SEMINARIO **LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS**
frente a un mundo tecnológicamente dependiente e interconectado

La necesidad de un marco normativo para Ciberseguridad Industrial

Abog. Marcelo Temperini*

*Abogado (UNL), especializado en Derecho Informático y Técnico Analista de Seguridad (ESR - Cisco). Es Doctorando de CONICET dedicado a la investigación de Delitos Informáticos y Cibercrimen. Es Socio Fundador de AsegurarTe: Consultora en Seguridad de la Información. Es Co-Director del Observatorio de Delitos Informáticos de Latinoamerica (ODILA). Es Miembro de la Comisión Directiva de la Asociación de Derecho Informático de Argentina (ADIAr). Es Prosecretario en la Comisión de Derecho Informático y Nuevas Tecnologías del Colegio Público de Abogados de Santa Fe, 1ra. Circunscripción Judicial.

SEMINARIO **LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS**
frente a un mundo tecnológicamente dependiente e interconectado

El derecho como herramienta

¿Donde estamos?

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Normativa: Resolución JGM Nº 580/2011

- Art. 3º — El "PROGRAMA NACIONAL DE INFRAESTRUCTURAS CRITICAS DE INFORMACION Y CIBERSEGURIDAD" tendrá a su cargo los siguientes objetivos:
  - a) Elaborar y proponer normas destinadas a incrementar los esfuerzos orientados a elevar los umbrales de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas en el ámbito del Sector Publico Nacional.
  - b) Colaborar con el sector privado para elaborar en conjunto políticas de resguardo de la seguridad digital con actualización constante, fortaleciendo lazos entre los sectores público y privado; haciendo especial hincapié en las infraestructuras críticas.
  - n) Elaborar un informe anual de la situación en materia de ciberseguridad, a efectos de su publicación abierta y transparente.

Normativa: Disposición ONTI Nº 3/2011

- Aprueba el "Formulario de adhesión al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad", mediante el cual las entidades y jurisdicciones definidas en el artículo 8º de la Ley Nº 24.156 y sus modificatorias, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado podrán adherir al ICIC
- Aprueba "Convenio de Confidencialidad" para los adherentes

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Normativa: Disposición ONTI 2/2013

- ARTICULO 1° — Créase el grupo de trabajo "ICIC - CERT" (Computer Emergency Response Team) en el marco del "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad", y bajo la órbita de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION.
- Crea además:
  - Grupo de trabajo "ICIC - GAP" (Grupo de Acción Preventiva);
  - Grupo de trabajo "ICIC - GICI" (Grupo de Infraestructuras Críticas de Información)
  - Grupo de trabajo "ICIC - INTERNET SANO"

Normativa: Disposición ONTI 03/2013

- Artículo 1° — Apruébase la "Política de Seguridad de la Información Modelo", que reemplaza a los mismos fines a la aprobada por Disposición ONTI Nº 6/2005, que como Anexo I forma parte integrante de la presente.
- Art. 2° — Las disposiciones de la Política de Seguridad de la Información Modelo servirán como base para la elaboración de las respectivas políticas a dictarse por cada organismo alcanzado por la Decisión Administrativa Nº 669/2004, debiendo ser interpretada como un compendio de mejores prácticas en materia de seguridad de la información para las entidades, públicas y adaptada a la realidad y recursos de cada organismo.

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Normativa: Decisión Administrativa JGM N° 15/2015

- Artículo 1° — Modifícase la estructura organizativa del MINISTERIO DE DEFENSA, en lo concerniente a la UNIDAD MINISTRO, aprobada por Decisión Administrativa N° 21 del 15 de abril de 2002 y sus modificatorios, incorporando la DIRECCIÓN GENERAL DE CIBERDEFENSA cuya responsabilidad primaria y acciones se detallan en la planilla Anexa al presente artículo.
- Entre sus responsabilidades, se encuentra la de (6)- Intervenir en el diseño de políticas, normas y procedimientos destinados a garantizar la seguridad de la información y a coordinar e integrar los centros de respuesta ante emergencias teleinformáticas.

Normativa: Decreto N° 1067/2015

- Crea la Subsecretaria de Protección de Infraestructuras Criticas de Información y Ciberseguridad y la Dirección Nacional de Infraestructuras Criticas de Información y Ciberseguridad ambas dependientes de la Secretaria de Gabinete de la Jefatura de Gabinete de Ministros.
- Entre sus objetivos principales tiene asistir a la SECRETARIA DE GABINETE en la formulación de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras críticas del SECTOR PUBLICO NACIONAL, y a las organizaciones civiles, del sector privado y del ámbito académico que así lo requieran, fomentando la cooperación y colaboración de los mencionados sectores.

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Normativa: Resolución JGM N° 1046/2015

- Aprueba la estructura organizativa de la Dirección Nacional de Infraestructuras Criticas de Información y Ciberseguridad, dependiente de la Subsecretaria de Protección de Infraestructuras Criticas de Información y Ciberseguridad de la Secretaria de Gabinete de la Jefatura de Gabinete de Ministros.
- Crea tres Direcciones:
  - DIRECCIÓN DE ELABORACIÓN E INTERPRETACIÓN NORMATIVA
  - DIRECCIÓN TÉCNICA DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD
  - DIRECCIÓN DE CAPACITACIÓN, CONCIENTIZACIÓN Y DIFUSIÓN

Otra normativa relacionada

- Disposición Administrativa: 669/2004
- Ley Nro 26.388
  - Agravante del 153 bis: La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.
  - Agravantes del 184: 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Otra normativa relacionada

- Disposición Administrativa: 669/2004
- Ley Nro 26.388
  - Agravante del 153 bis: La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.
  - Agravantes del 184: 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

Normativa española

- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (Objeto, Finalidad, Alcance, Catálogo, Organismos y Responsabilidades)
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas
- Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

¿Cómo podemos regular?

Consideraciones sobre una futura regulación

- Definir Objetivos, Funciones y Responsabilidades
- Regular un sistema de Auditorías y Controles
  - Realización de auditorías anuales (internas o externas)
  - Inventario y requisitos de software utilizado en infraestructuras críticas
    - Certificaciones en desarrollo seguro (security by design)
    - Adopción de estándares internacionales en materia de seguridad de la información
    - Adecuados sistemas de logs y registros, que permitan la investigación ante el caso de incidentes

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

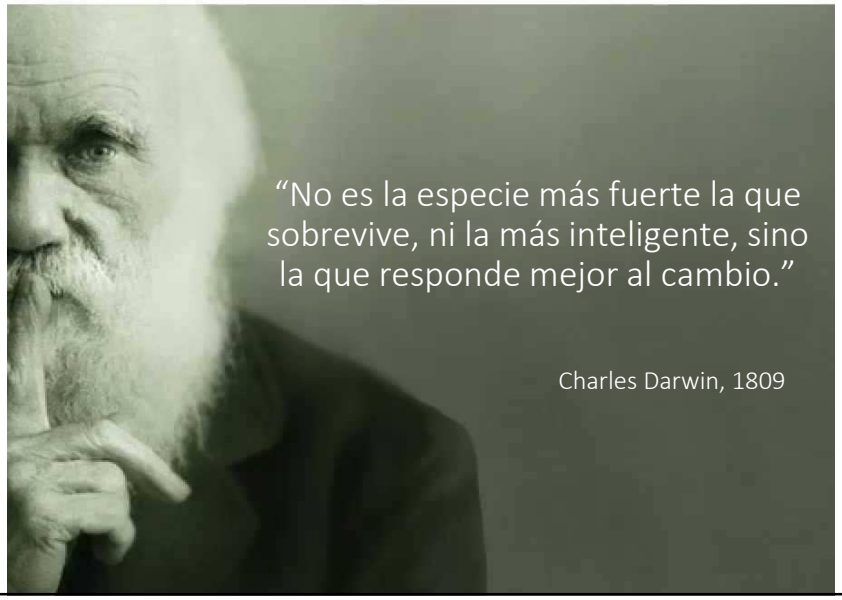
Conclusiones

La necesidad de avanzar en una normativa

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Una buena regulación legal es necesaria… pero no es suficiente

SEMINARIO **LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS**
frente a un mundo tecnológicamente dependiente e interconectado



SEMINARIO **LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS**
frente a un mundo tecnológicamente dependiente e interconectado

La necesidad de un marco normativo para Ciberseguridad Industrial

Muchas Gracias

Abog. Marcelo Temperini

mtemperini@asegurarte.com.ar

@mgitemperni

AseguraTe Protegiendo su Información

ODILA Observatorio de Delitos Informáticos de Latinoamérica

CONICET

FCJS UNL
UNIVERSIDAD NACIONAL DEL LITORAL
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES