

Mesa de trabajo "Industria de Tecnología"

Autor

Agesic

Fecha de creación

11/10/2024

Tipo de publicación

Informes

Resumen

Informe del intercambio realizado en la mesa de trabajo **Industria de Tecnología**" desarrollada en el marco del proceso de cocreación de la Estrategia Nacional de Ciberseguridad realizada el 8 de julio 2024.

Introducción

En el marco del proceso de cocreación de la Estrategia Nacional de Ciberseguridad (ENC) de Uruguay, en el mes de junio y julio 2024 se realizaron nueve mesas de diálogo para recoger aportes respecto a la propuesta borrador. Participaron diferentes actores de instituciones públicas, privados, de la sociedad civil y de la academia, para intercambiar ideas que permitan cocrear la ENC. En este espacio se dialogó acerca de la visión y alcance de la Estrategia, así como los principios, objetivos y acciones específicas a impulsar.

En la jornada del 8 de julio se realizó el análisis de la visión del sector de tecnología en materia de ciberseguridad. En este informe se detallan las propuestas y aportes compilados en esta mesa de diálogo.

Este documento presenta en forma sintética los intercambios en esta mesa.

Participantes

Abitab, Sebastian Hernandez.

Agesic, Adolfo Nidegger, Andrés Morillo, Clara Michelini, Maite Rodriguez, Mauricio Papaleo, Mariana Ferraro, Maria Noel Hernandez, Natalia Salazar y Nicolas Correa.

ATOS, Joaquin Perez.

Bamboo Payment, Israele Bellizzi.

Datasec Soft, Guillermo Rodriguex y.Hugo Köncke.

Deloitte, Carlos Carrara.

EQUIFAX, Andrés Duffour y Paulo Perez.

Genexus consulting, Alfonso Berriel, Andoni Goicoechea, Lorena Veiga y Sebastián Passaro.

Getnet Uruguay, Mario Beron y Ramiro Cejas.

Grant Thornton, Ignacio Lagomarsino.

HG, Damian Alvez e lilian Cazalas.

ISBEL, Nicolás Martinez.

ITC, Leonardo Vidal.

PLEXO, Tomás Rodriguez y Roberto Facello.

Prex, German Oddo.

QoxIT, Rodrigo de la Fuente.

Security advisor, Angel Bertolotti.

Sonda, Andrés Farro y Marcelo Mariatti.

Teledata, Alejandro Pereyra y Lía Merialdo.

TILO, Ana Lucero.

Tilsor, Gustavo Betarte y Rodrigo Martinez.

Total Net, Juan Moreno y Miguel Ferreyra.

Willinn, Diego Rosas e Inés Jakubovski.

Resumen del intercambio

A continuación se presenta el informe general de la mesa de trabajo “Industria de tecnología” donde se encuentran sistematizados y sintetizados los aportes del grupo.

Regulaciones

- Inversión obligatoria en ciberseguridad: en la estrategia, se debe considerar establecer regulaciones sólidas en sectores como salud, finanzas y telecomunicaciones. Los reguladores deben exigir cumplimiento y tener capacidad de sanción.
- Identificación de sectores críticos: regular aquellos sectores o productos que puedan interrumpir servicios clave. Por ejemplo, empresas cuyos fallos puedan afectar el pago de pensiones deben estar reguladas.
- Ranking de sectores críticos: establecer un ranking de empresas y sectores según la criticidad de sus servicios, con intervención estatal cuando sea necesario.
- Apoyo estatal a empresas críticas: fondos, capacitaciones y consultorías para empresas consideradas críticas, como salud, con un plan estratégico a 5 años.
- Roles de Agesic: fomentar la implementación de regulaciones y un modelo de transición que facilite la adaptación a tendencias tecnológicas.
- Protocolos de respuesta a ataques: mejorar la conciencia sobre protocolos existentes y promover su cumplimiento.

Incentivos

- Motivación empresarial: incentivos vinculados al negocio para invertir en ciberseguridad, destacando cómo puede ser una ventaja competitiva.
- Bonos y créditos: intercambiables por inversiones en ciberseguridad, incentivando mejoras y cumplimiento.
- Fondo de desarrollo en ciberseguridad: apoyo a soluciones y productos específicos de seguridad de la información, fomentando el desarrollo nacional.

Comunicación y Marketing

- Mensajes más atractivos para la comunicación de las carreras de ciberseguridad
- Estrategia 360 de comunicación: identificación de actores clave para clarificar los mensajes y acciones. Por ejemplo, trabajar con políticos en grupos de trabajo debido a su rol crucial.

Acciones de apoyo a actores claves

- Priorización de proveedores críticos: obligación de cumplimiento en la cadena de suministro crítico.
- Apoyo a pymes: incentivar la demanda de ciberseguridad entre clientes, mostrando los beneficios para el negocio.
- Educación desde la escuela: sensibilizar a niños y niñas en temas de ciberseguridad en el currículo escolar para desarrollar una cultura desde temprana edad en hábitos seguros y responsables.

Métricas y Evaluación

- Importancia de métricas: desarrollar métricas claras para evaluar la seguridad y concienciar sobre la gestión de datos personales.

Leyes y Marco de Ciberseguridad

- Actualización del marco regulador: simplificación de guías e implementación de CSIRT (Computer Security Incident Response Team) para sectores específicos.

Capacitación y Desarrollo de Talento

- Reskilling y formación: necesidad de capacitación continua y desarrollo de profesionales en ciberseguridad, integrando estas competencias en la formación de TI desde el inicio.

Infraestructura Crítica

- Enseñanza práctica: incluir prácticas en la educación sobre ciberseguridad, como el uso de ciber-range, para mejorar la comprensión desde la experiencia práctica.

Anexo

A continuación, se detalla las notas del intercambio realizado.

Visión del sector en materia de Ciberseguridad

- En estos dos años nos ha sido muy difícil el arrastrar a gente que le interese la ciberseguridad. Lo que me gustaría proyectar de aquí en adelante, como persona a la que le gusta difundir el conocimiento.
- La motivación a que las empresas toquen temas de ciberseguridad.
- Ver cómo afecta la ENC a cada industria.
- Rol de Agesic: momento propicio para que el rol del estado referido a la industria de TI, sea *pasar de hacer a hacer*. Habría pensar un modelo de transición que permita y regule el hacer. Pensar en cómo involucrar a la industria en el “hacer” Si pensamos más en el “*hacer – hacer*”, vamos a tener tiempo para adaptarnos.
- Quiero aportar una mirada desde el mercado. La toma de decisiones a nivel empresarial no acompaña, por lo que es importante sensibilizar a los líderes en que no es opción no dar presupuesto dado que no hay opción. El estado debe marcar lineamientos en que es importante
- Cuáles son los grandes impedimentos que tenemos a la hora de pensar en la ciberseguridad de la información, que son actitudinales porque las organizaciones están formadas por personas.
- A la hora de llevar adelante una iniciativa como es seguridad de la información se dan determinados escollos en determinados tamaños y tipos de organizaciones, que no podemos olvidarnos de ellos, uno de ellos es la APATIA (ya llegara alguien que se encargue de esto), la MIOPIA (este problema va por este lado y nos estamos perdiendo otras manifestaciones que en el fondo esta alineado). Como sensibilizamos, como enamoramos, como hacemos que se acerque más gente. Ese conocimiento falta para que todo esto pueda traccionar, sino pasa que somos un círculo chico donde somos los mismos. Esto lleva a que no terminemos rompiendo el cascarón. Esto lleva a que los que están de afuera estén alejados.
- Es importante no olvidarnos que son personas los líderes y directores, de manejar este tema con seres humanos, como llegarles y explicarles que de esto es importante.
- Hay un desconocimiento en la gente de esta problemática, donde no hay una persona en el sótano, sino que hay corporaciones del otro lado del mundo dedicándose a esto.
- Esto esta alineado con lo que decía Sebastián (Genexus), es difícil convocar y que en una institución entiendan de dónde vienen los tiros. Esto está en todos los ámbitos.

Educación y capacitación

- En lo que es educación, es muy importante impulsar la práctica.
- Apoyo que hayan creado una carrera y que estén dando.
- Leí en otras mesas y me pareció bárbaro: la Educación desde primeras etapas: absolutamente necesario.
- Sensibilización: necesitamos gente capacitada, técnicos en ciber. Necesitamos poblar varios niveles de educación. Se lanzo un analista técnico en ciber, la única institución que se animó es UTU. Quiere hacer carreras y no tienen quien dicte y diseñe esos cursos. ¿De donde podemos esperar que surjan docentes? De este ecosistema.
- Nosotros tenemos un montón de cosas para hacer, en las cuales podemos contribuir y en cuales necesitamos apoyo del Estado.
- Necesitamos desarrollar técnicos en ciber, pero en el resto de la industria de TI no ven ciberseguridad en sus carreras, lo cual es un problema. Sería bueno contemplar eso.
- Capacitación y concientización: A nivel escuela importante concientizar. Lo de la UTU está bueno, cuando yo salí de facultad no había nada.
- Aclara nuevamente: Los checklist no son suficientes, a veces no se sabe que incluyen y como están hechos.
- Comparto totalmente lo que dijo Ana. Faltan técnicos que sepan cual es el problema.
- Tenemos que hacer concientización, para nosotros entender el problema. Tenemos 10 millones de empresas que auditan y no saben que auditan. Vienen profesionales a auditar y no saben qué auditar. Hay que entender la pregunta, y validar lo que te está diciendo la persona, pero si el Auditor no sabe, pone check sin revisar, la empresa te dice lo que quieres escuchar y pasa la auditoria.
- Hoy las empresas no tienen para invertir en todo, y tienen que decidir en qué. La 27000 hace que las empresas inviertan en cosas sin valor. Y no mejoran nada de la ciberseguridad que tienen.
- La industria tiene que recomendar, de acuerdo con el nivel de madurez, y ver Uruguay en qué invertir en ciber.
- Regular la industria, será Agesic o quien sea del estado.
- Difícil conseguir desarrolladores capacitados en ciber. En otros países ya están incluidos la ciber en su concepción misma y su formación. Tenemos que generar esa cultura, llevará tiempo. Las certificaciones son complejas, las empresas chicas cumplirán porque es obligatorio.
- Difícil arrastrar gente que le interesa la ciberseguridad. Después de 2 años asistencia de 2 a 35, 40 personas. Lograr impulsar. Práctica con Cyberrange. Aprendizaje. Acotado específico que aporta un montón. Educación tratar de impulsar que la gente aprenda con la práctica en lo posible.
- Festeja que hayamos creado una Carrera de ciberseguridad.

Problemáticas y desafíos

- Hay tantas personas como percepciones.
- Me complace ver que está bastante alineado con lo que están comentando.
- Difícil conseguir desarrolladores capacitados en ciber. En otros países ya están incluidos la ciber en su concepción misma y su formación. Tenemos que generar esa cultura, llevará tiempo. Las certificaciones son complejas, las empresas chicas cumplirán porque es obligatorio.
- Es el Clearing de informes en Uruguay. Y la forma de expandirse ha sido esa, cuando empiezas a adquirir compañías, empiezas a adquirir riesgos que son inmanejables. En 2017 se dio esa filtración, y viví todas las etapas del proceso. Lo que vi, es que cuando se dan estos incidentes ves que no falla una cosa sola, son varios controles que fallan en esa cadena. De ahí vimos la transformación de Equifax los sistemas.
- ¿Como motivar y meternos en la ciber, siendo que en empresas somos números, como nos metemos en los objetivos de negocio para que sea importante? Ver la ventaja competitiva y transmitirla a los directores de las compañías. No términos tan técnicos, sino términos de negocio.
- Tenemos que el 90% de las empresas son pymes. Hay otra realidad pasando Santa Lucia, que hay más confianza y te pasan las contraseñas sin problema. Veo dificultad para entrar a esas empresas, que no suelen acceder a empresas como nosotros que estamos en empresas grandes y resultan costosos para ellos.
- ¿Si vamos a salir a ofrecer, podemos cumplir con la demanda? Porque los cupos son limitados.
- Hacerlo atractivo para pymes, es complicado entrarles y pasar de reactivo a proactivo.
- Atado a los contratos, hay un problema de contratación. Donde en los contratos
- ¿Qué acciones concretas ven para implementar en la ENC?
- Ver cómo hacer para que los demás verticales se puedan regular: salud, industria.
- Estamos trabajando con los reguladores, BCU, para que ellos le exijan a sus regulados lo que mencionan. Ese es el camino que los reguladores le exijan a sus regulados. Eso es una capacidad que Agesic no tiene. BCU tiene la posibilidad de sancionar, URSEC también.
- Estoy de acuerdo con sancionar.

Propuestas y soluciones

- Se propone: Fondo para apoyo para soluciones de empresas nacional: desde la I+D, o apoyo para soluciones.
- Encontrar la forma de apalancar, llegando con un mensaje claro a los políticos: diputados, senadores. Hablar de la problemática como es, con gente con posición/poder para articular iniciativas.
- Hablábamos de Chile, la Agencia Nacional de Ciberseguridad, que eso implica voluntad política.
- La ENC debe tener un capítulo de armar el “camino” del capital por industria, que tiene que estar la normativa y como comunicamos a las industrias. En ese marco la priorización la debe hacer el gobierno.
- Armar un equipo de trabajo Agesic – Cuti, para lograr llegar a cámaras empresariales y gremiales, para concientizar y acercarse.
- Más que castigar, iría por la positiva de generar la ventaja competitiva de negocio, una puede ser: si alcanzas determinado nivel de seguridad puedes acceder a ciertos préstamos, por ejemplo.
- Implementación de bonos de ciberseguridad.
- El estado es un traccionador natural de cambios. El estado puede poner multas si no cumples, ejemplo: si no tienes determinado nivel de seguridad, no puedes participar de licitaciones del estado.
- Pensando en el negocio y la realidad, si cumplo desde la ciberseguridad puedo acceder o descontar x cosas. Incentivo a la demanda de clientes, y no tanto al mercado de las pymes. Nuestro discurso tiene que cambiar, tiene que hablar al negocio.
- Fui a un negocio de un amigo, chacinería, la instalación eléctrica un desastre, pero nunca le paso nada. Le dije, invertí en instalación eléctrica.