CONVERSATORIO: DESAFÍOS DE LA NUEVA LEY MARCO DE CIBERSEGURIDAD

Organizador:

Centro de Estudios de la Administración del Estado,
de la Contraloría General de la República

Moderador:

Ricardo Arancibia, oficial de ciberseguridad de la Contraloría General de la República

Participantes:

Marco Antonio Álvarez, Carlos Bustos, Kenneth Pugh, Claudia Santa Ana

Fecha:

17 de julio de 2024

Lugar:

Auditorio de la Contraloría General de la República y transmisión en *streaming*

1. Palabras iniciales

Dorothy Pérez Gutiérrez[1]

El objetivo de este encuentro es interiorizarnos, prepararnos y, sobre todo, estar atentos frente a la próxima entrada en vigencia de la ley Nº 21.663, que regula las acciones de ciberseguridad de los organismos públicos, pero también su relación con las entidades privadas y establece una serie de elementos muy relevantes.

1 Contralora General de la República (S).

Todos sabemos que se trata de una ley marco, así que el detalle vendrá en el reglamento, pero contiene desde ya algunos requisitos mínimos para enfrentar incidentes de ciberseguridad. Un tema relevante son las atribuciones y deberes de los organismos del Estado en la materia. Además establece mecanismos de control de supervisión y responsabilidades frente a las infracciones que se puedan producir y definiciones significativas sobre auditorías de seguridad. Lo interesante es cómo va a operar esto en el aparato público en general y también en el ámbito privado.

Esta ley crea instituciones que prestarán servicios esenciales y de importancia vital, así como fija deberes para la continuidad operacional ante incidentes.

Asimismo, da definiciones relevantes sobre ciberataques e incidentes en esta materia y crea una institucionalidad nueva. Esto es muy importante y, en atención a su facultad de dictaminar, la Contraloría va a tener que hacer muchos análisis al respecto.

Esta ley crea:

1) un equipo nacional de respuesta a incidentes de ciberseguridad;

2) la Agencia Nacional de Ciberseguridad —ANCI— que:

a) asesora al Presidente de la República,

b) dicta protocolos,

c) fija estándares en estas materias y

d) administra un registro de incidentes de ciberseguridad.

3) el Consejo Multisectorial de Ciberseguridad, que asesora a dicha agencia para buscar las mejores maneras de prevenir y enfrentar este tipo de situaciones y salir rápido de los problemas cuando se producen.

Todos estos temas serán tratados por nuestro expositor principal y los panelistas.

En suma, esta legislación crea una institucionalidad y, sobre todo, procura impulsar medidas para la seguridad de Chile en este ámbito, para que podamos prevenir, reportar en el menor tiempo posible y resolver con la mayor celeridad los incidentes de ciberseguridad que podamos sufrir. Todo esto desde el punto de vista de la seguridad tridimensional, que es un concepto y una mirada clave que debemos tener presentes para el debido resguardo de nuestro país y de la ciudadanía. Esa es nuestra obligación y con el apoyo de los expositores, hemos organizado este evento, a través del Centro de Estudios de la Administración del Estado.

2. El punto de vista de la Asociación Chilena de Ciberseguridad

Marco Antonio Álvarez Mesa[2]

La Asociación Chilena de Ciberseguridad es una organización de derecho privado, sin fines de lucro, que representa a entidades del sector público, del sector privado y de la academia y que, junto a sus miembros y aliados estratégicos, comparte un profundo interés por el desarrollo y la promoción de la ciberseguridad, en aras de un mundo digital interconectado y seguro.

En este contexto, la Ley Marco de Ciberseguridad es un hito relevante para el quehacer de la alianza, por lo que celebramos su reciente promulgación y agradecemos a las autoridades del Poder Ejecutivo y del Poder Legislativo por habernos entregado la oportunidad de dar a conocer nuestro punto de vista sobre el proyecto de ley que conocimos durante su tramitación.

Es evidente que los servicios en la nube, la pandemia, el trabajo remoto, el uso de la inteligencia artificial y la computación cuántica gatillaron la inminente transición hacia la transformación digital en diversos sectores de la economía. Como suele ocurrir, la incorporación de nuevas tecnologías trae consigo innumerables beneficios, pero también mayores amenazas y riesgos que desafían nuestras soluciones para contrarrestarlas, ya que los ciberataques se van perfeccionando para burlar la ciberseguridad.

Por otra parte, constituye un incentivo para los ciberdelincuentes el hecho de que gran parte de la información almacenada por los usuarios sea de alto valor, por lo cual intentarán vulnerarla y sustraerla ilícitamente.

De ahí que, desde la alianza, hagamos un llamado para contar con una institucionalidad robusta en ciberseguridad, lo que implica promover iniciativas regulatorias que nos hagan un país más seguro, que entregue confianza para el desarrollo de su economía y nos posicione como líderes de la región.

En particular, debemos aunar esfuerzos para contar oportunamente con el reglamento de la Ley Marco de Ciberseguridad, con la Agencia Nacional de Ciberseguridad y con una ley de protección de datos personales robusta.

Estimamos que el Foro Nacional de Ciberseguridad es una instancia relevante que complementa lo anterior, por lo que desde la alianza invitamos a todos los actores a participar activamente en él.

2 Es presidente de la Alianza Chilena de Ciberseguridad.

En la alianza apoyamos decididamente la capacitación continua en ciberseguridad, para así disminuir la brecha de talentos que se observa en el mercado. Por las razones que hemos expuesto, sugerimos un aumento de la inversión en tecnología de ciberseguridad.

Por último, promovemos firmemente la colaboración entre los distintos actores. Creo que los convenios de cooperación de la Alianza Chilena de Ciberseguridad con la Contraloría General de la República y con el Senado son muy buenos ejemplos de colaboración y, como es muy bien sabido, en ciberseguridad no se compite, se colabora.

3. Desafíos de la nueva Ley Marco de Ciberseguridad

Kenneth Pugh[3]

Una ley marco permite dar un paraguas a algo que es esencial para nuestra vida en el ciberespacio: la protección de los datos de las personas, de infraestructura que estas usan, de los servicios de los que dependen aquellas. Entonces, esto no es mera tecnología, sino nuestra vida digital, nuestra permanencia en este ciberespacio.

Esta ley es un compromiso de Estado que ha trascendido los Gobiernos de turno y quiero destacar eso como punto político. En el segundo Gobierno de la presidenta Bachelet, ella elaboró una política nacional de ciberseguridad que tenía como primer elemento la construcción de institucionalidad y la generación de una agencia nacional de ciberseguridad. Esa política fue desarrollada en el Gobierno del presidente Piñera a través de un mensaje presidencial que fue ingresado al Senado, para posteriormente ser retomada por el presidente Borić, cuyo mensaje presidencial se tramitó en 18 meses. Esto significa que, en 18 meses, fuimos capaces de llegar a un acuerdo político transversal.

Quiero destacar la altísima votación obtenida en la Cámara de Diputados, 143 presentes, todos a favor, nadie en contra y nadie se abstuvo. Ver el tablero de la Cámara de Diputados en color verde es algo que uno nunca pensaba que podía ocurrir. Eso mismo pasó después en el Senado. Por eso les voy a contar, más que la parte técnica, la trastienda que permitió sacar adelante este gran esfuerzo nacional.

3 Es senador por la 6ª circunscripción de la región de Valparaíso, miembro permanente de la Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación entre 2022 y 2023.

El 26 de marzo de este año fuimos convocados a La Moneda. A las 7:30 se había invitado a 120 parlamentarios y se pensaba que llegarían 50 o 60. Llegaron 130. Ese día se hizo la firma, vale decir, el nacimiento de este gran esfuerzo político que vio finalmente la luz en el Diario Oficial el 8 de abril. Esa es la fecha que tenemos que considerar para calcular los plazos de entrada en vigencia de la agencia y, más importante, de los reglamentos.

Quiero destacar la gran participación femenina en el desarrollo de nuestro proyecto, a pesar de la gigantesca brecha de género que existe en ciberseguridad, un problema común en todo el mundo. Sabemos que las mujeres representan menos de un 15 % de los profesionales que trabajan en este ámbito, por lo que es un desafío incorporar más, no solo ingenieras, sino también abogadas y cientistas sociales.

Esa misma semana del 8 de abril, junto al coordinador nacional de ciberseguridad, Daniel Álvarez, fuimos invitados por el Gobierno de España, la OEA y el BID, que financiaron la asistencia al evento más importante de tecnologías de información y seguridad organizado por el Centro Nacional Criptológico español. España es el segundo país europeo mejor calificado y es un referente mundial, pues tiene un buen sistema y habla en español. En ese primer evento, solo se habló de la Ley Marco de Ciberseguridad.

Entonces, no solo tenemos el acuerdo político detrás para decir: «vamos a avanzar y vamos a avanzar bien», también contamos con reconocimiento internacional y podemos sentirnos orgullosos, porque estamos construyendo un país mejor, que va a dar muchas oportunidades y protección a aquellos que tomen este camino digital.

Esto es algo concreto, Chile va avanzando, es un referente. Primero protegemos la información, pero después la usamos. Los datos son el combustible que tiene esta nueva maquinaria, pero la maquinaria en sí tiene capacidad para hacer cosas, le sacamos el provecho después con la inteligencia artificial.

Desde el encuentro en España, han sido demandadas todo tipo de conferencias. Yo ayer estaba exponiendo en Perú, Daniel Álvarez está en Washington y lo menciono porque nos toca estar en múltiples lugares. De aquí me voy a la Embajada de Rumania, porque su Gobierno me va a condecorar con la orden al mérito en el grado caballero, precisamente por acciones que hemos desarrollado en este ámbito.

Rumania ganó el concurso europeo para instalar en Bucarest el Centro de Competencias Europeas de Ciberseguridad y, por eso, desde temprano, lo identificamos como un país con el que queríamos relacionarnos. Antes del concurso, apoyábamos al Instituto Nacional de Ciberseguridad español, pero ganó Rumania, por su talento y capacidad. Todo lo que les estoy contando

está en construcción, es decir, veremos un mundo digital con nuevas normas y actores, donde las oportunidades son para todos y este es el primer mensaje: oportunidades.

¿Qué es lo que dice nuestra ley? Primero, define una institucionalidad que necesitamos para que el director de esta nueva agencia sea capaz de poder asesorar al presidente y dirigir toda esta institucionalidad, además de vincularse con el mundo, pues en ciberseguridad no existen fronteras. Ello, toda vez que estamos a un clic de distancia de todo el mundo, a un clic de las oportunidades y a un clic de los riesgos, porque las amenazas ya no provienen de jóvenes que están tratando de decir que saben, sino de bandas de crimen organizado con una industria que usa al máximo sus herramientas, incluida la inteligencia artificial, para destruirnos.

El *ransomware*[4] es quizá lo peor y lo estamos viendo todos los días, no hay empresa que se salve. Somos testigos de casos increíbles en Europa en estos últimos días, que incluyen también actores estatales. Sí, la Guerra Fría del siglo XXI es la ciberguerra, no hay descanso en el ciberespacio y por eso tenemos que entrar y entrar muy bien.

3.1. Los principios

Quiero aludir al trabajo hecho por Marcela Pallero, académica argentina quien tomó nuestra ley y la ordenó. Los principios son:

1) Control de daños. La ciberseguridad busca prevenir. Sin embargo, una vez que ocurre algo hay que actuar y, para pasar de la prevención a la actuación, se debe tener doctrina.

2) Cooperación con la autoridad.

3) Coordinación. Si entendemos que cada uno no puede valerse por sí mismo, necesitamos a un coordinador con todos los mecanismos a su disposición para generar las confianzas. Pero más que el principio de coordinación del Estado necesitamos aquí interoperabilidad a tiempo real. Por ejemplo, España trabaja con sondas que están reportando y que no esperan horas, días, sino que están casi en línea y por eso están en un lugar tan alto.

4) Seguridad en el ciberespacio.

5) Respuesta responsable. Ante un ataque no se contraataca, eso está fuera de las atribuciones. Ello no obsta a que se aprendan técnicas de ataque para verificar la idoneidad de los sistemas de los que se está encargado. Solo por decisión presidencial se puede contraatacar.

---

4 Es un tipo de código malicioso que impide a los usuarios acceder a su sistema o a sus archivos y exige el pago de un rescate para recuperar el acceso.

El artículo 51 de la Carta de las Naciones Unidas permite la legítima defensa de un Estado en caso de ataque o agresión, pero es el Estado el que responde, no la empresa ni el organismo del Estado que fue atacado. Esto no impide a Chile hacer uso de la defensa activa, vale decir, ciberataques ofensivos como respuesta a un ataque, pero solo es el presidente el que puede decidir. Estados Unidos lo tiene así definido, porque se considera *casus belli* el ataque a las organizaciones vitales –infraestructura de la cual se depende–. Entonces, el ciberespacio si bien no tiene fronteras sí tiene efectos y consecuencias. En consecuencia, el principio siempre hay que interpretarlo pensando en que queremos que todos estén esperando los ataques, pero no esperamos que se pongan a atacar, porque de hacerlo van a generar una distorsión gigantesca.

6) Seguridad informática.

7) La racionalidad. No solo es la racionalidad de la acción es la racionalidad de la autoridad y por eso tenemos que elegir muy bien a la persona que va a construir esto que nace. Sí, aquí son muy pocos los que saben, hay poca experiencia y nosotros somos parte de este proceso de aprendizaje para contribuir con el resto de los organismos.

8) Seguridad y privacidad configuradas por diseño. No hay que poner el *ticket* para estar seguro, ya viene seguro si somos capaces de diseñar sistemas que sean seguros y estén basados en la protección de datos; la privacidad predeterminada por diseño implicará tener menos problemas. Este es un tema de gestión de proceso de control de calidad. Entonces este es un gran desafío para tener en mente.

3.2. Directiva sobre seguridad de las redes y los sistemas informáticos –NIS–

Durante la discusión del proyecto de ley, salió la versión actualizada de la norma europea de seguridad de la información –la norma NIS, que ahora se conoce como NIS 2– y nosotros estábamos recién partiendo. ¿Qué hicimos? usar la NIS 2.

La NIS 2 considera todos los sectores y áreas, entre ellos, los sistemas que hay que revisar para saber si efectivamente nos van a afectar. Incluye a toda la Administración pública, dado que es fundamental que el Estado siga funcionando, aunque llueva, truene, tengamos terremotos o tsunamis; los ciberataques son solo un riesgo más. Hay que gestionar los riesgos, ya que nuestra vida es gestión de riesgo.

El 18 de octubre de 2024 es el plazo de los 27 Estados europeos para tener bajada la NIS 2 en sus leyes. Chile ya les ganó a varios de los países de la unión. ¿Por qué?, porque la nuestra es del 8 de abril. Esto a los europeos los tiene

desconcertados, se preguntan cómo este país fue capaz de ponerse a la misma altura y lograr un acuerdo político.

Estamos en este momento en el Congreso, en la Cámara de Diputados, aprobando el acuerdo marco avanzado con la Unión Europea. Ella es la tercera economía del mundo después de Estados Unidos y China, pero son 27 Estados que hacen política pública de calidad y eso es lo que nos interesa.

Tenemos una comisión mixta parlamentaria chilena —5 senadores y 10 diputados— con 15 eurodiputados y sesionamos dos veces al año —una en Santiago, una en Bruselas—. Y digo sesionamos, porque soy miembro de esa comisión permanente mixta para ir revisando la política pública.

Aquí viene la primera experiencia que yo siempre entrego: no nos peleemos entre nosotros, usemos un tercero confiable; si ese tercero confiable nos da garantía a los dos, bueno, incorporemos eso dentro de nuestra legislación. Porque cuando uno se pone muy creativo distorsiona algunas veces las cosas, uno pone más de un lado, el otro pone más del otro lado, entonces aquí tenemos una buena fórmula para resolver nuestras legítimas diferencias. Pero seamos prácticos: «más data, menos guata y usemos información que funciona».

No debemos olvidar que la NIS 2, en su artículo 16, crea esta organización de coordinación y cada 18 meses va a revisar su legislación. Entonces tenemos que imponernos nosotros estar mirando qué están haciendo ellos, ¿para qué?, para no quedarnos desconectados. Tuvimos una muy buena ley de protección de datos personales cuando no existía nada. Hoy hay que actualizarla. Entonces este es el desafío de usar política pública de otros países.

3.3. Ciberespacio: tecnologías de la información-tecnologías operativas

El ciberespacio es difícil de explicar, porque se trata de un ecosistema —como la tierra, el mar, el espacio—. A diferencia de la tierra, que tiene miles de millones de años, el ciberespacio es un ecosistema que creó la humanidad hace 30 años atrás.

Sabemos que en él confluyen lo físico y lo digital de forma inseparable. Antes, cuando no podíamos confiar entre personas, recurríamos a un tercero confiable: el notario, el banco, la autoridad. Actualmente es la ciberseguridad la que construye confianza digital y ella se basa en algo esencial: la identidad digital, es decir, que sepamos que es realmente una persona y no una inteligencia artificial. Hoy en día ni siquiera podemos tener certeza de si es humano o no el que ingresó, porque la inteligencia artificial se comporta de modo indistinguible de un humano. Aquí tenemos un problema, porque nuestra democracia depende de derechos como el derecho a la libertad de expresión, derecho humano que es de humanos, no de máquinas, no de inteligencias artificiales, entonces es relevante cómo filtramos los humanos de las máquinas.

En el ciberespacio, habrá organizaciones o empresas que no van a resultar afectadas por la ley. Otras, en cambio, sí, como los operadores de importancia vital. Sobre ellos recaerá la mayor responsabilidad y estarán sujetos a exigencias superiores, porque controlan sistemas de impacto significativo como seguridad, orden público, provisión continua de servicios. Por ejemplo, somos dependientes de la electricidad y, por lo mismo, esta tiene que funcionar a pesar de un ciberataque.

Somos frágiles no solo ante el ataque humano —sea cibernético o físico, como el corte de cables—, sino también frente a la acción de la naturaleza —por ejemplo, cuando los vientos derriban los postes—. Por esta razón, habrá que regular y fiscalizar con criterios de calificación, los que serán definidos por la agencia.

En cuanto a los deberes específicos, es importante la gestión de la seguridad de la información. Muchas empresas y organismos ya cuentan con ella, porque entienden los riesgos y como son responsables se han autorregulado. En su implementación, registrar es fundamental, pues tiene que otorgar certeza jurídica de los actos digitales. Ella se logra con la interoperabilidad —que da trazabilidad: sé quién y cuándo entró— y la integridad —los datos no pueden ser modificados—. Entonces esa es la verdadera confianza digital de la que hoy depende una transacción.

En estos momentos estamos en gestión documental —PDF, Excel, Word— y tenemos que pasar a gestiones transaccionales. Podríamos decir que es preciso sustituir el motor del vehículo, que todavía funciona manual y con combustibles fósiles, por uno automático con otro tipo de condiciones. Entonces resulta inoperante digitalizarnos y tener ciberseguridad si seguimos con el mismo motor. No podemos quedarnos en la gestión documental. Debemos pasar a gestiones transaccionales que nos darán mayores oportunidades de hacer una buena gobernanza de datos y con eso entregar un buen servicio a los individuos, resolver más rápido las situaciones, tomar mejores decisiones. Hacia allá vamos y, por eso, la ciberseguridad es tan importante.

La agencia podrá homologar certificaciones técnicas internacionales o extranjeras sobre ciberseguridad, mediante resolución fundada de su director (ley Nº 21.663, artículo 28). Esto beneficia a quienes han hecho un buen trabajo, para que no partan de cero.

Asimismo, es esencial informar a los afectados. Por ejemplo, dar a conocer las dependencias e interdependencias involucradas cuando se cortaron las cadenas logísticas de apoyo, como sucedió con GTD, que afectó a 78 municipios que dejaron de funcionar.

Obviamente es fundamental tener programas de capacitación y educación continua, pero también es conveniente desplegar campañas de ciberhigiene y de alerta temprana.

Finalmente, hay que dar visibilidad al delegado de ciberseguridad, para que un responsable lleve el tema y sea escuchado por su directorio, su gobierno corporativo, su ministro, el presidente. Si esto no ocurre, se va a transformar en lo que ha sido siempre: un problema técnico o de gestión de riesgo. Si se logra entender ese nivel, todo se desarrollará más fácilmente.

3.4. Plazos para reportar que tiene el Equipo de Respuesta ante Incidencias de Seguridad Informáticas –CSIRT[5]–

1) 3 horas. Los plazos se buscaron de forma racional. Por ejemplo, en un incendio forestal, cuando partió el fuego y se ven las primeras llamas, no sabemos qué se va a quemar, quién la generó, qué está pasando. Pero esta es la primera alerta que permite el control de daños, no importa si se trata de una falsa alarma, porque es mejor tener falsas alarmas que enfrentar después un siniestro que es imposible controlar. No se trata de que por un «escaneo puerta» van a dar la alarma de ataque; ese tipo de análisis simplemente significa que alguien pasó por fuera el muro de la casa y vio que probablemente la chapa estaba abierta, pero no hizo nada. Hay que definir bien qué es una situación crítica, cuáles ataques implican riesgo.

2) 72 horas. Son el plazo mínimo que uno esperaría para tener una respuesta técnica y aquí estamos hablando de indicadores de compromiso, el ADN de lo que nos está atacando, qué cosa está pasando. No es obligatorio esperar 72 horas para poder entregar información. En la medida que se va conociendo lo que está pasando, se va entendiendo. Toda esa información debe fluir y esos canales también tienen que ser seguros. Aquí se produce el primer problema: la interoperabilidad entre el Estado y los privados, porque hoy solo tenemos interoperabilidad dentro del Estado, aunque limitada. Hay que ver cómo instalamos una red de seguridad integral nacional.

3) 15 días. Son para presentar el informe.

   El plazo más importante son 3 horas, pues si con ese mínimo de tiempo somos capaces de advertir y después hacer el seguimiento para ir compartiendo información que sea necesaria, habremos sido capaces de controlar el riesgo.

3.5. Sistema nacional de ciberseguridad

1) Agencia Nacional de Protección de Datos. En el sistema, la agencia de protección de datos está pendiente. Curiosamente llevamos más años tramitando la ley de protección de datos de lo que nos demoramos en tramitar la de ciberseguridad.

---

5 *Computer security incident response team.*

Datos personales. Es esencial, solo falta una o dos sesiones, una comisión mixta —que también integro— entre el Senado y la Cámara de Diputados para resolver cuatro divergencias que quedan y después sale la ley y la agencia.

2) Agencia Nacional de Ciberseguridad. Aquí surge la primera pregunta: ¿a quién le informa? Al portal único. ¿Y las multas? Siempre se van a aplicar las más altas, para que no haya ninguna duda. Esto es un criterio que permite simplificar y saber que aquellos que cumplen y cumplen bien no van a tener problema.

3) Instituto Nacional de Ciberseguridad. Nos falta investigación avanzada, un instituto como el que tiene España, en León, que está 348 km al norte de Madrid, o como el que van a tener los rumanos en Bucarest. Sin generación de conocimiento propio, no tenemos ninguna posibilidad, porque todo cambia, esto es permanente. Necesitamos preparar personas y ojalá a edad temprana. En España se parte en la academia hacker a los 14 años, porque la ley de protección de datos dice que ya los datos no son del menor y se pueden usar. A los 16 años ya están atacando los delincuentes y si no les damos oportunidades van a irse por el lado oscuro, entonces tenemos que abrir áreas por el otro lado.

3.6. Relaciones

El Equipo de Respuesta ante Incidencias de Seguridad Informáticas va a depender de la Agencia Nacional de Ciberseguridad. Por primera vez, habrá una entidad que va a recoger toda la información del país. Hasta ahora teníamos un equipo de respuesta que veía algunas cosas de los que reportan al Gobierno voluntariamente. A partir de esta ley van a estar todos obligados.

Aquí el reporte es esencial, pues cuando se ve todo, se sabe lo que está ocurriendo y se va anticipando. Esa es la ventaja de tener esta gran coordinación nacional y en espejo con el CSIRT, donde se delimiten bien cada una de las áreas.

El Comité Interministerial de Ciberseguridad —CIC—. Diez ministros tuvieron que firmar la Ley Marco de Ciberseguridad; diez, porque se trata de un tema complejo, no de un ministerio sectorial, es transversal a todos e incluso podría haber firmado el gabinete completo.

Tenemos un Consejo Multisectorial de Ciberseguridad para poder relacionarse con todos: el Estado a través del comité interministerial y el consejo para todo lo que es industria y sociedad civil. El comité está presidido por la Agencia Nacional de Ciberseguridad y lo integran el subsecretario de Interior o de Seguridad —si sacamos el ministerio no lo sabemos todavía—, el subsecretario de Defensa, el subsecretario de Relaciones Exteriores, el Ministerio Secretaría General de la Presidencia, la Superintendencia de Telecomunicaciones, el Ministerio de Hacienda —Heidi Berner, subsecretaria de Hacienda, estuvo en Estonia dos

semanas atrás, viendo precisamente todas las capacidades que tiene ese país báltico para usar identidad digital de verdad y en transacciones seguras–, el Ministerio de Ciencia Tecnología Conocimiento e Innovación y el director de la Agencia Nacional de Inteligencia.

Hacia afuera, la Agencia Nacional de Ciberseguridad va a tener un consejo multisectorial compuesto por seis miembros, que durarán seis años, pero serán renovados cada tres. En consecuencia, tres durarán seis años; y el resto, tres años. Habrá dos representantes de la industria, por ejemplo, del sector eléctrico, el comercio, la banca, turnándose para que vayan apareciendo todos, pero tienen que estar presentes, porque su voz es importante.

La Alianza Chilena de Ciberseguridad nació el 30 de mayo de 2018. Una semana antes del ciberataque al Banco Chile, se había previsto su formación, pero el incidente sirvió para darle más notoriedad. Los convocados lo han hecho muy bien colaborando con el Senado y con los foros nacionales de ciberseguridad.

Ahora hay que institucionalizar y después vamos a tener que sacar proyectos y presupuestos. Por ejemplo, en Europa, se hace un campeonato de ciberseguridad entre jóvenes de 18 a 24 años. En cuanto al financiamiento, todavía no se ha determinado.

3.7. Las atribuciones de la Agencia Nacional de Ciberseguridad

Se definió muy bien qué puede hacer con sus facultades. Sin embargo, si no actúa con la debida reserva, se pierde toda la capacidad que tiene un país de actuar contra amenazas que son gigantescas, pues las bandas criminales no son amateurs. Esto ha llevado a que sean secretos los planes de continuidad, los planes de acción y mitigación y las matrices de riesgo. Y esto es particularmente relevante, porque habrá que determinar cómo se comprarán aquellos productos cuya existencia debe permanecer en reserva. Si la gente que trabaje en esto es desprolija, dichas vulnerabilidades van a ser explotadas por los ciberdelincuentes.

En cuanto los temas más importantes:

1) La Agencia Nacional de Ciberseguridad va a tener un sistema híbrido, para tener lo mejor del Estatuto Administrativo y del Código del Trabajo. Esto debería ayudar a generar una organización pequeña, flexible y capaz, donde estén las mejores personas.

2) Hay sanciones leves, graves y gravísimas. Tratándose de los prestadores de servicios esenciales, las leves parten en 5.000 UTM y se duplican en caso de los operadores de importancia vital. Por su parte las sanciones graves van de 10.000 UTM a 20.000 UTM, mientras que las gravísimas se sitúan entre 20.000 UTM y 40.000 UTM. Se impusieron estos montos elevados para incentivar el cumplimento, no hay interés en sancionar a las empresas, es

más, la Agencia Nacional de Ciberseguridad no se financia con ingresos no operacionales producto de las multas. Se pretende con este mecanismo fijar los límites y fomentar los esfuerzos.

Hubo un gran acuerdo político: el «*hacking* ético», que es una modificación responsable. Aquí estamos actuando sobre el corazón del conocimiento. Los *hackers* son individuos con grandes habilidades en el manejo de computadoras que investigan un sistema informático para avisar de los fallos y desarrollar técnicas de mejora (Real Academia Española, s.f., definición 2). El *hacker* tiene talento, conocimiento, habilidades y dedica su tiempo a encontrar fallas en los sistemas. Por esta razón, no lo penalizaremos y para eso fijamos lineamientos sobre lo que tienen permitido hacer, de manera que aquellos que se ciñan a estas reglas no van a ser objeto de sanción penal (ley Nº 21.663, artículo 55). Esto es significativo, porque sacamos nuestra ley de delito informático, que sigue el Convenio de Budapest[6] y los europeos nos podrían haber cuestionado. Bélgica sacó antes que nosotros una ley más exigente, pero fuimos capaces de tomar lo último que había en política pública y esto implicó muchos problemas, aunque solo para aquellos sistemas del Estado, porque los privados tienen que dar su consentimiento —el *pentest*[7] gratuito hecho de forma desprolija puede generar problemas muy grandes—.

No pudimos dictar normas sobre *ransomware*, porque no tuvimos el piso político. Algunos recordarán que en los años 70 y 80 se secuestraban aviones y que la reacción de los Gobiernos y las empresas fue aumentar la seguridad. Actualmente, no se secuestra ningún avión, porque no se toleró pagar rescate en el pasado. Eso para un operador de importancia vital debiese ser su norma. Muchos lo han hecho, como GTD que rechazó pagar, con todos los costos que significó. Ese es el ejemplo que queremos. No debemos alimentar el crimen organizado sabiendo que vamos a financiar más ataques debido a nuestras desprolijidades, por eso hay que estar preparados para ser resilientes. Resiliente significa que nos prepararemos para estos eventos, para resistir, si nos caemos, nos paramos y después evolucionamos, eso es lo que queremos que ocurra en Chile.

3.8. Marco jurídico de la ciberseguridad

Tenemos un mes de la ciberseguridad, en octubre. Esa fue la primera ley. A nivel nacional, vamos a hacer ejercicios durante ese período y tendremos una agencia.

Nuestra ley de delito informático es la Nº 21.459, que sigue el Convenio de Budapest. Aún no hemos resuelto las cuatro divergencias la ley de protección de datos personales, pero ya contamos con ley Nº 21.663, que fue capaz de darnos este marco de ciberseguridad.

---

6 Convenio sobre la Ciberdelincuencia. https://www.bcn.cl/leychile/navegar?idNorma=1106936

7 Ataque a un sistema informático para encontrar las debilidades de seguridad.

Todavía nos falta interoperabilidad, gobernanza y gobernanza de datos, aunque se ha constituido una mesa de diálogo con el Ejecutivo. Esta fue una de las condiciones que se puso para lograr la aprobación del proyecto marco de ciberseguridad, porque no podemos avanzar si no tenemos certeza jurídica de los actos digitales. Entonces ese es el elemento que nos falta para completar.

El 8 de octubre esperamos que esté toda la documentación y el 8 de abril de próximo año cortaremos la cinta de nuestra Agencia Nacional de Ciberseguridad.

Solo lo que se controla funciona y esa es una norma que es básica. Estamos agregando nuevos mecanismos de control. La ciberseguridad nos va a permitir tener control para mejorar muchas cosas, partiendo por la transparencia, pero lo que es más importante: la gestión, resultados reales, medibles, porque esos son, nadie los ha alterado ni los ha cambiado.

4. Preguntas del moderador

Moderador: en relación con la nueva ley, ¿cuál sería el diagnóstico del Estado y la situación del sector público, en cuanto a materias de ciberseguridad y cómo esta nueva ley ayudaría a mitigar brechas ya existentes?

Claudia Santa Ana[8]: personalmente me tocó conversar sobre si se digitaliza o no, si llevamos servicios a la nube o no, si era Microsoft un proveedor confiable y todas esas conversaciones se rompieron con la pandemia, cuando nos vimos en la necesidad de digitalizar servicios, el Estado tuvo que hacerlo de forma rápida. Eso generó vulnerabilidades que hoy están siendo aprovechadas por las organizaciones criminales que ven un público objetivo en nuestro país, pues son conscientes de nuestras vulnerabilidades. ¿Cuán preparados estamos frente a un ataque, cuánto tiempo, cuál es el impacto que puede haber tenido un GTD, un IFX, cuáles son las relaciones que tenemos con nuestros proveedores? Son temas que debemos dilucidar.

Creo que tenemos varios espacios de mejora y esta ley marco nos obliga a poner esto como prioritario en nuestras agendas. La ciberseguridad no empieza y no se resuelve solo desde las áreas tecnológicas, de modo que esta ley marco es fundamental para el país y para llevar esta conversación a los directorios y a niveles más transversales. No creo que un cambio cultural dentro de las organizaciones del Estado hubiera sido posible sin esta ley marco que tenemos hoy.

Senador Kenneth Pugh: los encargados de ciberseguridad son quienes menos pueden dormir, porque no saben si la inteligencia artificial generativa les va a hacer un *phishing* que los va a complicar con alguien de su organización. Si bien estaban designados por decretos —todos deben tener alguno—, ahora

8 Es directora de la Alianza Chilena Ciberseguridad.

ya quedan dentro del sistema para algo que es fundamental: la formulación presupuestaria, que exista realmente el presupuesto que se requiere, no solo de inversión, sino también de capacitación, de ejercicio, pues hay que invertir en las personas. Ese el primer problema. El segundo, el personal: sabemos que un 20 %, 25 %, 30 % de los trabajadores se puede ir al año, porque si bien el Estado va a ser el empleador principal, las empresas, tanto de nivel alto como las pymes, necesitarán muchos especialistas y existe en este momento una brecha de casi 30.000 individuos que faltan en el sistema. Entonces ese es un problema delicado y para eso requerimos formación de conocimiento temprano. Es preciso partir en la educación media técnico-profesional, pues ahora ya no se necesitan títulos universitarios, basta con competencias acreditadas. El problema es que el Estado no los puede contratar, la agencia sí, pero esas cosas son las que tenemos que ver. Yo entiendo la realidad de cada uno y por eso vamos a tratar de generar el Club CISO —*Chief Information Security Office*— del Estado, porque tienen los mismos problemas comunes, o sea, juntarlos a todos y tener los CISO de la empresa, pero los del Estado tenemos que preocuparnos de ellos, porque están en la batalla diaria.

Carlos Bustos[9]: lo que yo miro son tres índices. Hay un índice global de desarrollo digital, en el cual Chile está en el puesto número 32 —el último estudio creo que fue en 2023—. Después hay un índice de Gobierno digital, en el cual Chile está en lugar 36, puntero en Latinoamérica. Y después hay un índice de desarrollo general de ciberseguridad y en ese estamos entre el lugar 74 y el 83 —ese es de 2021—. La última lectura es que somos un país atractivo digitalmente, tenemos una transformación digital interesante, tenemos activos digitales importantes, pero no están suficientemente protegidos.

Ahora, en cuanto a la madurez de la ciberseguridad en el Estado, adhiero a lo que afirma el senador: esta ley nos va a ayudar a aumentar la madurez. Tuvimos el decreto presidencial Nº 8 en octubre de 2018 y, en mi opinión, lo más interesante de ese decreto es que nombraba un encargado de ciberseguridad. En 2008, la nominación se hizo por correo electrónico y ahí tuvimos que empezar a aprender. Al final, este déficit de 30.000 profesionales es una realidad. No había profesionales, pero llevamos 6 años madurando el tema. Definitivamente hay mucho por hacer y claramente esta nueva ley nos va a permitir elevar el piso del nivel de madurez que tenemos. No hay más, somos nosotros los que tenemos que hacer este cambio y seguir madurando para poder llegar a niveles de protección que estén acordes al nivel de transformación digital que tenemos y al nivel de Gobierno digital que tenemos.

Moderador: senador, el año pasado en octubre se creó el Foro Nacional de Ciberseguridad en el Senado en conjunto con la Alianza Chilena de Ciberseguridad. ¿Nos podría explicar los objetivos y alcances de ese foro?

9 Carlos Bustos, director de la Alianza Chilena de Ciberseguridad.

Senador Kenneth Pugh: este foro nace de una iniciativa española en León, a raíz de la conclusión de que era necesario generar una instancia donde todos se pudieran reunir, porque en ciberseguridad no se compite, se colabora y había que generar un lugar donde todos pudiesen juntarse y llegasen todos: las diferentes profesiones, actores públicos y privados, académicos. Nosotros decidimos hacerlo en el Congreso Nacional, en Santiago, con una propuesta que es básicamente usar una métrica —la medición de madurez— y que es la que usa la Organización de Estados Americanos para medir el avance. Fue desarrollada por la Universidad de Oxford, que alberga el centro global de ciberseguridad. No les explico la cantidad de doctorados que tenemos en literatura inglesa de Oxford, pero no tenemos a nadie en ciberseguridad. Entonces tenemos que empezar a formar talento y usar la métrica.

Por cierto, buscamos instalar una política pública de largo plazo, que no sea de un Gobierno turno, que se pueda mantener en el tiempo.

Moderador: Claudia y Carlos, como representantes de la Alianza Chilena de Ciberseguridad, ¿cuál es su rol y la contribución de la alianza en este Foro Nacional de Ciberseguridad?

Carlos Bustos: quiero destacar la colaboración entre la academia, el sector privado y el Estado. Es importante el aporte de todos para resolver este problema y tener mejores regulaciones. Además es relevante poder medir el avance, adoptar este índice de madurez de la Universidad de Oxford.

Claudia Santa Ana: esos espacios de colaboración son fundamentales para entender cómo lo están haciendo afuera, cómo deciden otros. Frente a problemas cotidianos que hay que resolver —por ejemplo, ¿corresponde usar un segundo factor de autenticación en un celular no corporativo?— nos sirve mucho esa colaboración, tanto en aspectos tácticos como estratégicos. Por esto, creo que la alianza y el foro logran unir de forma exitosa ese mundo público y privado.

Senador Kenneth Pugh: agrego un punto que es nuevo. Se va a crear el Consejo Multisectorial y este va a ser el foro, el instrumento que va a tener el consejo. La gobernanza va a mejorar y así tendrá mayor proyección; por ello, es necesario institucionalizar, de manera que estamos buscando la fórmula para dejarlo bien instalado y que sirva a la política pública. Procuraremos que esta última sea actualizable para que se vaya adaptando. Estamos trabajando ahora con inteligencia artificial y esto es parte de lo mismo, no es que sea esto con un apellido, es transversal, es para todo.

Moderador: en 2022 se produjeron varios ataques de ransomware al sector público y a proveedores de telecomunicaciones. ¿Qué recomendaciones darían a los encargados de ciberseguridad del sector público, en cuanto a lo preventivo y lo correctivo, con respecto al *ransomware,* dada toda esta experiencia que ha vivido en Chile y qué medidas de mitigación pueden tomar?

Senador Kenneth Pugh: cuando se creó internet 30 años atrás, nunca se pensó en los ataques, no se diseñó seguridad, pues todos confiaban. Ahora es preciso partir de la premisa de que vamos a recibir ataques. No se trata de que la seguridad llegue a niveles paranoicos, pero debemos ser extremadamente cautos, pues así va a ser mucho más fácil actuar. Actualmente los ciberdelincuentes no fabrican el *ransomware*, sino que lo arriendan —*ransomware as a service*—, lo que representa un peligro, porque si se tiene un computador, ellos tendrán acceso a él y nos podrán atacar.

Bajando a lo más particular, los usuarios son los primeros y los últimos que pueden detener algo —alguien encontró lo que había que hacer y logró librarse—. Si no somos capaces de prever un ataque por *ransomware* y reaccionar adecuadamente no sirve. Probablemente habrá que tener sistemas redundantes, todo encriptado, todo listo y todos los equipos para cambiarnos de un lado a otro, en otras palabras, el sistema tendrá que disponer de algo como el *uptime* de los data center 99,9 % o podría estar detenido por dos o tres horas. Los críticos pensarán que el *ransomware* va a desaparecer, pero esto equivale a imaginar que «no habrá más influenza ni más COVID». Todos sabemos que es parte de nuestro ecosistema, tenemos que saber convivir con él.

Claudia Santa Ana: yo creo que ha sido el principal modelo de negocio de los cibercriminales durante los últimos años, siendo, por las rentas obtenidas, la tercera actividad económica mundial. La cuestión es clara, el *ransomware* actúa sobre los sistemas digitales críticos inutilizándolos y sin posibilidad de recuperación por parte del usuario. Luego, hay que pagar para que nos devuelvan el sistema.

Objetivamente es una negociación con un delincuente, con alguien que no nos da ninguna garantía. Por esta razón, el *ransomware* crece exponencialmente como servicio, particularmente en las pymes, cada año está por encima del 100 %, lo que es un punto relevante para los temas de ciberseguridad. Esto nos lleva a preguntarnos cómo movemos la ciberseguridad desde lo preventivo a lo reactivo. Si recibo un ataque de *ransomware* en una entidad de Gobierno ¿cuál es el impacto que va a tener en otras?, ¿generará impacto en cascada?, ¿cuáles son mis planes de respuesta?, ¿cuáles son mis proveedores? Hay que obrar con resiliencia digital, asumir que se producirá un ataque y que debemos estar preparados para responderlo. No podemos confiar solo en nuestros sistemas de prevención, necesitamos entender cómo vamos a responder, cuáles son nuestros planes de respuesta a los ataques que estamos viendo hoy en día.

Carlos Bustos: el *ransomware* va a seguir existiendo como industria y esto hay que tenerlo muy claro: son criminales. Dentro del Estado tenemos instituciones que están muy maduras desde el punto de vista de la ciberseguridad y otras que son incipientes, por lo que hay que aprovechar las economías de escala para tener una unidad centralizada que las esté ayudando, por ejemplo, con

capacitación. Asimismo, es fundamental contar con el inventario actualizado, porque así sabemos qué tenemos que proteger, cómo podemos gestionar la vulnerabilidad y preocuparnos del parchado. Después hay otros factores como tener controlados a nuestros usuarios privilegiados con doble factor de autenticación. Finalmente, es imprescindible disponer de un equipo centralizado de respuesta a incidentes.

Claudia Santa Ana: el *ransomware* como servicio funciona así: detectan la vulnerabilidad que van a explotar, mandan el mismo mensaje electrónico, el usuario hace clic en el mismo archivo con la misma información, se aprovecha la misma vulnerabilidad. Entonces, de alguna manera tenemos algo que hacer y sabemos lo que podemos hacer, vale decir, son medidas higiénicas básicas que están publicadas —confianza cero, sistemas actualizados, parchado, multifactor de autenticación—. Tenemos esperanza de que esto sea un modelo de servicio que aproveche las economías de escala. Nos hace entender cómo se van a comportar. Obviamente tenemos ataques que son distintos, pero sabemos cómo operan muchos de ellos y cómo entran, por eso es útil el reforzamiento de las medidas básicas de higiene.

Moderador: las nuevas tecnologías como la inteligencia artificial y la computación cuántica ¿cómo se han incorporado desde el lado del ataque y desde el de la prevención?

Carlos Bustos: los cibercriminales están usando inteligencia artificial. Desde el punto de vista de la defensa, también estamos incorporando herramientas de inteligencia artificial y automatización de temas para responder más rápido.

Respecto a la computación cuántica, todavía no es algo masivo y básicamente el temor ahí es que aparezcan algoritmos para desencriptar las llaves que existen actualmente. Con suficiente poder de cómputo, las llaves actuales se podrán desencriptar, o sea, es un peligro. Sin embargo, ya se están desarrollando tecnologías. Por ejemplo, en Chile hay una *startup* que está trabajando con una multinacional de la tecnología para elaborar una encriptación capaz de resistir esta computación cuántica. Básicamente, en la encriptación es más fácil generar el encriptado que desencriptarlo, motivo por el cual persistirá el problema de que las llaves actuales puedan a futuro resultar infectadas.

Senador Kenneth Pugh: la tecnología evoluciona de forma impresionante. Un par de años atrás nadie estaba hablando sobre inteligencia artificial. En este minuto no solo estamos hablando, la estamos usando todo el día y algunos sin siquiera saberlo.

Regular es el problema. Cómo regulamos. Europa ya lo definió y tiene una fórmula, pero hay que entender que la inteligencia artificial sirve muy bien. Como toda tecnología, no es ni buena ni mala, es neutra. No es ni de la izquierda ni del

centro ni de la derecha, es de todos. ¿Cómo la vamos a usar? Lo primero es darle un uso responsable y ético, el problema es que después de la ética vienen los delitos. El mismo día que el Parlamento Europeo inició la votación, presentamos el proyecto de ley para crear la agravante penal: «aquel que comete un delito valiéndose de la inteligencia artificial». Y esto porque, si nos vamos al mundo real, todos los días alguien utilizará un utensilio como el cuchillo para cocinar, otro se servirá de él para tallar y, un tercero, para matar. Bueno, la persona que mata a alguien con el cuchillo, el delito va a ser con la agravante que corresponde por el cuchillo. Yo no regulo cuchillos, yo regulo los actos y los efectos que generan el uso indebido de estas herramientas.

La inteligencia artificial tiene un amplio margen para crecer, no sabemos dónde va a llegar. Ya las inteligencias artificiales generativas provocan el problema gigantesco de la incapacidad de definir qué es real y qué no: hoy me puede llamar mi hija para decirme que la están secuestrando. ¿Qué tienen que ustedes hacer? tener una prueba de vida, es decir valerse de una palabra, un gesto, algo que tú sepas que ella es ella. Entonces, el marco regulatorio es muy importante en todas las tecnologías. Se estima que en menos de 10 años la computación cuántica ya estará destruyendo toda nuestra criptografía, tanto a las claves públicas como las privadas.

¿Dónde está el problema? Que todo lo que se ha guardado –y hay gente que se ha dedicado a guardar cosas encriptadas– podrá ser desencriptado. O sea, vamos a saber si llegamos a la luna, quién mató al presidente Kennedy, una gran cantidad de cosas van a aparecer.

¿Qué hacemos entonces? Ahí está el conocimiento. Yo quiero destacar al Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, porque ha generado ecosistemas. Por ejemplo, la pyme penquista Sequor Quantum desarrolló sistemas de criptografía cuántica en colaboración con una universidad polaca. La criptografía hoy se basa en claves pseudoaleatorias –aquellas cuya generación no es aleatoria en un 100 %– y por eso se pueden quebrar y esta es la razón de la utilidad de la computación cuántica. La pyme en cuestión genera claves totalmente aleatorias con certificado. El riesgo que viene implica que debemos cambiar nuestro sistema a criptografía cuántica para poder resistir el embate. Entonces, está el conocimiento, el talento y está nuestra soberanía digital, nuestra independencia digital y el no depender de terceros. Veamos en 5 años más en qué estaremos. Respecto al conocimiento hay cosas que conocemos y entendemos; otras que entendemos, pero de las que no somos conscientes; cosas de las que somos conscientes, pero que no entendemos; y cosas de las que no somos conscientes ni entendemos. Esta última categoría es enorme, vale decir, nos queda mucho todavía por delante y para eso hay que invertir en las personas, en conocimiento, generar ecosistemas. Retener ese talento en el país será el principal problema, más que las tecnologías, porque estas las podemos ir adoptando en el tiempo.

Claudia Santa Ana: ¿en qué se usa más inteligencia artificial en el último tiempo?: en poder engañar a los usuarios para que hagan clic. Con la inteligencia artificial generativa ha evolucionado enormemente el *phishing.* Antes uno se daba cuenta fácilmente del engaño, porque el mensaje electrónico estaba mal escrito, pero ahora están utilizando inteligencia artificial tras ingresar a los sistemas para buscar vulnerabilidades. Asimismo, mucha inteligencia artificial está enfocada a difundir noticias falsas para generar estados de crisis.

Sin lugar a dudas, los ciberdelincuentes están utilizando inteligencia artificial en distintos procesos y eso nos lleva a dos sumas. En el fondo tengo a los ciberatacantes que están utilizando inteligencia artificial contra algún usuario que hizo clic, lo que ha generado que los tiempos en los que se mueven dentro de las empresas sean mucho mayores. Antes el atacante podía permanecer infiltrado tres meses para atacar, pero hoy 140 minutos después de su ingreso puede desplegar un ataque de *ransomware* muy rápidamente. Entonces, ante la escasez de personal idóneo y con estos niveles de tiempos, estoy en la necesidad de utilizar inteligencia artificial, computación cuántica o la tecnología que tenga disponible para poder protegerme y responder.

Frente a un atacante de una entidad con 1.000 trabajadores —en que basta que uno haga clic— solo tendremos 140 minutos para detectar el problema. Entonces, corresponde a la inteligencia artificial iluminar las áreas de ciberseguridad, identificar dónde está el problema y qué es lo que debo realizar.

Como responsables de ciberseguridad debemos comprender cuál es nuestro rol en las distintas entidades y saber cómo vamos a gobernar la inteligencia artificial. ¿Tenemos en ciberseguridad la capacidad de proteger los sistemas que utilizan inteligencia artificial? ¿Entendemos cuál es la diferencia entre proteger los sistemas tradicionales y aquellos que utilizan inteligencia artificial? ¿Cómo trabajo con estos? ¿Cómo vulnera el atacante la inteligencia artificial?

Referencias

- Ley Nº 21.663, *Ley Marco de Ciberseguridad.* Diario Oficial de la República de Chile, 8 de abril de 2023. https://bcn.cl/3isi2
- Naciones Unidas. (1945). *Carta de las Naciones Unidas.* Tratado constitutivo. https://www.un.org/es/about-us/un-charter
- Real Academia Española. (s.f.). Jáquer. En *Diccionario de la lengua española.* https://dle.rae.es/j%C3%A1quer?m=form
- Unión Europea. (2022). *The final text of the NIS 2 Directive* (14 December 2022). https://www.nis-2-directive.com/NIS_2_Directive_Articles.html