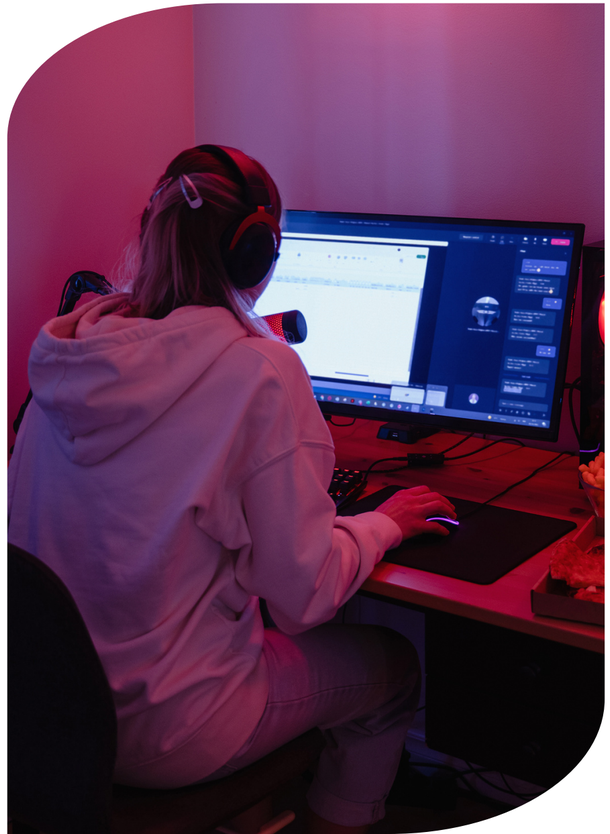


Programa de Competencias Esenciales en Ciberseguridad - PCEC

Versión 1.0
Diciembre 2023

Elaborado por:

REUNA
Ciencia y Educación en Red

Universidad De Los Lagos

Universidad de Valparaíso
CHILE

ICDT
INSTITUTO CHILENO DE DERECHO Y TECNOLOGÍAS

Programa de Competencias Esenciales en Ciberseguridad (PCEC)

Red Universitaria Nacional - REUNA
José Domingo Cañas 2819, Ñuñoa
www.reuna.cl - csirt.reuna.cl

Indice

1. Resumen Ejecutivo

Muchas actividades de la vida cotidiana, como trámites, procesos, transacciones, interacciones y más, se realizan hoy a través de sistemas digitales conectados en red, ya sea para relacionarse con otras personas o con el Estado, acceder a servicios, desarrollar actividades laborales o recreativas, o para ejercer nuestros derechos como ciudadanos.

Sin embargo, es un hecho que, en la gran mayoría de los incidentes de ciberseguridad, está involucrado el denominado "factor humano", lo que revela que, a nivel de la población general, existe una importante brecha en materia de conocimientos necesarios para que las personas puedan desenvolverse de forma segura en un mundo digital hiperconectado.

Este proyecto busca contribuir a elevar el nivel de competencias en las personas en materia de ciberseguridad, de forma masiva, esperando que ello genere un impacto significativo en la reducción de las tasas de incidentes y victimización a nivel país, y a futuro, a nivel internacional también.

Para lo anterior, se ha elaborado un Programa de Competencias Esenciales en Ciberseguridad (PCEC), que cuenta con dos principales componentes: el primero de ellos, propone un catálogo de competencias, que hemos considerado indispensables en esta materia.

El carácter de "esencial" se ha atribuido en un doble sentido: en primer lugar, como un "mínimo básico" para desenvolverse en el mundo digital de manera segura, y en segundo, como aquellas que, razonablemente, puedan ser adquiridas por cualquier persona, independientemente de su nivel de escolaridad o rango etario. Dicho en otros términos, el primer elemento fundacional de este programa es el desarrollo y mantención en el tiempo de un Marco de Competencias Esenciales en Ciberseguridad (MCEC).

El segundo componente, considera el desarrollo y validación de un instrumento de medición de dichas competencias, que permita comprobar y certificar que una persona cuenta con ellas. Esta herramienta, estará a disposición de todos los usuarios que requieran demostrarse a sí mismos y a otros actores, ya sea empleadores u otras entidades, que cuentan con las competencias consideradas esenciales en materia de ciberseguridad.

El Programa de Competencias Esenciales en Ciberseguridad es ideado e impulsado por REUNA, con la colaboración de la Universidad de Valparaíso, la Universidad de Los Lagos y el Instituto Chileno de Derecho y Tecnologías.

El presente documento, describe el proyecto, el avance a la fecha y los próximos pasos a seguir.

2. El desafío

La transformación digital está abarcando todos los sectores y esferas de nuestra vida, ya no solo en el ámbito personal, sino que también en la forma en que accedemos a servicios públicos y privados, ejercemos actividades laborales y educativas, e incluso, accedemos a prestaciones de salud. Sin embargo, no todos contamos con las competencias para desenvolvernos de forma segura en el ciberespacio. En efecto, es un hecho que, en la gran mayoría de los incidentes de ciberseguridad, está involucrado el “factor humano”.

En este contexto, un amplio sector de la academia y expertos del área de la ciberseguridad destacan la necesidad de contar con programas de concienciación. Del mismo modo, también hay consenso acerca de que la inversión en la formación en seguridad es la que mayor retorno produce, no sólo a nivel micro, sino que también a escala país. No obstante, ¿Cuáles debieran ser las competencias que debemos considerar como esenciales, para que puedan, razonablemente, ser adquiridas por un amplio y transversal conjunto de personas, independientemente de su nivel de escolaridad, rango etario u otros aspectos?, ¿Cómo lograr que este conocimiento llegue a todas las personas? Y finalmente, ¿Cómo deberíamos proceder para incentivar que estas competencias puedan ser adquiridas por las personas de forma masiva? Estas son las preguntas que nos hemos planteado para abordar el desafío.

3. Estado del arte

En primer lugar, nos preguntamos si existía una definición de cuáles debiesen ser las competencias esenciales en materia de ciberseguridad, para la ciudadanía en general. Para averiguarlo, a lo largo del primer semestre de 2023, se revisaron los principales marcos de competencias digitales que, en mayor o menor medida, abordan también competencias relacionadas con la ciberseguridad (ver Tabla 1).

De ello, resultó que ninguno de los marcos analizados está específicamente dirigido al tema de interés y, además, se pudo observar que ninguno de ellos aborda de forma exhaustiva el ámbito de la ciberseguridad para la ciudadanía en general, ni tampoco lo hace con un enfoque en la esencialidad, en el sentido que hemos planteado antes, en cuanto a su alcance universal y básico.

MARCO o PROGRAMA (8)	ORGANIZACIÓN
The Digital Competence Framework for Citizens DIGICOMP 2.2	European Commission
Digital Literacy Skills Framework	Department of Education Skills and Employment | Australian Government
Matriz de habilidades digitales	Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la UNAM | México
Marco de competencias de los docentes en materia de TIC	UNESCO
Digital capabilities framework - Learner profile - Six elements of digital capabilities	Joint Information Systems Committee – JISC | U.K.
ECDL/ICDL European/International Computer Driving License	ICDL Foundation
Matriz de Habilidades TIC para el Aprendizaje	Enlaces - Ministerio de Educación | Chile
British Columbia Digital Literacy Framework	University of British Columbia | USA

Tabla 1 - Marcos de competencias revisados

El marco que de forma más acabada y estructurada aparece abarcando competencias relacionadas con la ciberseguridad, y en particular para la ciudadanía, es el European Digital Competence Framework for Citizens DigiComp 2.2[1], que efectivamente identifica 4 competencias relacionadas en el área denominada “seguridad”, de un total de 21 que releva en el ámbito digital. La caracterización de cada una de dichas competencias está estructurada a través de 5 dimensiones descriptivas: 1. “Área de Competencia”, 2. “Competencia”, 3. “Niveles de Competencia”, 4. “Ejemplos de conocimiento, habilidades y actitudes” y 5. “Casos de uso”.

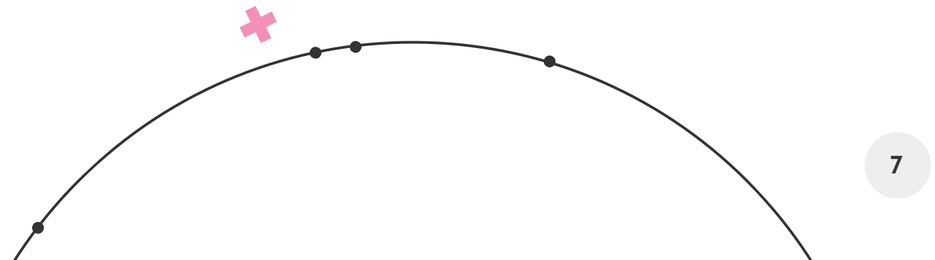
A pesar de que la dimensión 3 (“Niveles de Competencia”) proporciona formulaciones en distintos niveles para cada competencia, adolece de problemas de coherencia interna, que dificultan su adopción como modelo de trabajo. Como ejemplo, para la competencia 4.1 “Protección de dispositivos” incluye desde: “Identificar formas sencillas de proteger mis dispositivos...” (nivel 1) hasta: “Crear soluciones para resolver problemas complejos con muchos factores que interactúan...” (nivel 8), sin embargo, no declara qué niveles serían aquellos que debieran ser alcanzables por cualquier persona. Luego, en su siguiente dimensión descriptiva 4 (“Ejemplos de conocimiento, habilidades y actitudes”) se limita a proponer algunos ejemplos, declarando expresamente que no es exhaustivo, en cuanto a cuáles serían las habilidades, conocimientos y actitudes necesarios para obtener los resultados de aprendizaje esperables; tampoco indica la relación de dichos ejemplos con las formulaciones de Niveles de Competencia expresados en la dimensión 3 previa.

En conclusión, no hemos visualizado que este marco se corresponda con el objetivo que nos hemos planteado, pese a reconocer que se trata probablemente de uno de los marcos de competencias digitales para la ciudadanía más completos.

En segundo lugar, se revisaron 14 programas de concienciación o “awareness” en ciberseguridad, destinados a personas no profesionales del rubro, llevados a cabo por gobiernos y organizaciones nacionales e internacionales que juegan un rol reconocido en esta materia (ver Tabla 2).

Exploramos si alguno de los programas analizados declaraba basarse en algún marco de competencias existente y, como resultado, se pudo determinar que ninguno de ellos lo hacía. La relevancia de estos programas es que representan los contenidos que hoy en día se considera que es importante entregar a todas las personas en un mismo nivel.

[1] Vuorikari, R., Kluzer, S. and Punie, Y., DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415.



PAÍS / ORGANIZACIÓN (14)	ENLACE (URL)
AUSTRALIA	https://www.cyber.gov.au/
CANADA Public Safety	https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx
Center for Internet Security CIS	https://www.cisecurity.org/
Center for Development of Security Excellence	https://www.cdse.edu/
CISA Cybersecurity & Infrastructure Security Agency	https://www.cisa.gov/sites/default/files/publications/CAM22_PublicToolkit_FINAL_OCC_CSD_DIR_508c.pdf
Digital Citizen Alliance	https://www.digitalcitizensalliance.org/
ENISA	https://www.enisa.europa.eu/
ESPAÑA - INCIBE	https://www.incibe.es/
ESPAÑA - Oficina de Seguridad del Internauta	https://www.osi.es/es
ESTONIA	https://www.itvaatlik.ee/kontrolli/ y https://www.itvaatlik.ee/
IRLANDA	https://www.webwise.ie/welcome-to-webwise/us/
SINGAPORE	https://www.csa.gov.sg/
USA - Homeland Security	https://www.dhs.gov/privacy-training
USA - National Cybersecurity Alliance	https://staysafeonline.org/

Tabla 2 - Países y organizaciones cuyos programas de concienciación fueron revisados

Finalmente, nos preguntamos si existía algún programa que permitiera certificar competencias esenciales en materia de ciberseguridad para ciudadanos. Entre los que más podrían acercarse, encontramos la iniciativa “Digital Skills and Jobs Platform”, financiada por el Programa Europa Digital de la Unión Europea, y que busca mejorar la competitividad de Europa en la economía digital global, mediante el desarrollo de habilidades digitales en todos sus ciudadanos. En particular, la plataforma asociada al programa aspira a impulsar las competencias digitales de la sociedad y la fuerza laboral europeas, y pone a disposición herramientas para que las personas puedan medir sus habilidades digitales[2]. Sin embargo, este programa no permite certificarlas ni tampoco se enfoca exclusivamente o en particular en las competencias relacionadas con la ciberseguridad, sino que se dirige a un marco más amplio de competencias digitales[3].

Por otra parte, identificamos plataformas que permiten evaluar competencias, como Astride de Exin, y otras iniciativas de diferentes organizaciones y agencias nacionales en Europa, que se enfocan, principalmente, en el mundo laboral, y están basadas en el Marco Europeo de e-Competencias (e-CF)[4], común para todos los profesionales de las Tecnologías de la Información y la Comunicación (TIC). Es decir, se trata de iniciativas que tampoco se dirigen a toda la ciudadanía ni se refieren a la ciberseguridad en particular.

En conclusión, a pesar de que existen varias iniciativas y avances en la materia, no se ha encontrado un marco específico relacionado con competencias que puedan calificarse como esenciales en ciberseguridad, así como tampoco se han encontrado programas que estén dirigidos a acreditar o certificar que las personas cuentan con estas competencias. De ahí entonces que se ha considerado la necesidad y oportunidad de abordar este desafío, pensando también en el impacto y beneficios que podrían alcanzarse al cerrar esta brecha.

[2] European Union(s.f). Europass. Test your digital skills!. https://europa.eu/europass/digitalskills/screen/home?referrer=epass&route=%2Fen
[3] European Union(s.f). Digital Skills & Jobs plaform. Test your digital skills!. https://digital-skills-jobs.europa.eu/digitalskills/screen/home?referrer=dsjp
[4] European Commission (s.f.). European e-Competence Framework (e-CF). https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf

4. El proyecto

El proyecto tiene como objetivo lograr que una gran parte de la ciudadanía pueda adquirir y demostrar que cuenta con las competencias esenciales en ciberseguridad, para desenvolverse de forma segura en un mundo digital hiperconectado. Para ello, se ha diseñado un programa estructurado en dos componentes principales.

Por un lado, el desarrollo y definición de un Marco de Competencias Esenciales, como insumo básico para el programa. Este componente busca incorporar todas las competencias consideradas básicas para poder desenvolverse de forma segura a nivel de usuario, al mismo tiempo que responde a un imperativo de transversalidad y minimalismo, en el sentido de que se limite a aquellas que puedan ser adquiridas por la gran parte de la población, tal como ya se ha señalado anteriormente. De ahí el doble carácter del rasgo “esenciales”.

Por otra parte, el segundo componente consistente en una herramienta que permita la medición y certificación de dichas competencias, que sea susceptible de ser aplicada de forma masiva y transversal, por parte de toda o casi toda la ciudadanía. Con ello, se busca que esta certificación pueda ser reconocida por los demás actores e instancias de la vida social, económica, laboral, educacional, etc. en donde contar con estas competencias resulte relevante y valioso.

Como puede desprenderse de lo antes descrito, el beneficiario final del proyecto es la sociedad en su conjunto, al contribuir a su madurez en materia de ciberseguridad y en la reducción significativa de las tasas de incidentes de ciberseguridad, relacionados a casos en los que el “factor humano” pudo haber jugado algún rol.

5. Desarrollo del marco de competencias

En el desarrollo de este proyecto se optó por un enfoque basado en competencias, entendidas como: “las capacidades que todo ser humano necesita para resolver, de manera eficaz y autónoma, las situaciones de la vida. Se fundamentan en un saber profundo, no sólo saber qué y saber cómo, sino saber ser persona en un mundo complejo, cambiante y competitivo”[5], porque eleva a la persona como protagonista de su aprendizaje.

A partir del análisis de los marcos de competencias (Tabla 1) y los programas de concienciación (Tabla 2) se procedió a determinar los temas recurrentes, su profundidad, la correspondencia de sus contenidos y la factibilidad de organizarlos en categorías, para, finalmente, identificar las competencias que emanan de ellos.

Con este objetivo, tuvo lugar una serie de sesiones de trabajo, en las que participó un grupo multidisciplinario de integrantes de REUNA, la Universidad de Valparaíso, la Universidad de Los Lagos y el Instituto Chileno de Derecho y Tecnologías, facilitadas por un coordinador (ver más adelante los Miembros del Grupo de Trabajo).

[5] Beneitone, P., Esquetini, C., González, J., Maletá, M., Siufi, G., y Wangenaar, R. (2007). Reflexiones y perspectivas de la Educación Superior en América Latina. Informe Final - Proyecto Tunning - en América Latina 2004-2007. Universidad de Deusto. ISBN: 978-84-9830-645-3.

La primera ronda de sesiones de trabajo estuvo dirigida a identificar, expresar y consensuar los dominios de interés que se podían deducir, a partir de todo el trabajo previo de revisión de marcos de competencia y programas de concienciación. A través de esta ronda, se identificaron y acordaron siete dominios en los que se podían organizar las competencias esenciales.

En la siguiente ronda de sesiones de trabajo, se identificó, consensuó y formuló una competencia esencial en ciberseguridad asociada, respectivamente, a cada uno de los dominios identificados en el paso previo.

Y finalmente, a través de una tercera ronda de sesiones de trabajo, para cada una de las siete competencias establecidas, se formuló un conjunto de resultados de aprendizaje esperados, organizados en tres niveles, los que, junto con las respectivas competencias y dominios, han determinado la primera versión del componente Marco de Competencias Esenciales en Ciberseguridad (MCEC).

En aquellos casos en que el nivel 3 se consideró muy complejo para los objetivos de transversalidad y universalidad, los resultados de aprendizaje fueron omitidos. No obstante, esto no impide que, en el futuro, ante la evidencia de un mayor grado de validez, estos puedan ser incluidos.

6. Marco de Competencias Esenciales en Ciberseguridad v1.0

A continuación, se presentan los dominios, competencias y resultados de aprendizaje que conforman la primera versión del Marco de Competencias Esenciales en Ciberseguridad (MCEC), que corresponde al primer componente del Programa de Competencias Esenciales en Ciberseguridad (PCEC).

DOMINIO	COMPETENCIA ESENCIAL
1. Conciencia de amenazas cibernéticas	**CE1:** Reconocer las diferentes clases de amenazas y riesgos existentes en el espacio digital y su impacto, para comprender la importancia de adoptar medidas de seguridad.
2. Gestión de identidad y acceso en línea	**CE2:** Gestionar el perfil personal y credenciales asociadas al registro, ingreso e interacción en línea para proteger su identidad y dichas credenciales.
3. Seguridad de dispositivos y aplicaciones	**CE3:** Aplicar medidas de protección en dispositivos y aplicaciones para evitar accesos ilícitos a la información y minimizar el riesgo de fugas y ciberataques.
4. Seguridad en Internet y redes	**CE4:** Aplicar medidas de seguridad en la conectividad y navegación en red, para prevenir accesos no autorizados e intrusiones ilegítimas.
5. Ingeniería social y protección de la privacidad	**CE5:** Proteger su información frente a posibles amenazas o intentos de obtención indebida de sus datos personales en línea, para evitar ser víctima de fraudes y vulneración de sus derechos.
6. Manejo seguro de datos	**CE6:** Implementar medidas de gestión segura de información crítica, datos personales, datos personales sensibles e información confidencial de forma permanente, para prevenir o minimizar pérdidas, deterioros, accesos no autorizados e incumplimientos normativos.
7. Respuesta a incidentes	**CE7:** Detectar la ocurrencia de un incidente de ciberseguridad para informar y adoptar medidas de respuesta.

CE1: Reconocer las diferentes clases de amenazas y riesgos existentes en el espacio digital y su impacto, para comprender la importancia de adoptar medidas de seguridad.

Resultados de Aprendizaje

Nivel 1	Nivel 2	Nivel 3
RA1.1.1 Identifica las principales amenazas de ciberseguridad, tales como software malicioso, técnicas de ingeniería social u otros, que existen en el espacio digital para reducir la probabilidad de verse afectado	RA1.2.1 Comparte información sobre amenazas emergentes y buenas prácticas con su entorno para promover una cultura de conciencia de ciberseguridad.	
RA1.1.2 Reconoce las posibles consecuencias de las amenazas de ciberseguridad, relacionadas al quehacer cotidiano, para valorar la importancia del rol que puede ejercer como usuario.		
RA1.1.3 Comprende los elementos de una gestión básica de riesgos necesaria para tomar decisiones informadas sobre las prácticas de ciberseguridad en el quehacer cotidiano.		

CE2: Gestionar el perfil personal y credenciales asociadas al registro, ingreso e interacción en línea para proteger su identidad y dichas credenciales.

Resultados de Aprendizaje

Nivel 1	Nivel 2	Nivel 3
RA2.1.1 Reconoce los distintos componentes asociados a la creación de perfil personal en línea para configurar adecuadamente sus credenciales de acceso.	RA2.2.1 Registra en su perfil información válida y actualizada sobre su identidad.	RA2.3.1 Crea credenciales de autenticación y acceso robustas y únicas para cada servicio para minimizar el riesgo de accesos fraudulentos o ilegítimos, la suplantación de su identidad en línea o la realización de transacciones fraudulentas.
	RA2.2.2 Resguarda su identidad personal en aquellos servicios en los cuales no le consta la salvaguarda de sus derechos.	
RA2.1.2 Comprende la importancia de identificarse y autenticarse adecuadamente en los servicios tecnológicos en los que su actividad tiene impacto en su situación jurídica.	RA2.2.3 Protege su identidad y credenciales de acceso, al participar en los ambientes virtuales.	RA2.3.2 Crea perfiles especiales para aquellos sitios o servicios cuya seguridad y respeto de sus derechos no le consta.
RA2.1.3 Reconoce la importancia de resguardar la información que le permite a un tercero, identificarlo de forma únivoca.	RA2.2.4 Utiliza mecanismos de autenticación de más de un factor para sus aplicaciones y cuentas en línea para minimizar el riesgo de accesos fraudulentos o ilegítimos.	RA2.3.3 Asegura el cierre de sus sesiones en los equipos, dispositivos y servicios en línea posterior a su uso, cada vez que existe el riesgo de que terceros accedan a través del mismo medio.
	RA2.2.5 Aplica las buenas prácticas relacionadas con el resguardo adecuado de las credenciales de autenticación y acceso para prevenir que caigan en manos de terceros.	RA2.3.4 Configura adecuadamente sus preferencias de privacidad en sus cuentas y servicios en línea para el resguardo de su información personal y salvaguarda de sus derechos.

CE3: Aplicar medidas de protección en dispositivos y aplicaciones para evitar accesos ilícitos a la información y minimizar el riesgo de fugas y ciberataques.

Resultados de Aprendizaje

Nivel 1	Nivel 2	Nivel 3
RA3.1.1 Comprende la importancia y riesgo de no leer los Términos y Condiciones de Uso de las Aplicaciones y Software que utiliza.	RA3.2.1 Configura adecuadamente el software antivirus de sus dispositivos para prevenir la acción de software malicioso en los dispositivos que utiliza.	
RA3.1.2 Comprende la importancia de descargar aplicaciones solo de fuentes verificadas para prevenir software malicioso.	RA3.2.2 Verifica el origen de programas, aplicaciones y archivos previo a su descarga e instalación en sus dispositivos, para prevenir la instalación de software malicioso.	
RA3.1.3 Comprende la importancia de revisar y configurar adecuadamente los permisos de acceso y la configuración de privacidad de las aplicaciones que utiliza para proteger su información y sus activos digitales.	RA3.2.3 Configura adecuadamente el sistema operativo y las aplicaciones que utiliza para que se requiera autenticación del usuario con credenciales robustas previo a poder acceder a ellas con la finalidad de prevenir o minimizar la posibilidad de accesos indebidos.	
RA3.1.4 Comprende la importancia de proteger el acceso a sus dispositivos y las aplicaciones que utiliza aplicaciones (incluye el sistema operativo) a través de mecanismos de autenticación seguros.	RA3.2.4 Actualiza periódicamente el sistema operativo y las aplicaciones de los dispositivos que utiliza para parchar oportunamente las vulnerabilidades conocidas.	
RA3.1.5 Reconoce los riesgos relacionados con el uso de dispositivos extraíbles para prevenir verse afectado por software malicioso o pérdidas de información.	RA3.2.5 Aplica las opciones de cifrado de seguridad en los dispositivos y aplicaciones que utiliza para proteger la información que maneja e intercambia.	
RA3.1.6 Identifica los riesgos de perder el control de los dispositivos que utiliza.		

CE4: Aplicar medidas de seguridad en la conectividad y navegación en red, para prevenir accesos no autorizados e intrusiones ilegítimas.

Resultados de Aprendizaje

Nivel 1	Nivel 2	Nivel 3
RA4.1.1 Comprende la importancia de aplicar medidas de seguridad en la conectividad y navegación en red para prevenir intrusiones ilegítimas.	RA4.2.1 Aplica medidas tecnológicas de protección que resguarden sus canales de comunicación electrónicas para contribuir a la seguridad de las comunicaciones.	RA4.3.1 Evalúa las medidas tecnológicas de protección de los canales de comunicación en atención a la criticidad de los contenidos y actividades en línea.
RA4.1.2 Identifica las medidas de seguridad más relevantes cuando se conecta y navega a través de las redes y canales de comunicación para lograr una navegación y uso seguro de las redes.	RA4.2.2 Aplica tecnologías de cifrado de la información en tránsito para proteger la privacidad y confidencialidad de la comunicación.	
RA4.1.3 Comprende la importancia de constatar que la URL de un recurso en red sea legítima y corresponda al titular esperado.	RA4.2.4 Verifica que la URL de un recurso en red sea legítima y corresponda al titular esperado.	
RA4.1.4 Comprende el significado de lo que aseguran los certificados digitales asociados a los dominios de los sitios web y sus URLs	RA4.2.4 Verifica los certificados de los sitios y recursos en red a los que accede.	
RA4.1.5 Comprende los riesgos asociados a las WiFi públicas durante la navegación para evitar intrusiones ilegítimas.	RA4.2.5 Aplica medidas de protección de sus dispositivos y de los canales de comunicación cuando accede a WiFi públicas o de las que no tiene control para contribuir a la seguridad de las comunicaciones.	

CE5: Proteger su información frente a posibles amenazas o intentos de obtención indebida de sus datos personales en línea, para evitar ser víctima de fraudes y vulneración de sus derechos.

Resultados de Aprendizaje

Nivel 1	Nivel 2	Nivel 3
RA5.1.1 Conoce los conceptos clave de huella digital, phishing, spear-phishing, vishing and smishing entre otros, asociados a los ataques de ingeniería social para identificar posibles amenazas.	RA5.2.1 Comprende los conceptos clave de huella digital, phishing, spear-phishing, vishing and smishing entre otros, asociados a los ataques de ingeniería social para identificar posibles amenazas.	RA5.3.1 Comparte información relevante y buenas prácticas respecto a conceptos clave de ingeniería social para identificar posibles amenazas.
RA5.1.2 Conoce las amenazas de ingeniería social y los riesgos del uso indebido de su información para evitar ser víctima de fraudes y vulneración de sus derechos.	RA5.2.2 Detecta un ataque de ingeniería social evitando entregar la información solicitada fraudulentamente para minimizar la posibilidad de ser víctima de fraudes y vulneración de derechos.	RA5.3.2 Alerta a las comunidades en las que participa sobre intentos de ingeniería social que ha detectado para evitar que terceros sean víctimas de fraudes y vulneración de sus derechos.
RA5.1.3 Conoce la existencia de leyes y regulaciones asociadas a la protección de datos para manejar adecuadamente su información personal.	RA5.2.3 Comprende cómo ejercer sus derechos en materia de protección de datos para proteger su información personal.	RA5.3.3 Comparte información relevante y buenas prácticas respecto a la protección de datos para minimizar los riesgos asociados a la divulgación de la información personal.

CE6: Implementar medidas de gestión segura de información crítica, datos personales, datos personales sensibles e información confidencial de forma permanente, para prevenir o minimizar pérdidas, deterioros, accesos no autorizados e incumplimientos normativos.

Resultados de Aprendizaje

Nivel 1	Nivel 2	Nivel 3
RA6.1.1 Comprende sus derechos ARCOP respecto de su información personal (acceso, rectificación, cancelación o eliminación, oposición-bloqueo y portabilidad de los datos personales que obran en poder del organismo)	RA6.2.1 Ejerce sus derechos ARCOP cada vez que quiere controlar el acceso o uso que terceros hagan de su información.	RA6.3.1 Evalúa el posible impacto de la entrega y uso la información crítica, los datos personales, datos personales sensibles, e información confidencial.
RA6.1.2 Comprende la importancia de proteger su información personal y datos sensibles.	RA6.2.2 Encripta la información crítica, confidencial y los datos sensibles.	RA6.3.2 Evalúa los mecanismos de protección de la información de acuerdo a los niveles de seguridad que proporcionan.
RA6.1.3 Identifica la información crítica, los datos personales, datos personales sensibles, e información confidencial.	RA6.2.3 Protege las claves utilizadas para encriptar la información crítica, confidencial y los datos sensibles.	RA6.3.3 Clasifica la información y evalúa los riesgos asociados a su gestión.
RA6.1.4 Identifica la información que consta en dispositivos y su nivel de protección.	RA6.2.4 Realiza respaldos periódicos de información relevante para prevenir pérdidas o deterioros.	
RA6.1.5 Identifica los riesgos de perder el control de los dispositivos que utiliza para la gestión de la información.	RA6.2.5 Destruye de manera segura la información que consta en dispositivos de los cuales perderá el control.	

CE7: Detectar la ocurrencia de un incidente de ciberseguridad para informar y adoptar medidas de respuesta.

Resultados de Aprendizaje

Nivel 1	Nivel 2	Nivel 3
RA7.1.1 Comprende el concepto de incidente de ciberseguridad y su potencial impacto.	RA7.2.1 Detecta incidentes de ciberseguridad para informar y adoptar medidas de respuesta.	RA7.3.1 Evalúa el nivel de impacto de un incidente de ciberseguridad del que haya tomado conocimiento.
RA7.1.2 Comprende la importancia de aplicar medidas de respuesta para mitigar o reducir el impacto de un incidente de ciberseguridad.	RA7.2.2 Reconoce las distintas medidas de respuesta para mitigar o reducir el daño de un incidente de ciberseguridad	RA7.3.2 Evalúa medidas de respuesta pertinentes a un incidente de ciberseguridad del que haya tomado conocimiento.
RA7.1.3 Identifica los canales disponibles para notificar un incidente de ciberseguridad.	RA7.2.3 Informa incidentes de ciberseguridad a través del canal adecuado para que se adopten las medidas de mitigación y respuesta por parte de quien corresponda.	RA7.3.3 Documenta un incidente de ciberseguridad para los efectos de gestionar el conocimiento que permita prevenir o reducir el riesgo de nuevos incidentes.
		RA7.3.4 Comparte con sus pares información relevante sobre cómo identificar y notificar un incidente de ciberseguridad del que haya tomado conocimiento.

7. Miembros del grupo de trabajo

- Paola Arellano - REUNA
- Cristina Bonifaz - Universidad de Valparaíso
- Lorena Donoso - Instituto Chileno de Derecho y Tecnologías
- Mónica Gallardo - Universidad de Los Lagos
- Claudia Inostroza - REUNA
- Maurizio Mattoli - REUNA
- Patricia Reyes - Universidad de Valparaíso
- Claudia Saldía - Universidad de Los Lagos

8. Próximos pasos

A continuación, se describen las actividades que se desarrollarán a partir de 2024 en el ámbito del Programa de Competencias Esenciales en Ciberseguridad (PCEC):

1. Validación externa del MCEC v1.0

Conciliar la necesidad y aspiración de incorporar las competencias de ciberseguridad que permitan desenvolverse de la forma más segura posible en el mundo digital, con el objetivo de seleccionar solo aquellas que consideramos básicas y esenciales, representa un ejercicio de análisis, ponderación y mediación muy desafiante.

Para dar a la luz algo aparentemente simple, se requiere en realidad de mucha reflexión, desde diferentes miradas o perspectivas. El Marco de Competencias Esenciales en Ciberseguridad (MCEC) desarrollado hasta el momento, representa una primera versión que requiere una validación más amplia, para asegurar que se incorporen más perspectivas y pueda perfeccionarse. Del mismo modo, requerirá de un proceso de revisión periódica, puesto que vivimos en un mundo en constante evolución.

2. Desarrollo de una herramienta de medición de las competencias del MCEC

Por definición, toda competencia debe ser medible. Por esta razón, otro de los componentes fundamentales de este programa es contar con una herramienta que permita medir y certificar que una determinada persona cuenta con las competencias esenciales en ciberseguridad.

3. Pilotaje

A partir del MCEC validado y de la disponibilidad de un instrumento de medición basado en dicho marco, es preciso poner a la prueba estas herramientas, para ver si “resisten” el contacto con la realidad o si se requerirá introducir ajustes. Con este propósito, se diseñará e implementará, en primera instancia, un pilotaje de ambas componentes, dirigido preliminarmente a un universo inicial de personas que reúnan aquellas características que se correspondan al objetivo planteado.

De esta experiencia, se espera poder recoger insumos y aprendizajes, que puedan resultar útiles para ajustar y perfeccionar el programa.

Red Universitaria Nacional, REUNA, es una corporación sin fines de lucro integrada por universidades, centros de investigación de excelencia y grupos astronómicos internacionales. Es la Red Nacional de Investigación y Educación de Chile (NREN por su sigla en inglés) y actualmente, está conformada por más de 45 instituciones.

www.reuna.cl - csirt.reuna.cl

red_reuna

reuna.chile

reunachile