las niñas que acosaban a su hija; la solución iba a venir de sus padres. Los propietarios de los números de teléfono móvil eran sus padres, y lo que hizo fue poner una denuncia a los propietarios de los teléfonos móviles. En una semana se acabó el problema.

Con lo cual, esto no es un problema de niños; esto es un problema de la sociedad, es un problema que nos muchísimo a los padres también. De hecho, tuvo 18.000 visitas en un solo día el caso este del ciberacoso. En este momento estamos en cerca de 100.000 visitas en Hijos Digitales, y yo creo que es una forma de comunicar muy útil, francamente útil. Porque además hay mucha colaboración, el crecimiento de 2013 respecto a 2012 está en torno al 400%, 700% y creciendo. Es un tipo de contenido muy demandado sobre todo por los padres, porque como decía antes, no saben dónde están sus hijos realmente.

El segundo proyecto, el proyecto, digamos, más grande que hemos desarrollado, se llama ProtegITs, con esta imagen un tanto curiosa: la I y la

T es tecnologías de la información, y el paraguas representa seguridad, y sobre todo eso hemos montado, digamos, los elementos del proyecto.

Recuerden que antes les decía que para montar un proyecto de seguridad necesitamos diseñar mecanismos de cinco tipos. Este proyecto se diseñó técnicamente por un equipo de ingenieros, con un final que evidentemente tiene un final en instructores o en gente que ha dado clase a los niños; se diseñó un aula interactiva (que luego verán lo que es) con unos talleres prácticos, con una forma muy curiosa de dar los talleres, con unos pilotos que nos permitieron en un inicio conocer las amenazas a las que estaban expuestos los niños, con un guion, porque al final esto es prácticamente igual a una obra de teatro, con su guion perfectamente establecido, incluso con los ejemplos y todo, con un portal, un *kit* que lo que permitía era desplegar a través del portal mecanismos de protección con dos elementos, una barra y un hito que luego les presentaré (es la mascota del proyecto), un plan de comunicación, un centro de servicios y un club. Todo esto, que son medidas en torno a un proyecto, a una idea para echarles un cable a los chavales, tienen un grupo de medidas de disuasión (nosotros, evidentemente, no podemos legislar, con lo cual la parte legal no entra dentro de nuestras posibilidades), pero sí el comunicar la existencia de centros que se dedican a ayudar a los chavales en esta materia.

Hay un grupo de medidas que son medidas de protección. La concienciación, como decía antes, es una medida de protección fundamental. Hay un grupo de medidas que son de detección: intentan detectar situaciones de riesgo para los chavales. Y hay medidas que son de respuesta y recuperación: un sitio donde acudir, alguien a quien preguntar, alguien a quien decir "oye, necesito ayuda, por favor, ¿me puedes ayudar?".

Este proyecto: esta es el aula, es un aula muy controlada porque distribuimos troyanos y virus para que los chavales se den cuenta del riesgo, con lo cual todo lo montamos nosotros. De hecho, esta es una clase que damos en nuestras oficinas allí en Valencia, una clase donde tenemos una figura un tanto especial que es la de aquí del fondo, esta persona de aquí, es lo que nosotros llamamos "el malvado"; es una persona de nuestro equipo de *hacking*, y como ven, está detrás de un pequeño paraván (este paraván de aquí); esta persona es la instructora, en este caso es Eva, que es una instructora de chavales. El papel de la instructora es llevar el hilo conductor de la clase. El papel de nuestro amigo Javier, en este caso, del malvado, es darles unos cuantos sustos a los chavales. Y cuando digo "darles unos cuantos sustos" significa demostrarles lo que una persona con conocimiento podría hacer si fuese mala. Y lo que hacemos es demostrárselo en sus carnes. De hecho, diseñamos un guion con un montón de píldoras (que luego volveré sobre el concepto de las píldoras), que lo que son realmente son casos de incidentes anonimizados que hemos tratado con niños y con adultos, y que se los explicamos a los chavales de una forma muy sencilla. Utilizamos un concepto en este guion que llamamos "La bofetada digital". Claro, necesitamos que los chavales nos hagan caso y que se tomen en serio donde están. De hecho, cuando entran en un aula, que puede ser un aula parecida a esta, tienen todos sus portátiles, y nada más entrar en el aula, la mayoría de ellos entran en el Facebook o en el Tuenti, se "logan", se hacen usuario y contraseña y se meten; en ese momento, el malo ese que está ahí atrás, lo que les está haciendo es un *phishing*, y les está robando el usuario y la contraseña. Y el usuario y la contraseña lo publica. Y les dice "os acabamos de robar el usuario y la contraseña. Y además, estas contraseñas que estáis utilizando son malas". Y a partir de ahí empieza una dinámica en un aula donde lo que hacemos es distribuirles troyanos, robarles la cámara, para que se den cuenta ellos

mismos en sus propias carnes qué es lo que podemos hacer sabiendo un poco de tecnología. Bien, este formato ha tenido un éxito increíble. De hecho, los chavales son los que nos van contando y los que nos van escribiendo el guion, y el guion se va adaptando a lo que nos piden. Una de las cosas que hicimos es meter un informe de seguridad de juegos *online*, porque nos dimos cuenta de que las niñas utilizan mucho las redes sociales; los niños juegan, juegan *online*. Entonces, alguno de ellos nos hablaba del dinero electrónico. Y entonces empezamos a estudiar qué era aquello del dinero electrónico, y alucinamos, o sea, fue impresionante. Hicimos un informe, que está además en nuestra página web, *Seguridad de los juegos online en 2011*; descubrimos, por ejemplo, mafias, pero mafias organizadas; el dinero es un dinero virtual, es un dinero con el que se compran roles, son juegos de rol, y que yo tengo desde la posición 0 hasta la 99, soy más machote si estoy más alto en el rol. Y evidentemente, esto en la comunidad de los niños tiene mucho peso. Esto lo saben los niños y también lo saben los malos. Y en China, de hecho (hay alguna foto en el informe) hay cárceles donde los carceleros tienen a presos jugando a juegos de rol a los que juegan los chavales para conseguir dinero virtual, que luego se van a las páginas web de venta en Internet y las venden por dinero físico. Con lo cual, algo que aparentemente es un juego *online* que juegan con dinero virtual se convierte en un juego donde los niños están jugando con dinero físico, y donde estamos teniendo una cantidad de problemas, porque en teoría esos juegos no tienen dinero real, pero se está convirtiendo en una mafia, en un mercado negro impresionante.

Otro caso es el de un chaval que vino y que n os decía que lo primero que hacía él cuando llegaba a un sitio era robar la WiFi. ¿Cómo que robar la WiFi? Dice: “sí, mira”. Y nos enseñaba los programas que utilizaba. Yo alucinaba. Estos chavales son *hackers* en potencia. Pero te enseñaban los programitas que utilizaban... Claro, este era un chaval de 15 años, a este

tipo de chavales no les puedes decir que esto es un delito, porque es que yo creo que ni lo entienden, ellos necesitan estar conectados. Con lo cual dicen "¿cómo va a ser un delito?, si necesito conectarme, pues me conecto". Entonces, lo que hicimos fue darle un poco la vuelta: metimos una píldora en la clase lo que le contábamos qué es lo que una persona mala puede hacer, si yo soy malo y me roban mi WiFi, a partir de ese momento todo el tráfico que pasa por aquí lo veo, pero lo veo entero, con lo cual te robo tu usuario, tu contraseña, tus fotos, te lo robo todo. Eso sí que les hacía daño, ¿vale? Con lo cual buscamos la forma de intentar convencerles de que no hiciesen eso.

El proyecto tiene un portal. Tiene un *kit*, que nosotros intentamos diseñar herramientas que faltan. Evidentemente, filtros de control parental, herramientas antivirus hay un montón. Lo que pasa es que nosotros detectamos, digamos, dos agujeros, dos huecos en las herramientas que utilizan tanto hijos como padres.

Una es aquella que nos permite pedir ayuda. ¿Dónde piden ayuda y cómo? Los chavales, cuando están navegando están utilizando un navegador, herramientas, y lo que necesitan es tener algo que mientras estén navegando les permita, por ejemplo como es el caso este, una pequeña barra cuyo único objetivo es tener un botón rojo que digas "necesito ayuda", y poner en contacto al chaval en este caso con un centro de servicios donde tiene a alguien que, con conocimiento tanto desde el punto de vista legal como desde el punto de vista técnico, es capaz de echarle un cable. Pero ese tipo de elementos de ayuda no existen en el mercado. O sea, filtros de control parental, sí; pero, ¿y cuando no funciona un filtro de control parental? Un filtro de control parental no sirve para cortar contenidos en una red social donde un niño está quedando con un adulto, no sirve para nada. Ahí necesitamos otro tipo de herramientas. Esta era una.

Y la otra es una que tuvo mucha polémica. Nosotros somos una empresa de seguridad, y como empresa de seguridad utilizamos herramientas que interceptan el tráfico, y lo hacemos en las redes de nuestras empresas para buscar tráfico anómalo, intentos de intrusión, intentos de ataque; estas herramientas son herramientas muy potentes, herramientas que nos permiten analizar el tráfico que funciona por una red. En este caso diseñamos una herramienta cuyo objetivo, a partir de una taxonomía de amenazas, por ejemplo, un diccionario de palabras con palabras como por ejemplo "anorexia", porque estamos hablando siempre de la pornografía infantil, pero nos olvidamos algunas veces de otro tipo de problemas que tienen los chavales en las redes, identificaban algunos tipos de palabras de forma que pudiesen disparar una alerta, decirle al padre "oye, mira a ver qué pasa, porque tu hijo está hablando de anorexia, de bulimia, de *sexting*, de sexo o de quedar". ¿Vale? Con eso, lo que hicimos fue diseñar una herramienta utilizando técnicas de las que nosotros utilizamos en la empresa para diseñar un cacharrito que se ponía en un ordenador y detectaba situaciones de riesgo. Ahora bien, evidentemente, esto es intercepción de comunicaciones. Y lo que hicimos es irnos a hablar con un grupo de fiscales, fiscales especializados en menores para pedirles su opinión. Nos dijeron: esto no se puede hacer. No se puede hacer. Por mucho que seas padre, tú no puedes interceptar las comunicaciones de un niño. Y nos propusieron que creásemos, así nació Ito, que es la mascota del proyecto, que es un elemento que lo que pretende es, primero, decirle al niño que existe, y decirle qué hace. Es decir, un elemento de análisis de comunicaciones le dice, Ito le dice al niño qué está utilizando –sobre todo para los niños más pequeños–, "estoy aquí y hago esto". Segundo, tiene que poderse desconectar. El niño tiene derecho a desconectarlo. Claro, cuando te enfrentas a esto dices "vamos a ver, si desconecto Ito, la protección que intento montar sobre mi hijo o sobre mi familia ha desaparecido". No; no,

porque la desconexión de la mascota, la desconexión de Ito es en sí mismo una alarma. Es decir, mira, yo te digo: "padre, tu hijo ha desconectado esto. Vete a hablar con él". Y así cumplíamos otra labor, que era el fomentar la comunicación entre los padres y los hijos para que todo esto funcionase un poco mejor.

Este es el aspecto de Ito. Ito, cuando estaba grabando decía que estaba grabando. Insisto que esto sobre todo está orientado a los chavales más pequeños. Cuando detectaba una amenaza se ponía en rojo y daba un montón de consejos, y el niño en este caso podía desconectarlo, y a partir de ese momento Ito dejaba de interceptar cualquier comunicación.

Como veis, este es un proyecto que tiene todas las piezas; tiene herramientas o mecanismos de protección, de detección, de disuasión y de respuesta y recuperación, con el centro de servicios.

A partir de ahí, esto tuvo tanto éxito que diseñamos, haciendo uso de la misma estrategia, un proyecto que se llamó ProtegITs y en el cual ya nos fuimos a hablar con empresas, no para hacer la concienciación típica en empresas en materia de seguridad, sino con departamentos de responsabilidad corporativa y con departamentos de tecnología, aunar esfuerzos y decirles "mira, vamos a hacer una labor social y además vamos a cumplir los requisitos que tienes tú en materia de seguridad dentro de tu compañía". Y empezamos a montar jornadas de seguridad familiares donde iban hijos de empleados y empleados, y jornadas orientadas al empleado. El éxito ha sido impresionante. Volvemos otra vez a lo mismo, es el cómo hacerlo. Está claro que lo que hay que hacer es concienciar, pero hay que buscar una forma de hacerlo que llegue a los niños, que llegue a los adultos y que nos sirva para realmente incrementar ese nivel de concienciación. Esto lo hemos hecho en organizaciones, entre otras, como Endesa, Red Eléctrica, que están apostando mucho por la concienciación de seguridad,

no solo de sus compañías, sino también de las familias, de las personas que están trabajando en estas compañías.

Porque también tienen claro que el problema es un problema global. La seguridad de una empresa no se puede conseguir simplemente con la seguridad de los ordenadores de la empresa ni con la seguridad de los empleados; sino también necesitamos la seguridad de los entornos. Al final es un problema global, ¿de acuerdo?, como decíamos al principio.

Al final, en las jornadas familiares repartíamos una serie de decálogos. Aquí tienen algunas fotos, en este caso son David y Patxi, el bueno y el malo, en una preparación de una clase; algunas clases con chavales, de hecho hemos ido por toda España dando cursos de concienciación tanto a nivel empresarial como a nivel, digamos, social. En sitios donde nos lo han pedido también nos hemos ido a dar este tipo de charlas, que son las que entendemos que son francamente útiles.

¿Cosas que nos han pasado? Nos ha pasado de todo. Por ejemplo, una cosa que nos llama muchísimo la atención es que solo el 10% o el 15% de los asistentes suelen tener Facebook, y ninguno Tuenti. Lo primero que hice yo cuando mis hijas me dijeron que querían Facebook y Tuenti fue sacarme un perfil mío, con mi nombre y apellido, no un perfil falso, sino el mío, José Rosell. ¿Por qué? No se pueden imaginar el tiempo que tardó mi hija mayor en mejorar la seguridad de su perfil. Bueno, ya conseguí algo: que se preocupe por quién tiene que ver qué. Eso para mí, en ese momento fue suficiente. Ahí hay una labor inicial de saber qué es Facebook, qué es Tuenti. Por ejemplo, mi hija hace cuatro días vino con que en el colegio le habían pedido que se diese de alta en una red social que se llama Ask, que es "pregúntame y yo te respondo". De estas hay un montón. Y una de las cosas que necesitamos o que les transmitimos a la gente es que lo del parque de antaño, lo de llevar al hijo al parque y decirle "la tierra no se come", lo tenemos igual pero en formato digital. Y el parque, el recreo, el

colegio es digital. Con lo cual, no tenemos más remedio que estar donde están nuestros hijos. Y no vale decir "es que ellos saben mucho". No saben mucho, se pasan más horas. Pero no saben más que nosotros, ¿vale?

Aquí hemos utilizado un concepto de píldora formativa donde exponemos casos, hacemos análisis de las consecuencias del caso y recomendamos prácticas para evitarlo. Esto lo copiamos de una cosa muy antigua en nuestro país, que son las campañas de la Dirección General de Tráfico. Las campañas de la Dirección General de Tráfico tuvieron mucho éxito, han tenido durante mucho tiempo mucho éxito porque mostraban los problemas derivados de no hacer un uso responsable, en este caso de la educación vial o de la conducción. En materia del ciberespacio pasa lo mismo: hay que enseñarle a la gente lo que pasa al no cumplir ciertas reglas.

Esto es una clase, digamos, de empleados, donde utilizamos también la píldora. Aquí tenemos, ya no vestidos de negro y blanco, porque esto no es para niños, es ya para empleados, tenemos al instructor y a una persona de nuestro equipo de *hacking*; hacemos una representación de un día del buen empleado en una compañía, donde a lo que volvemos otra vez es a incidir en el cómo damos la concienciación y no en el qué; el cómo es enseñándoles con píldoras, con sucesos, con incidentes qué es lo que le puede pasar a una persona de una organización cuando hace un uso de una tecnología despistado. Ya no con mala fe, sino simplemente por no tener en cuenta determinado tipo de mecanismos. Todo esto lo estamos pasando ahora a *online*, y la verdad es que el resultado está siendo francamente bueno, lo que nos anima a seguir con todo este tipo de trabajo. Al margen de nuestro trabajo normal, que es trabajar en seguridad para las empresas, es que la gente está muy contenta, la gente nos pide más. De hecho, hay algunas cosas (les he puesto aquí y esto se lo pasaré completo), algunas respuestas de los chavales que son graciosísimas. Cuando les preguntas a

los chavales "¿tú has tenido algún problema de estos que vemos aquí?". Casi ninguno, el 25% dice que sí, el resto que no. ¿Y conoces a alguien que haya tenido este problema? El 85% dice que sí, y el resto que no. Claro, es muy significativo. Cuando hablas con ellos te das cuenta de que los problemas de suplantación de identidades están a la orden del día, y es muy difícil pelear contra todo eso.

Hay un caso que a los padres sobre todo les causa mucha impresión, que es el del geoposicionamiento de las fotos. Y vuelvo a incidir sobre lo mismo: esto es una píldora que utilizamos. A los chavales se lo enseñamos y a los padres se lo contamos. Y hacemos la jornada paralela: los niños por una parte y los padres por otra. Cuando los padres le dan a un chaval (ahora con 9 o 10 años) un móvil de estos de última generación, un *smartphone*, una de las cosas que la mayoría no sabe es que el *smartphone* lleva de serie el geoposicionamiento de las fotos. Los chavales cogen la foto, las suben a Twitter, la suben a Tuenti, la suben a Facebook, e implícitamente están diciendo dónde están. Pero es que si sigues a algunos de ellos en Twitter, te dicen: "mira, me acabo de hacer una foto que estoy en el cumpleaños de fulanita", y suben la foto al Twitter. Y dicen "ya ahora me voy a casa". Y la casa la tengo yo grabada de dónde es. Con lo cual, si sé dónde está y sé dónde va, no tengo más que ponerme en medio para interceptarlos. Claro, a la gente... Hay programitas como este de aquí, aquí sale un mapa, que lo que hace es geoposicionar las fotos de una cuenta de Twitter en un mapa, y sabes conductas de desplazamiento, por dónde va, a qué horas va, te lo saca todo. Esto no es un problema de los niños. Al niño, a un chaval de 10 o de 11 años le das un móvil con el geoposicionamiento conectado; y cuando sube fotos al Tuenti o al Twitter está diciendo dónde está, dónde voy, por dónde me suelo mover o por dónde vuelvo del cole a casa.

Bien, como conclusión yo quería poner un corto de un vídeo que dura tres minutos, que es muy significativo de lo que ocurre en términos generales.

[LOCUTOR VÍDEO]: *Yo puedo comentaros un poco qué hay relacionado con la seguridad, relacionado con la ciberseguridad dentro de nuestra oferta formativa. Nosotros, en la escuela tenemos en este momento un grado en Informática...*

El señor **SOCIO DIRECTOR DE S2 GRUPO**: (Rosell Tejada): Esto es una conferencia de una persona que tiene un alto cargo en una escuela de informática en una universidad politécnica, en el ámbito de una conferencia de protección de infraestructuras críticas, algo que desde el punto de vista del riesgo, para un país como España o cualquiera de la Unión Europea es un riesgo muy elevado, evidentemente, es un problema muy importante.

[LOCUTOR VÍDEO]: *Los nuevos grados son de cuatro años, son 240 créditos, y a fin y al cabo es equivalente a las antiguas ingenierías; de hecho el grado se llama en Ingeniería Informática. Y básicamente, puede pasar un alumno a hacer ese grado y no recibir específicamente ninguna formación en seguridad. Tenemos apenas 9 créditos de esos 240, es decir, algo menos de un 4%, de una formación optativa en algún aspecto relacionado con la seguridad.*

El señor **SOCIO DIRECTOR DE S2 GRUPO**: (Rosell Tejada): Ahora el segundo corte. Son cuatro cortes.

[LOCUTOR VÍDEO]: *Y algo parecido sucede en nuestra oferta de másteres. Tenemos en este momento seis másteres alrededor del centro en temáticas de informática, y de esos seis másteres, pues cuatro no tienen nada de oferta de temas de seguridad; y los dos que lo tienen, pues también de nuevo tienen asignaturas con un carácter optativo.*

El señor **SOCIO DIRECTOR DE S2 GRUPO**: (Rosell Tejada): El tercero.

[LOCUTOR VÍDEO]: *Nosotros nos encontramos en lo que es la enseñanza reglada un poco en una situación parecida a lo que comentaba Sebastián respecto a cuáles son los plazos; él hablaba de que en una normativa había que revisar cada cinco años, que en otra normativa había que revisar cada dos los planes. En nuestro caso nuestros planes de estudio se aprueban en un momento determinado y no tienen fecha de caducidad, aunque normalmente más pronto o más tarde se acaban renovando. Pero sí adolecemos en ocasiones de una cierta rigidez. Y a mí me ha preocupado especialmente el lugar que ha ocupado en esta mesa, porque no quiero, no me gustaría que la universidad, que la academia se encuentre un poco separada del resto de la sociedad, como me ha tocado en esta mesa. Entonces, realmente nosotros desde la academia, desde la escuela, aun siendo sensibles a esta problemática, consideramos que nos hemos centrado en ofrecer una formación generalista de ingeniería. Yo estoy convencido de que los estudiantes de ingeniería mecánica no necesariamente reciben una formación específica, no sé, en antirrobos de coches, ¿no? Lo cual no quiere decir que no sea una temática importante; lo cual no*

quiere decir que no pueda ser incluso una iniciativa empresarial de interés. Pero, claro, hay otras muchas cosas. Y a veces es difícil enfocar con precisión lo que es más adecuado en...

El señor **SOCIO DIRECTOR DE S2 GRUPO**: (Rosell Tejada): Y la última ya.

[LOCUTOR VÍDEO]: *...en cada momento. Y prácticamente, yo quería terminar un poco con la reflexión de que por ejemplo, cuando el señor Ford se plantea hacer el modelo T, pues posiblemente en lo último que esté preocupado es en a ver si se van a robar mucho los coches o no. Entonces, está claro, y creo que mis compañeros han hablado con mucha claridad respecto a la seriedad en particular de la protección de estas infraestructuras críticas, es decir, que no consideréis que no lo veo importante, sino más bien intento un poco disculpar en cierto modo el que nosotros, en lo que es la formación generalista, no tengamos una mayor abundancia de especialización. Yo puedo contaros un poco qué hay relacionado con la ciberseguridad dentro de nuestra oferta formativa...*

El señor **SOCIO DIRECTOR DE S2 GRUPO**: (Rosell Tejada): Ya está. En definitiva, yo creo que esto lo resume un poco todo: nosotros, en la sociedad en la que estamos, estamos trabajando todos los días en materia de seguridad; ya habéis visto que con niños en una parte, con adultos, con empresas. La conciencia de la sociedad en general en materia de ciberseguridad es escasa o nula. Ni siquiera en las universidades, que deberían estar mucho más cerca de los problemas empresariales o de los problemas de Estado ligados directamente con los temas de seguridad (seguridad nacional, robo de patentes, etc.), ni siquiera ahí tenemos una

conciencia clara de los temas de seguridad. Y en ese contexto, pues qué le vamos a pedir a los menores. Yo creo que tenemos un problema antes que resolver, y es un problema general de la sociedad.

Y en este sentido, simplemente para concluir, el problema que tenemos, en mi opinión, es muy grave; si queremos ayudar a los niños tenemos que resolver antes el problema que estábamos comentando, el de la cultura de la ciberseguridad en la sociedad, empezando por sus madres y padres y por sus profesoras y profesores, que no tienen ni idea, pero ni idea, es algo increíble, porque no han tenido la oportunidad tampoco.

Con esto, yo creo que resolveremos parte del problema, pero no todo; yo creo que ahí hay que ponerse manos a la obra con los temas de ciberseguridad en general. "Concienciación", para mí es la palabra clave; la clave es concienciación, no formación; estamos aún en la fase de concienciar, no formar; la formación es larga y cara; la concienciación no tanto. Y creo que nos tenemos que centran en cómo tratamos la concienciación y no tanto en que hay que hacer concienciación. Es decir, la concienciación tiene que ser efectiva. Yo he ido a conferencias, de hecho he leído incluso, en las ponencias que han tenido ustedes aquí, de la policía, algún policía que decía que en las conferencias que iban a dar a colegios, realmente no iban casi personas, y que incluso las personas que iban realmente no recibían el mensaje que ellos querían dar; con lo cual volvían a lo suyo: es que nosotros somos policías, no somos comunicadores ni formadores ni instructores. Yo creo que hay que trabajar muchísimo en cómo debemos dar esa concienciación más que en qué. Yo creo que una forma de hacerlo es las campañas parecidas a las Dirección General de Tráfico con las píldoras formativas o los casos de uso, como quieran llamarlo ustedes.

Y hasta aquí. Muchas gracias.