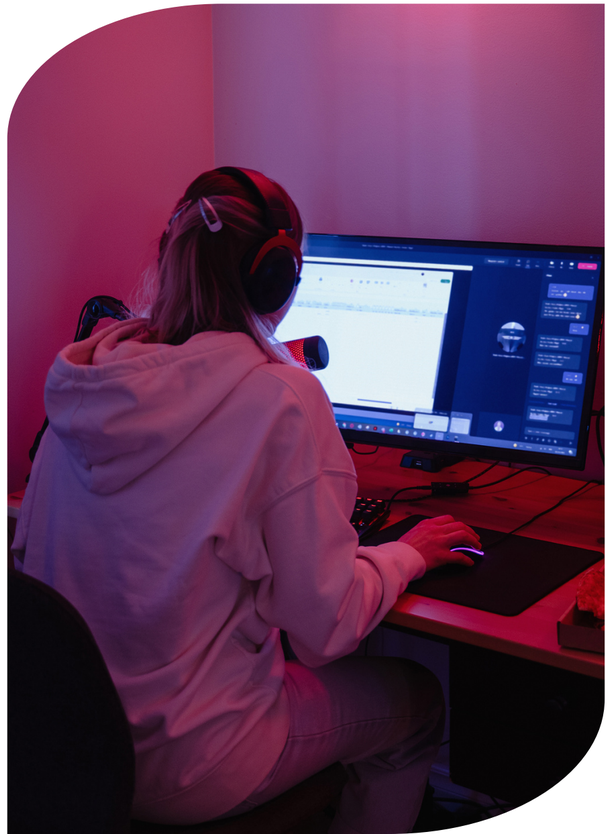

Marco de Competencias Esenciales en Ciberseguridad - MCEC

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

Marco de Competencias Esenciales en Ciberseguridad (MCEC)

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

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.

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