COMPARECENCIA DEL DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN (INTECO), D. MANUEL ESCALANTE GARCÍA, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES EL DÍA 9 DE MAYO DE 2013.

El señor **DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN (INTECO) (**D. Manuel Escalante García): Muchísimas gracias, presidentes, senadores. Para mí es un auténtico honor estar aquí con todos ustedes, es mi primera experiencia en este ámbito, y la verdad es que estoy encantado de tenerla.

Tengo una doble dificultad: una es que las exposiciones han sido muy buenas y muy prolijas y que las preguntas también han sido muy buenas, con lo cual el tema se me ha ido acotando bastante. En cualquier caso, todavía hay cosas sobre las que se puede profundizar y voy a intentar ir precisamente a esos temas en los que yo creo que merece la pena que profundicemos.

Antes de empezar con mi presentación, querría comentar algunas notas que he tomado y que creo que nos pueden ayudar a enfocar bastante el problema. Así, deberíamos hacer un zoom mayor de la problemática; es decir, estamos hablando de los menores, pero a mí me gustaría reflexionar sobre qué está pasando con la sociedad en su conjunto, porque nos puede ayudar mucho a entender qué es lo que está pasando con los menores, qué es lo que se puede hacer en el ámbito de los menores y qué es lo que no se puede hacer en el ámbito de los menores, porque es probablemente imposible.

Haciendo ese *zoom-out*, nos damos cuenta de que es un problema global que afecta a toda la sociedad. En Inteco nos dedicamos a la ciberseguridad y eso nos hace tener una visión y una perspectiva de conjunto muy amplia de lo que sucede. Estamos viviendo una auténtica revolución, lo sabemos todos. Lo que no

sé si tenemos muy claro es cuál es la dimensión de esa revolución que estamos viviendo, que probablemente explique muchas cosas de las que están sucediendo y que veremos a continuación.

El aumento del uso de la sociedad de la información y de las tecnologías de la información es constante y exponencial: hace diez años no estábamos hablando de lo que estamos hablando hoy aquí, ni dentro de diez años estaremos hablando de lo que estamos hablando aquí hoy. Es decir, es una verdadera revolución. Cuanto más valor añadido hay en la Red, hablando por ejemplo en el ámbito empresarial, en el ámbito bancario, en las administraciones, mayor valor añadido, mayor posibilidad de hacer un negocio para el ciberdelicuente y, por tanto, aumenta el riesgo. Esto es así.

Y luego sucede otra cosa muy importante y es que hemos decidido vivir de espaldas al riesgo. Las sociedades han decidido vivir de espaldas al riesgo. Y probablemente eso hila con lo que he dicho antes, porque la revolución es de tal dimensión que hemos decidido vivir de espaldas al riesgo: a mí esto me aporta tantísimo que sé que pueden suceder cosas, pero no pueden ser tan graves. Y no será porque no hay noticias todos los días en los medios de comunicación, todos los días, sistemáticamente, cosas gravísimas que están sucediendo. Bueno, pero es que esto me aporta demasiado. Esa revolución es demasiado grande, es mi percepción.

Incluso, lo estamos viendo, en empresas de carácter estratégico. Incluso el nivel de preparación en materia de seguridad no es el que uno esperaría en empresas o en instituciones de ese nivel. Por hacer un símil, ¿qué sucedió cuando entró el ferrocarril en España? Era una revolución. Sin embargo, inmediatamente, en una revolución no tan socializada ni probablemente tan grande, se percibió el riesgo: cuidado, esto es una vía de entrada para una invasión. ¿Qué hicimos? Pues se crearon las brigadas de ferrocarriles, no recuerdo exactamente cómo se llamaban, y se puso un ancho de vía distinto a España (por aquí no entran porque descarrilan los trenes); drástica pero

totalmente real. ¿Por qué? Porque había una percepción muy clara del riesgo, estaba muy claro, por ahí podían entrar. Ahora no, y está clarísimo también, porque lo estamos viendo todos los días. Hace diez años podíamos decir “no está claro que esto puede suceder”. Hoy está clarísimo que esto está sucediendo.

Pero está sucediendo a empresas no de pequeño tamaño, puesto que todos los días estamos resolviendo problemas de empresas de 100, 200, 500 empleados; está sucediendo a empresas estratégicas, cuya información, cuya propiedad intelectual es la base de su negocio, y le ha sucedido a Northern Networks, que ha estado a punto de desaparecer con una bajada en bolsa de sus acciones terrible, por un problema de robo de propiedad intelectual procedente de algún país. Le ha pasado a Sony, le ha pasado a Google, le ha pasado a SpamHouse, que es una empresa de seguridad; le ha pasado hace muy poquito a una empresa que se llama Kinetics Systems, que es una empresa de altísima tecnología que trabaja para el ejército de Estados Unidos, que todos entendemos que deberá de tener unos niveles de seguridad terribles; pues le ha pasado también, llevan un año robándole propiedad intelectual a Kinetics Systems. Quiero decir, esta es la situación.

Les está pasando a las instituciones. Ahora mismo hay un tema con el ciberespionaje, y está pasando a ámbitos diplomáticos, a ámbitos de alto nivel de decisión de las administraciones. Todos hemos oído hablar del famoso “Octubre Rojo”. “Octubre Rojo” no es más que un virus que se dirige hacia una determinada persona que maneja unos determinados niveles de información, que infecta las organizaciones, que es dificilísimo –por no decir imposible, en algunos casos– de detectar, y que es dificilísimo –por no decir imposible también– en muchos casos de limpiar. Es decir, estamos hablando ya de otra historia. Esto no tiene nada que ver con lo que vivíamos hace unos años: el 2010 marcó el antes y el después en el ámbito de la ciberseguridad.

Y también ocurre con las infraestructuras críticas. En Estados Unidos, por poner un ejemplo, son conscientes de que tienen muchos aviones, muchos

barcos y muchos portaaviones, pero que a través de las redes de comunicaciones pueden “apagar” el país. Y cada vez más lo van a poder “apagar” en la medida en que las redes de distribución eléctrica estén informatizadas a través del *smart grid*. Por tanto, la vulnerabilidad está en casa: alguien con escasos medios, al que ni siquiera voy a ver la cara, va a poder causar un daño terrible en mi territorio.

Y les pasa también a los adultos. Lo sabemos porque conocemos lo que está pasando en los hogares, ya que tenemos 3.500 hogares panelizados y estudiamos sus hábitos de navegación y analizamos el nivel de seguridad y de infección de sus equipos. Los adultos, los usuarios habituales del ordenador, no es que tengan infectado el ordenador una vez, es que lo tienen infectado cien veces y no son conscientes. Esos adultos, ¿qué les van a contar a los menores? Es difícil ayudar cuando no se cuenta con el conocimiento completo.

¿Cómo se resuelven estos problemas en el ámbito empresarial? No pretendo dar miedo, pretendo hacer una radiografía del problema, de lo que está sucediendo, porque es importante. ¿Cómo se resuelve esto en el ámbito empresarial, en las infraestructuras críticas, en las instituciones públicas? Pues se resuelve con un doble factor, que son los medios tecnológicos y el capital humano formado en materia de seguridad de la información, ambos imprescindibles. También es imprescindible la formación de los usuarios, puesto que pueden tener mucha tecnología a su alrededor, pueden estar rodeados de medidas de seguridad, pero siempre hay alguna forma de sortear una medida de seguridad. Entonces, o el usuario está formado y es consciente del riesgo primero y del daño que puede infligir a su organización, o da igual las medidas de seguridad que despleguemos. Y esto lo estamos viendo todos los días. Las cosas entran porque alguien abre un correo que no debe abrir, enchufa un *pendrive* que nunca debería haber enchufado –esto pasó en una central nuclear de Irán, todos lo sabemos, alguien enchufó un *pendrive* en un sistema SCADA de control de las centrifugadoras de uranio con un virus sofisticadísimo–.

Bueno, pues esto es porque los usuarios no están preparados. En el ámbito empresarial, en estos ámbitos profesionalizados, una parte muy importante del problema se puede resolver con las medidas tecnológicas y un porcentaje un poco menor con las medidas de carácter humano.

¿Y qué pasa en el ámbito de los menores? Pues muy parecido al de los adultos: necesitamos medidas tecnológicas y necesitamos –ahí voy a repetirme, pero es que es la clave– que estén muy formados para el mundo en el que van a vivir. Ya no solo para cuando tengan 13 años u 11 años y entren en las redes sociales, es que van a vivir en un mundo completamente distinto y, o son capaces de utilizar las nuevas tecnologías y que eso no sea un agujero para ellos, para su seguridad, para sus finanzas, para su privacidad, o no van a poder desenvolverse adecuadamente en el mundo.

En este caso además, por fortuna, las medidas formativas, lo que son los controles humanos – como lo llamamos habitualmente – que puede desplegar un menor, resuelven un porcentaje muy alto de los problemas graves, al contrario de lo que sucede en las organizaciones. El sentido común que seamos capaces de desarrollar y la formación que seamos capaces de desarrollar en los menores resuelven los problemas graves. El problema de los menores es que su personalidad no está desarrollada, y el daño que le pueden infligir no es un daño económico o un daño a su imagen, es un daño psicológico o es un daño incluso a su integridad física. Ese es el gran problema. Y eso en general no se resuelve con tecnología eso se resuelve con formación. Porque que el ordenador va a estar infectado, esa es la realidad que vivimos hoy. Y puede estar infectado para capturar su webcam.

Otro problema que nos encontramos y que también es importante enmarcarlo es que no existen fronteras. No existen fronteras en ningún sentido. No existen fronteras legislativas: en un porcentaje muy alto de los casos de ciberataques o de los incidentes en los que nosotros trabajamos no se producen desde España, prácticamente nunca, o alguna vez hay algún servidor o un

reducido número de usuarios involucrado. Igual sucede en Estados Unidos o en Alemania: el ataque tampoco se produce en esos países, sino que a lo mejor se produce desde España, o desde Rusia o China, que suelen estar entre los países de origen. Pero no suele suceder dentro. Con lo cual tenemos una dificultad añadida muy grande con el tema legislativo.

Prueba de que hay un problema jurisdiccional muy grande es que la figura de los CERT –los CERT son los *Computer Emergency Response Team*, los equipos de ciberseguridad– han proliferado en el ámbito internacional y han ganado muchísimo protagonismo. ¿Por qué? Porque estos problemas en general son problemas que duran horas, días o semanas. Y el ámbito judicial no actúa en esos tiempos, es imposible literalmente. Cuando pedimos una orden judicial el problema original ha desaparecido y ha derivado en otros problemas. Con lo cual, esto no funciona. ¿Qué tienen los equipos de respuesta? Que trabajan bajo el radar, trabajan, por decirlo de alguna manera, en base a redes de confianza, que no tienen nada que ver con el ámbito judicial. Hay un ISP donde hay un servidor que está infectado y que está inyectando malware en equipos españoles. Pues nosotros contactamos con el CERT y le avisamos de que hay un equipo que está infectado en dicho ISP y de la actividad que está desplegando. Y ellos, con sus relaciones de confianza internas dentro de su país, se encargan de solucionar el problema.

Eso solo funciona en ese ámbito. En el ámbito judicial, cuando llegamos a ese servidor ha hecho todo el daño que tenía que hacer, ha robado todo lo que tenía que robar y el virus en cuestión ha desaparecido. Esto es lo que hace que los CERT cada vez tengan mayor importancia y que la coordinación sea no necesaria, sino crucial en este ámbito.

Ahondando en el tema de las fronteras, ¿qué tipo de fronteras podemos establecer? ¿Podemos marcar aquello que nos parece mal y filtrarlo? Lo digo porque es un debate también muy interesante y que en algunos países ya se han planteado. La pregunta es qué es malo y qué es bueno. Y qué es malo y qué es

bueno, no digo en cuanto al contenido, sino que muchas veces los servidores desde los que se ataca no son servidores malos, son servidores buenos infectados. Es decir, el bueno que tiene un negocio en ese servidor no sabe que hay un malo que le ha infectado y que está haciendo cosas malas desde su equipo.

Entonces, ¿qué es malo y qué es bueno? ¿Podemos filtrar, podemos establecer fronteras? Pues difícilmente. Estaremos filtrando un negocio legal cuya seguridad ha sido vulnerada. Por eso tenemos también muchas dificultades cuando hay un servidor que está haciendo algo malo y decimos "ese servidor, habría que bloquearlo". Y seguimos escalando y vemos que realmente hay un servicio de comercio electrónico totalmente lícito, además hay en el mismo servidor una red social totalmente lícita, pero alguien ha conseguido infectar ese servidor y está distribuyendo *malware* a nivel global. ¿Cómo se soluciona ese problema? Pues no es evidente. No puedes ir y capar la IP, digamos, para que no se acceda desde un determinado país, sino que habrá que resolver el problema de forma individual. Es un problema técnico y tendrá que resolverse en ese plano.

Un tema importante que también tenemos que tener en cuenta –esto es introducción pero es importante– se refiere a los medios con los que cuentan "los malos". Este es el entorno, quiero decir que esto es lo que vivimos y, si no somos conscientes de esto, difícilmente vamos a ser conscientes de cómo tenemos que abordar el problema con los menores. Sobre todo para no pensar que podemos hacer cosas que no podemos hacer. Y que la respuesta puede estar en otro sitio. Y hay ejemplos ya; Internet tiene ya un tiempo de vida suficiente como para que tengamos ejemplos en la mano de que "poner puertas al campo" en Internet es prácticamente imposible.

Los medios con los que cuentan los delincuentes son tremendamente sofisticados. En ámbitos como el de la pornografía infantil hay un modelo de negocio y los medios tecnológicos que utilizan para la ocultación y para el intercambio de contenidos son tremendamente sofisticados. Aquello que se

colgaba en un servidor, en una red social... No, eso no está ahí, no nos equivoquemos. Los contenidos de verdad perjudiciales están en redes anónimas, en particular existe la llamada red Tor, que además se da la paradoja de que es una red que inventó Navy y la puso a disposición del mundo y que ahora está siendo utilizada por los terroristas para intercambiar información y los pederastas para también intercambiar contenidos. Ahí hay un modelo de negocio. El nivel de sofisticación es terrible y las herramientas que ellos tienen son tan potentes o más que las de "los buenos". Y eso es un grave problema y nos mete en una carrera tecnológica muy compleja.

Y eso es una de las conclusiones también: hay una carrera tecnológica y una carrera por la persecución del delito que no podemos olvidar, por lo que debemos tener capacidades técnicas para abordar este problema. Hace pocos días salió una noticia de que se ha construido ya y están circulando por la Red planos de una pistola que se puede imprimir en una impresora 3D y que es perfectamente funcional. Hoy en día la tecnología está a disposición de todo el mundo y en el caso de Internet, ni siquiera tengo que disponer de una impresora 3D, puedo pagar 50 dólares y tengo a mi disposición una red de equipos infectados para hacer lo que me dé la gana. Esos negocios están en la Red, hay una profesionalización, hay un modelo de negocio, en el que unos desarrollan tecnología y la ponen a disposición de los demás y otros la utilizan para cometer delitos con ella. Por ejemplo, uno comete el delito robando, por ejemplo tarjetas bancarias, y lo pone a disposición de otro, que es el que se atreve a establecer una red de muleros para que al final el dinero salga. En el momento en que hay un modelo de negocio y hay unos ingresos, hay sofisticación y hay inversión en tecnología. Y a eso es a lo que nos enfrentamos.

Decía que la ocultación de la identidad es muy sofisticada. Estoy hablando de los temas de pederastia, pornografía infantil, ciberterrorismo y otros temas, pero utilizan los mismos medios, que son básicamente estas redes anónimas, donde la estrategia tecnológica es muy compleja. Es más, estamos en

ello, quiero decir que es un tema que nadie ha resuelto. Porque de hecho esto son unas redes que diseñó la Navy estadounidense para poder intercambiar información confidencial a través de Internet sin más medios que Internet, con la garantía de que esa información no podía ser vista por nadie. Pues esto, que socializó Navy igual que se socializó en su día Internet, se puso a disposición del mundo y ahora lo utilizan los malos, como suele suceder con esas cosas.

El tema de la identidad digital es complejísimo. Si no existen fronteras y no existe interoperabilidad en los modelos de identidad digital en los diferentes países, o hacemos negocios locales – cosa que creo que está muy claro que no es viable –, o el tema de la identidad digital es muy complicado. El DNI funciona en España, y es verdad, lo decía Borja, tenemos un Ferrari en el bolsillo, sin lugar a dudas. Pero de ahí a la obligación hay un paso muy grande. Si obligamos, por ejemplo –una cosa que se me ocurre–, a que todos los usuarios de Tuenti tengan que entrar con el DNI electrónico, Tuenti no puede tener un negocio internacional. Entonces hemos dejado a Tuenti frente a Facebook, por ejemplo, no en inferioridad de condiciones, sino es que lo hemos matado, entre otras cosas porque los niños se irán a Facebook. Y Facebook tratará diseñará su modelo de negocio con los menores.

Y es más, incluso aunque fuéramos capaces de imponer la identidad digital en todas las redes sociales, sospecho que los chavales se irían a otros medios, igual que antiguamente utilizábamos el IRC Chat. Con la propiedad intelectual ha pasado un caso muy parecido: empezamos con Napster para el intercambio de música. En Napster había un servidor centralizado, encontrábamos la música, nos la bajábamos gratuitamente. Y alguien dijo “ese repositorio es ilegal” y *¡pumba!*, Napster desapareció. Y tardó muy poco tiempo en aparecer esa distribución de contenidos a través de páginas web: cifrado, recortado con una aplicación que se llamaba Hacha, comprimido, etcétera. El modelo de negocio duró una temporada; aquello era incómodo, pero, bueno, uno se bajaba las canciones; como era, digamos, identificable, las sociedades de

gestión principalmente fueron a por ello; y de nuevo desapareció. Y entonces apareció el Napster sin servidor centralizado. Entonces, esto ya era más difícil, puesto que ya no había un servidor que tuviera la lista, sino que estaba distribuido. Este modelo ya era más complicado de eliminar. Pero de nuevo han ido apareciendo otros modelos de negocio diferentes, como el negocio de las descargas y luego el *peer-to-peer*. Y si el negocio de las descargas lo cortamos por aquí, el *peer-to-peer* ganará presencia. Por último, aparecen los *cyberlockers*; y ahora los *cyberlockers* están cifrados. Por ejemplo, el servicio Mega de king.com ahora está cifrado, ya nadie le puede pedir responsabilidades a Mega de los contenidos que alberga en sus servidores. Es decir, que la tecnología es tan flexible, tan versátil y avanza tan deprisa que va a haber una respuesta alternativa a cualquier cosa. Eso ya lo estamos viviendo, eso ya es una lección que tenemos aprendida.

Todo esto, y por hacer un poco el *conclusions first*, me lleva a la actividad a la que nos dedicamos y, por la experiencia que nos da esa actividad, a una aproximación muy realista. Y la aproximación es que probablemente se puedan hacer bastantes cosas, pero la aproximación tiene que estar centrada en el individuo. El individuo tiene que estar preparado para esto que va a vivir, donde las puertas al campo van a ser muy difíciles de poner. Entonces, tenemos que formar al individuo.

Formar al individuo se puede hacer de diferentes maneras. Por ejemplo, que el propio individuo acuda a formarse, cosa que por experiencia ya sabemos en Inteco que no suele suceder. El menor cuando entra en Internet, y más los pequeños, ni lo entienden; pero cuando entran van a ver los dibujos, van a jugar, los que son un poquito más mayores ya van a chatear,... Con lo cual, por ahí lo tenemos todo perdido.

La siguiente es: vamos a intentar que los padres naveguen con ellos y que tengan contenidos divertidos para poder formar a los menores. Tenemos un problema y es que los padres no perciben el riesgo. Todavía no han entendido

que esto es un grave riesgo para sus hijos. Es más, en una encuesta, en un trabajo de campo que realizamos hace un par de años obtuvimos un dato escalofriante y es que de todos los menores entrevistados, que fueron 1.250 en todo el país, solo el 1% decía que ante un caso de ciberacoso o de un problema en una red social, por ejemplo, acudiría a sus padres. El problema es terrible, ya no es una cuestión solo de tecnología ni de formación: es que los menores no confían en los padres para eso, entre otras cosas porque se avergüenzan, porque las tácticas utilizadas por los acosadores están muy orientadas a que el menor en un momento dado tenga algo de lo que avergonzarse, que puede ser una tontería, pero desde el punto de vista del menor ya tiene algo que ocultar. Y cuando el menor tiene algo que ocultar, el que está al otro lado se aprovecha.

Y luego, otro tema que yo considero que es básico es que el colegio como institución tiene que tener un protagonismo en todo esto, no solo en la formación, sino también el despliegue de protocolos de actuación frente a casos de ciberacoso. Estoy hablando un poco del "patio del colegio", esto es, que alguien está acosando al compañero de allí y está diciendo que es feo o le ha suplantado o lo que sea; entonces, esto es el patio del colegio, pero el patio del colegio digital. El centro educativo tiene que tener un papel en todo esto.

Y decía, teniendo claro que el menor no se va a aproximar a la formación, teniendo claro que los padres no están preparados, y que intentaremos llegar a ellos y lo hemos intentado en el pasado, tenemos la experiencia pero es muy difícil llegar a ellos, lo que sí que seguro no nos va a fallar es la escolarización. Y puesto que todos pasamos por el sistema educativo, ese es el filtro y el tamiz por el que tenemos que formar a los ciudadanos del futuro.

Por otro lado –y es un tema muy interesante también, y lo decía Borja–, el equipamiento en prácticamente todos los colegios y los contenidos digitales, son limitados y no siempre suficientes. ¿Qué le pasa al profesor que tiene que llevar a los niños al aula de informática? Este colectivo necesita contenidos de calidad en materia de seguridad de la información –que se pueden hacer muy atractivos,

luego veremos un par de ejemplos– para dar una clase amena y que fuera del interés de los alumnos.

Empiezo con mi presentación, que voy a ir muy rápido, insisto, porque creo que es importante que ustedes conozcan las capacidades y los organismos que trabajamos en este ámbito. Inteco es una sociedad estatal, adscrita al Ministerio de Industria, Energía y Turismo a través de la Secretaría de Estado de Telecomunicaciones. Inteco lo preside el secretario de Estado, don Víctor Calvo-Sotelo. El accionista único es Red.es, como ha mencionado antes Borja Adsuara. Somos, dentro de la estrategia de la secretaría de Estado, entidad de referencia en confianza digital y en ciberseguridad, de lo que hablaremos luego en el ámbito de la Agenda Digital para España.

Y los tipos de actividades que desarrollamos son por un lado la prestación de servicios ¿Qué tipo de servicios? Pues servicios claramente preventivos para intentar evitar que las cosas sucedan, para desplegar servicios de alerta temprana monitorizando lo que está sucediendo en Internet. Así, los incidentes que están teniendo otros los utilizamos para analizar cuál es el problema e intentar desplegar soluciones antes de que se materialice la amenaza, como decimos nosotros. También servicios reactivos, cuando se produce un incidente. Puesto que cuando esto ocurre, las empresas están absolutamente perdidas, es el caos; ese día descubren hasta qué punto sus sistemas de información son críticos para su negocio. Ahora mismo estamos trabajando con un caso en el que hay un virus, un *ramsonware*, que infecta a los servidores corporativos, cifra los archivos que hay ahí (de recursos humanos, financiero, control logístico o lo que sea) y entonces pide un rescate de, por ejemplo, 5.000 dólares por descifrar aquellos ficheros. La mayor parte de las empresas lo que nos preguntan es "¿cómo les pago?" No preguntan "¿cómo desinfecto?" Están tan desesperados, necesitan tanto sus sistemas de información que lo que quieren saber es cómo pagar. Evidentemente, nosotros les decimos: "quieto, tenemos respuesta.

Mándanos información y nosotros acudimos en tu rescate". Ahí hay un problema muy grave que vemos todos los días.

Y luego, por supuesto, prestamos servicios de concienciación y de sensibilización, que son tan importantes en todos los ámbitos, incluidos los empresariales.

También realizamos investigación, por dos motivos. El primero, porque necesitamos tecnología para poder prestar esos servicios; esa tecnología en general no está en el mercado porque el concepto CERT es relativamente reciente, por lo tanto tenemos que desarrollar tecnología y tenemos que tener capacidades para desarrollar tecnología. Y luego, por otro lado, porque necesitamos saber cuáles son las nuevas tendencias en amenazas. Alguien lo ha preguntado, no recuerdo quién ha sido: ¿estamos viendo qué es lo que va a suceder en el futuro? Pues sí, claro que lo estamos viendo, lo estamos viendo constantemente; necesitamos estar investigando cuáles son las nuevas tendencias porque tenemos que tener soluciones preparadas para el día en que las cosas sucedan. Y ojo, no siempre lo conseguimos, lo conseguimos en un porcentaje "equis" de las ocasiones.

Y como decía, trabajamos en coordinación, porque la ciberseguridad es un tema en el que, si no es con la colaboración con otros, es imposible ser efectivo. No solo colaboración en el ámbito nacional, que también es importante, sino muy especialmente en el ámbito internacional, cuando estamos de alguna forma atravesando fronteras de carácter jurisdiccional.

¿Cómo hacemos esto? Pues ya decía, Inteco es confianza y ciberseguridad. Ponemos mucho énfasis en generar inteligencia, recibimos volúmenes ingentes de datos, de dato crudo a través de nuestra sensorización; nosotros tenemos sensorizada una parte importante de lo que sucede en Internet, ojo, sin saber quién es la persona y sin saber cuáles son los contenidos que circulan por allí, eso ni lo sabemos ni lo queremos saber; simplemente obtenemos información de posibles amenazas, de focos de amenaza, de

generadores de *spam*, de quién está inyectando *malware*, quién está haciendo ataques de denegación de servicio... Generamos esa inteligencia que nos permite dar alerta temprana a las instituciones.

Damos soporte, como decía, imprescindible cuando se produce un incidente y tratamos de dinamizar, por qué no, la industria española de ciberseguridad, que es pequeña pero potente.

Y tenemos nuestros valores de excelencia, cooperación, servicio, sostenibilidad, etc.

¿A quién prestamos servicio desde Inteco? Pues prestamos servicio a todos esos sectores de la sociedad: a los ciudadanos, con especial atención a los sectores más vulnerables, que son los menores (objeto de este debate); a las empresas, y en particular a los ISP y prestadores de servicio en la Sociedad de la Información –que son una gran parte de la solución, no del problema –, así como a los sectores estratégicos. Los sectores estratégicos ahora mismo tienen un problema, y es que el ciberespionaje industrial está a la orden del día. Grandes empresas de defensa, bancos, empresas de telecomunicaciones están sufriendo espionaje industrial, están siendo infectados con *malware* destinado a robar su propiedad intelectual, con lo cual estamos perdiendo competitividad internacional, sin lugar a dudas.

Damos servicio también al dominio.es, al ESNIC que gestiona Red.es y también estamos trabajando en dar soporte en materia de respuesta a incidentes y de alerta temprana a RedIRIS (que también gestiona Red.es), la red académica y de investigación que une a los centros universitarios y organismos de investigación.

Eso es de alguna forma lo que está enmarcado dentro de la Agenda Digital para España, y que forma parte de nuestro contexto de referencia como instrumento político estratégico. Y junto con la Agenda, está el convenio que ha mencionado el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información con la Secretaría de Estado de Seguridad, el cual nos permite

trabajar en dos ámbitos más: uno, que es la lucha contra el ciberdelito y la ciberdelincuencia con Fuerzas y Cuerpos de Seguridad del Estado, y otro, en la protección de las infraestructuras críticas en aquello que afecta a los sistemas de información que dan soporte a esas infraestructuras, ya sea energía, transporte o banca, entre otras.

Ese es nuestro marco de actuación, que no es pequeño.

No me voy a parar en las iniciativas de referencia porque las ha contado muy bien el secretario de Estado. Simplemente, llamo la atención sobre un tema, y es que en Estados Unidos, que van un poquito por delante de nosotros en este tema, han decidido que deben tener contenidos de seguridad en los itinerarios educativos como algo imprescindible para la competitividad de su sociedad del futuro. Eso es algo en lo que nos tenemos que fijar.

Y luego, por supuesto, las iniciativas de la Unión Europea, en particular la Estrategia europea en favor de una Internet más adecuada para los niños, que es lo que digamos que viene más al caso en el día de hoy.

En cuanto a las iniciativas de referencia en el ámbito nacional, hay muchas: se puede destacar el Observatorio de la Infancia, el Inteco, Red.es... Ahí se incardinan las iniciativas de la SETSI. Son muchas. En algunos casos podría haber algún solapamiento, y también podría suceder que haya alguna cosa interesante que se nos esté escapando, es algo que en ese grupo de trabajo que ha mencionado Borja, que yo creo que va a ser un gran éxito, identificaremos y trataremos, tanto para que aquello que no se está haciendo se haga, como para que aquello que se está haciendo dos veces procuremos hacerlo solo una vez y mejor.

Esta es la actividad de Inteco; esta es la estrategia de Inteco con respecto a los menores. Estamos participando en el diseño estratégico; gracias a que tenemos experiencia y tenemos conocimiento, parece razonable que de alguna manera influyamos en aquello que se va a hacer. Prestamos servicios de ciberseguridad intentando encontrar un entorno más adecuado para los niños.

Trabajamos en el desarrollo de soluciones tecnológicas para ayudar a las Fuerzas y Cuerpos de Seguridad del Estado a perseguir este tipo de ciberdelito, insisto, tan sofisticado en muchos casos. Y luego, por supuesto, trabajamos en la concienciación y sensibilización para elevar la cultura de seguridad de los menores, de los padres y de los educadores, incidiendo en la importancia de trabajar todos los colectivos, no exclusivamente el de los menores.

Y luego, por último, tenemos una capa transversal de colaboración sin la cual sería imposible nuestro trabajo. Es importante que veamos la correspondencia que hay entre esa estrategia y la mencionada Estrategia europea en favor de una Internet más adecuada para los niños, porque se cubren todos los ámbitos que se desarrollan en esa estrategia, y esto no es fortuito, esto es que lo hemos trabajado en paralelo y hemos visto que la estrategia europea tiene muchísimo sentido y ¿por qué no empezar ya a dar respuesta a algo que en cualquier caso va a ser preceptivo?

En cuanto a la participación en el diseño estratégico, pasaré directamente a la Agenda Digital para España y al convenio con la Secretaría de Estado de Seguridad, por ir acortando un poco. La Agenda Digital para España ya la ha comentado el secretario de Estado: hay un objetivo, que es el objetivo IV, que pretende reforzar la confianza en el ámbito digital, y en él está desarrollada en seis puntos la estrategia de Inteco, que cubre muchos de los aspectos de los que hemos hablado hoy.

Uno, extender la participación de Inteco a todos los ámbitos de la confianza. En este sentido, había ámbitos en los que de alguna manera no trabajábamos (el ámbito de la privacidad no es un ámbito en el que estuviéramos trabajando directamente). Y se reconoce también de alguna manera el trabajo de Inteco, la implicación de Inteco en el ámbito de los menores.

Otro, situar a Inteco como una entidad de referencia en ciberseguridad para sectores estratégicos. Insisto, esto es nuevo, entre nuestros clientes no

estaban antes estos sectores, que ahora sí lo están junto a empresas y ciudadanos.

En tercer lugar, esto es muy importante, establecer las capacidades necesarias para estudiar los riesgos emergentes, que era lo que comentaba antes, estar preparados para lo que va a venir. Saber que Facebook, por ejemplo, ha anunciado que su aplicación Graph permite en un momento dado encontrar restaurantes en función de los restaurantes que han visitado mis conocidos o permite saber qué cosas debo visitar en una ciudad porque sé automáticamente que esa ciudad la han visitado mis conocidos (las implicaciones desde el punto de vista de la privacidad son terribles). Tenemos que estar viendo todas estas cosas para ver dónde están los agujeros en la privacidad, por ejemplo, como sucedió en su día con el Timeline, con la biografía que se introdujo también en Facebook. Hay que alertar a los usuarios y decirles: "Oye, esto es fantástico, pero mira, esta pestañita de aquí si la pones de esta manera sucede esto y las implicaciones son estas; esta pestañita de aquí si la pones así, sucede de esta otra manera,… Entonces, te recomiendo por defecto esta configuración". Eso, que parece algo muy simple, es importantísimo, porque el usuario cuando se enfrenta a unas opciones que cada vez son más difíciles de entender y cada vez son más numerosas, necesita que alguien le diga "mira, si vas por aquí vas bien, si vas por aquí te puede pasar todo esto".

En cuarto lugar, se encuentra el desarrollo de programas de sensibilización, concienciación, educación y formación, que comentaba antes.

Tras estos programas, hay un planteamiento en el que ya estamos avanzando, relativo al desarrollo de contenidos de seguridad para su inclusión en los itinerarios del sistema educativo. Estamos avanzando, intentando lanzar una experiencia piloto, para lo cual hemos tenido reuniones con una dirección provincial y con una consejería de Educación. Desde luego, la receptividad es muy grande y hay interés por parte de numerosas comunidades autónomas, porque esto tiene sentido sin lugar a dudas.

Y por último, y muy importante, hay que hacer un seguimiento y un diagnóstico de lo que está sucediendo. Y aquí también tenemos algunas barreras que superar.

Inteco dispone también de otro instrumento estratégico, el convenio entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, que básicamente consiste en unir esfuerzos y capacidades para intentar entre todos "parar el tsunami", por decirlo de alguna manera. ¿En qué ámbitos? Pues en la lucha contra los ciberdelitos y contra el ciberterrorismo, con las Fuerzas y Cuerpos de Seguridad del Estado, y ahí en particular hay una línea que es la protección de los menores; el alcance es mucho mayor, pero por centrarme es la línea de protección de los menores, y la protección de los menores yendo al delito más grave, que es el delito de la pederastia y la explotación infantil; ayudar a las Fuerzas y Cuerpos de Seguridad del Estado a disponer de tecnología para poder captar evidencias en los registros. Ahora los registros ya no son como antes, el agente de las FCSE no se lleva un libro de cuentas o un cuadro, no; tiene que recoger evidencias electrónicas y que además lo vea un juez. O incluso llega a un registro y se encuentra con ordenadores, discos duros, discos duros externos, USB, DVD, etcétera y un registro no puede durar un mes, no va a estar el secretario judicial con el agente un mes, eso es imposible. Por ello, necesitamos facilitarles herramientas para que en un registro haya tecnología que ayude al profesional a buscar aquellas evidencias que hacen más probable que allí se esté cometiendo un delito.

Y luego un trabajo muy importante es la lucha contra las *botnets*, las redes de ordenadores zombi, u ordenadores cuyos usuarios no saben que están infectados y controlados y que constituyen una infraestructura muy potente para cometer cualquier otro tipo de delitos. Esto da para muchas horas. Por citar un ejemplo, una *botnet* que desarticuló el FBI el año pasado, y que contó con la colaboración de Inteco en la parte de España, había afectado a 5 millones de

máquinas en el mundo, una sola *botnet*, y en España había 500.000 equipos infectados. Y *botnets* hay todos los días, cada mes. Por supuesto, la gente no lo sabe. El individuo puede, en un momento dato, detectar que su conexión a Internet va un poco más lenta y a lo mejor está participando en un ataque de denegación de servicio al Senado y no lo sabe. Lamentablemente, esto funciona así. Una *botnet* es una infraestructura latente y se utiliza para determinadas cosas.

Junto con la lucha contra los ciberdelitos y contra el ciberterrorismo, trabajamos en la protección de las infraestructuras críticas también con el Ministerio de Interior, con el Centro Nacional para la Protección de Infraestructuras Críticas, en lo que creo que es un modelo de racionalización. El Centro Nacional para la Protección de Infraestructuras Críticas del Ministerio de Interior necesitaba tener capacidades de respuesta a incidentes en seguridad de la información, y decidieron que en vez de reinventar la rueda se iban a apoyar en las capacidades, en el conocimiento del CERT de Inteco, y de esa manera hemos ampliado de alguna forma la clientela de nuestro CERT, y junto con el Ministerio de Interior estamos ya dando respuesta a los incidentes que afectan a las infraestructuras críticas; incidentes que todavía no son muy numerosos (exceptuando el caso de la banca), pero que lo serán sin lugar a dudas. En el momento en que nuestra red eléctrica sea una red con cierta capacidad de inteligencia, sin lugar a dudas va a ser un foco de atención para los ciberdelincuentes y para los ciberterroristas.

Y además, trabajamos con ellos en difusión, concienciación, formación y capacitación, que esto es transversal pero en muchos casos es lo más importante.

De un vistazo, esa es la actividad que desarrolla Inteco: servicios de prevención y asistencia, útiles gratuitos y enseñamos a los usuarios a manejar esos útiles gratuitos (gestores de correo para niños, filtros para niños, herramientas, por supuesto, antivirus, control de horas de uso del ordenador, etc.), contenidos para la concienciación para diferentes rangos de edades –luego

voy a enseñar muy rápidamente la web para que veamos cuál es el modelo–, y luego, muy importante, una línea de formación a padres y educadores (insisto, esa es la línea en la que más expectativas tenemos, por experiencia, de que funcione).

Y luego, junto con todo eso, pues desarrollamos tecnología e investigamos para poder dotar de herramientas a las Fuerzas y Cuerpos de Seguridad del Estado, colaboramos con todos los agentes que tienen algo que decir en esta materia, hemos impartido también charlas presenciales, que nos da un *feedback* muy interesante también de los padres o de los tutores, incluso también de los niños, y nos permite redefinir nuestros servicios; y ahora estamos trabajando en esa propuesta de contenidos educativos.

En el ámbito de los servicios de ciberseguridad, en cuanto al contexto simplemente he tratado de poner ahí un poco las iniciativas que hay, para que veamos que en general no solemos estar solos, hay muchos haciendo cosas. En cuanto a esos servicios de ciberseguridad, los prestamos a partir del portal Menores OSI y también a través de los perfiles de las redes sociales, que son muy interesantes porque están muy a mano y, si alguien se apunta a nuestros perfiles estará recibiendo consejos muy interesantes y alertas muy interesantes. Es decir, todos los días aparecen aplicaciones maliciosas en las redes sociales y la gente no lo sabe. Entonces, un perfil como este nos sirve para alertar de situaciones del tipo “esta aplicación es muy bonita, pero lo que va a hacer es infectar tu equipo”. Esta es una labor constante a través de los perfiles de redes sociales, que es la forma de estar “embebido” dentro de la propia red social y ser un individuo más de esa red social.

Hemos dado más de 500 alertas y destacados sobre riesgos para los menores. Y luego, mantenemos una relación de herramientas gratuitas de control parental, protección en todas las líneas. Y colaboramos, insisto, con otros CERT del ámbito internacional; en particular nosotros colaboramos con 273 CERT en el ámbito internacional, que es con los que nos relacionamos día a día.

Y en cuanto a las actividades que tenemos previstas para el futuro, recogidas en la Agenda Digital para España, está el refuerzo de la colaboración público-privada en detección, prevención y respuesta. ¿Por dónde hemos empezado? para que esto no parezca una frase vacía, os diré que por Tuenti, como no puede ser de otra manera. Nosotros ya tenemos presencia en Tuenti, pero vamos a intentar hacer que nuestra presencia en Tuenti sea todavía más efectiva mediante un esquema de colaboración. Y estamos a punto de firmar un convenio con este objetivo.

Desarrollamos soluciones tecnológicas para el ciberdelito, como decía. Ahí los protagonistas son las Fuerzas y Cuerpos de Seguridad del Estado, que son los que tienen que perseguir el delito, sin lugar a dudas.

Estamos desarrollando herramientas para que sean capaces de automatizar la actividad que hacen los policías. Necesitamos desarrollar sistemas de visión artificial para que un policía no tenga que ver millones de imágenes y millones de vídeos, sino que haya un sistema que sea capaz de decirle “esto tiene pinta de ser, esto tiene pinta de no ser; aquí hay un cuadro que tiene pinta de parecerse mucho a ese cuadro que está en la base de datos y que está asociado a otro caso; los metadatos de esta cámara se parecen a los metadatos de aquella otra cámara; las evidencias que había en el sistema operativo donde se capturó esto se parecen a estas y a estas, etcétera”. Conseguir que la labor policial de establecer relaciones, buscar evidencias y tirar del hilo sea más sencilla, porque estamos hablando de un volumen tan grande que la actividad policial se complica muchísimo. Y lo que sucede hoy es que el número de casos que se pueden perseguir, a pesar de la abnegación y de la capacidad de trabajo y de sacrificio que tiene la Brigada de Investigación Tecnológica de la Policía y el Grupo de Delitos Telemáticos de la Guardia Civil, es la que es porque no se puede llegar a más.

Estamos desarrollando también una herramienta para la detección de evidencias en registros.

Y luego, estamos empezando a realizar ya algunos experimentos de monitorización de fuentes abiertas, redes sociales, de redes de intercambio (*peer-to-peer*) y de esas redes anónimas que comentaba anteriormente. Hemos hecho una primera aproximación de monitorización de Tuenti y hemos encontrado que hay no uno, sino muchos perfiles de Tuenti que están ofreciendo contenidos y solicitando abiertamente contenidos de pornografía infantil. Todo esto hay que perseguirlo y sabemos que es muy complicado. Después de identificar estas situaciones de riesgo hay que acudir a Tuenti para que nos dé evidencias de cuáles son las IP desde las que se han conectado y se han subido esos contenidos. Todo esto es muy complejo: identificas un perfil – evidentemente nadie se da de alta con su nombre y apellidos – y entonces empieza una investigación hacia atrás que choca con Tuenti y con la legislación de Tuenti. En fin, todo esto es muy complicado, pero en ese camino hay que avanzar, sin lugar a dudas.

Se pueden hacer muchas cosas, hay que formar al individuo, pero a la vez hay que perseguir a "los malos". Eso siempre, seguro. Si no, el problema cada vez es mayor.

En este caso estamos finalizando los desarrollos. Algunas de estas herramientas serán utilizadas por Fuerzas y Cuerpos de Seguridad del Estado de ámbito europeo porque así nos lo pide la Comisión Europea.

Llegamos a la parte de concienciación y sensibilización y formación, que es tan importante. En este campo, ¿qué necesidades detectamos? Que los educadores necesitan orientación y formación, si no, difícilmente van a ser capaces de trasladar esa información. A día de hoy no se está haciendo de un modo oficial, no hay –que sepamos– nadie que tenga un programa oficial de formación a formadores para que luego puedan dar clase a los alumnos, y sí existen actividades o iniciativas más o menos dispersas. Se requieren contenidos de seguridad de la información, no basta con que estos profesionales estén formados, sino que tenemos que darles contenidos de seguridad atractivos para

que eduquen a los chavales sin aburrirles. Esta es una premisa básica: hay que contar las cosas de un modo ameno –y ahora veremos cómo lo intentamos nosotros– e introducir esos contenidos en el itinerario educativo.

Y hay diagnóstico, pero no somos muchos los que estamos haciendo el diagnóstico: el 50% o el 60% estamos sentados aquí ahora mismo. Y, por otro lado, en general no existe homogeneidad en ese diagnóstico, con lo cual se dificulta la comparación. Y por otro lado, no tenemos datos consolidados de todas las denuncias o de todos los incidentes que se están reportando en los diferentes sitios, no existe una ventanilla única, y por tanto no tenemos ese dato para decir qué es lo que está pasando de verdad. Yo sé lo que está pasando en cuanto a lo que me está llegando a mí, pero no sé lo que le está llegando al de al lado, ni sé lo que le está quedando al de al lado ni lo voy a saber razonablemente nunca, salvo que nos pongamos entre todos de acuerdo. Ahí hay un punto débil y una oportunidad.

Por seguir con la concienciación y sensibilización, el portal Menores OSI se ha inventado para públicos de edad, de 5 a 8 años, de 9 a 12, de 13 a 17, y luego ya están los padres y los educadores. Desde que se lanzó el portal hemos tenido más de 585.000 páginas vistas que, si bien no parece mucho, lo es teniendo en cuenta que son contenidos de seguridad; no es mucho teniendo en cuenta que es un portal de Internet, pero va aumentando el interés. Un reto es hacer que esto se conozca más y que se utilice más.

Además, se han desarrollado guías y materiales de concienciación. En particular hay publicadas seis guías en materia de protección del menor en Internet que son interesantes y que han tenido 48.000 descargas. También hemos tenido 63.000 reproducciones de nuestro canal Menores OSI en YouTube; hemos desarrollado juegos educativos; tenemos 40 recursos pedagógicos recopilados; ponemos a disposición del público una plataforma de formación on-line en la que actualmente se ofrece un curso para padres y educadores, con más

de 1.700 inscritos a pesar de la reciente publicación de esta formación y del que sabemos que va a tener muchísima demanda.

Siguiendo con las actividades de concienciación, hemos dado más de 90 charlas, en las que hemos tenido a más de 7.000 asistentes. Como hemos visto que el impacto de nuestras charlas no es suficientemente grande estamos haciendo ya experiencias piloto on-line para llegar a muchísima más gente con nuestras charlas. E insisto, esta actividad, que es intensiva para nosotros en recursos humanos, nos obliga a desplazarnos, nos obliga además a llevar a una persona con un perfil experto y que, mientras que está haciendo esto, no está haciendo otra cosa, pero el *feedback* que recibimos de los oyentes es muy importante para nosotros.

También quiero mencionar el desarrollo de contenidos que hemos realizado para el canal Clan TV de Televisión Española, que es probablemente lo más visto por los niños, y tenemos ahí un personaje que se llama Mosi que es un marcianito que empieza a contarles cosas a los niños de cómo se utilizan las tecnologías.

En redes sociales tenemos los perfiles que nosotros llamamos "pienso, luego clico" y que tienen ya más de 3.000 seguidores en Tuenti y en Facebook, que me va a decir Borja que es muy poco, pero ahí estamos, intentando subirlo.

Y, por último, hemos mantenido durante los últimos años más de 50 indicadores sobre menores, de los que muestro algunos ejemplos en la presentación.

Y como Borja, me gustaría extraer algunas conclusiones, también, por supuesto, de carácter personal de todo esto que hemos hablado.

La primera conclusión, y como transversal y de igual manera que he empezado mi intervención, es mejorar en general el nivel de ciberseguridad de la Red, lo que afecta a todos los sectores de la sociedad, porque si no, difícilmente vamos a poder proteger a nuestros menores. Ahora mismo existe un elevadísimo número de iniciativas que pueden provocar efectos perversos, como

son la gran dispersión de las actuaciones, lo cual genera confusión por parte del usuario, de quien va a consumir esos servicios. No hablo solo de contenidos, sino también de canales de soporte o de denuncia. La ciudadanía tiene que tener muy claro una marca a la que va a acudir cuando tenga un tema de menores. Ahí va a ser muy interesante este grupo de trabajo que nos permitirá a todos aunar esfuerzos, evitar duplicidades, y que no se quede por cubrir ningún ámbito que debería estar cubierto.

A día de hoy hay un ámbito que no está cubierto, que son los protocolos de actuación en los colegios. Por tanto, la actuación que se requiere pasaría por desarrollar esos protocolos – para lo cual ya existen ideas e iniciativas importantes en la materia – y por que los colegios asuman que tienen una responsabilidad como institución en todo esto. Eso tampoco es un detalle menor.

Es necesario elaborar la cultura de seguridad entre los más pequeños, para lo cual necesitamos contenidos específicos en el itinerario educativo, esto también consideramos que es clave.

Debe dotarse a los padres y educadores, que son los que tienen que utilizar estos contenidos, de los conocimientos necesarios (ahí hablaba también de los protocolos de actuación).

Y volviendo otra vez a lo mismo, es imprescindible habilitar fórmulas de colaboración que permitan aunar esfuerzos, evitar duplicidades, tener indicadores saneados y todo este tipo de cuestiones.

Y yo creo que he ido muy rápido, pero espero haber sido claro. Y muchísimas gracias por mantener la atención después de tantas horas.

Sin más, por mi parte quedo abierto a las preguntas que consideren formularme.