



Servicios laborales y productivos para
personas con diversidad funcional

Ciberseguridad para usuarios de Entidades de la Economía Social: Estudio Integral de Riesgos y Estrategias de Protección



MINISTERIO
DE TRABAJO
Y ECONOMÍA SOCIAL





www.fundacioel7.org





www.fundacioel7.org

Índice

Resumen Ejecutivo	6
Principales Hallazgos y Recomendaciones Estratégicas	7
Impacto Esperado y Sostenibilidad	7
Introducción y Marco Conceptual	9
Contexto y Motivación de la Investigación	9
El Sector de la Economía Social: Definiciones y Características	10
Poblaciones Vulnerables y Exclusión Digital	11
Objetivos y Alcance de la Investigación	12
Metodología de Investigación.....	13
Contexto Normativo y Regulatorio Español	15
Marco Regulatorio Actualizado para 2025	15
Actualizaciones Normativas Relevantes para 2025.....	16
Protecciones Especiales para Usuarios Vulnerables	17
Obligaciones de Notificación y Transparencia	17
Régimen Sancionador Adaptado	18
Colaboración con Autoridades Competentes	18
Panorama de Ciberseguridad en la Economía Social.....	20
Estadísticas de Ciberataques en el Sector	20
Tipos de Entidades y Vulnerabilidades Específicas	20
Limitaciones de Recursos y Capacidades	22
Desafíos de Infraestructura Tecnológica	22
Casos Reales Documentados	23
Impacto en Poblaciones Vulnerables	24
Tendencias Emergentes de Amenazas	24
Hoja de Ruta de Blindaje Cibernético	26
Marco Estratégico Integral.....	26
Gobernanza y Cultura de Ciberseguridad.....	27
Medidas Técnicas Prioritarias	27
<i>Gestión de Identidad y Acceso.....</i>	<i>28</i>
<i>Protección de Datos y Cifrado.....</i>	<i>28</i>



www.fundacioel7.org

<i>Copias de Seguridad y Recuperación</i>	29
Estrategias Diferenciadas por Recursos	29
<i>Organizaciones de Recursos Muy Limitados</i>	29
<i>Organizaciones de Recursos Limitados</i>	30
<i>Organizaciones de Recursos Medios</i>	30
<i>Organizaciones Grandes</i>	30
Análisis de Riesgos para Usuarios Vulnerables	31
Perfiles de Vulnerabilidad y Factores de Riesgo	31
<i>Vulnerabilidades Relacionadas con la Edad</i>	31
<i>Vulnerabilidades Relacionadas con Discapacidades</i>	32
<i>Vulnerabilidades Socioeconómicas</i>	33
Vectores de Amenaza Específicos.....	33
<i>Phishing y Estafas por Correo Electrónico</i>	33
<i>Vishing y Suplantación Telefónica</i>	34
<i>Estafas en Redes Sociales y Mensajería</i>	34
<i>Malware y Ransomware Dirigido</i>	35
Análisis Cuantitativo de Riesgos	35
<i>Estadísticas de Victimización por Demografía</i>	35
<i>Factores Psicológicos en la Susceptibilidad</i>	36
<i>Metodología de Evaluación de Riesgos</i>	36
Vulnerabilidades en Procesos Digitales.....	37
<i>Trámites Administrativos Obligatorios</i>	37
<i>Uso de Dispositivos Compartidos</i>	37
<i>Dependencia de Terceros para Asistencia Digital</i>	38
Protocolos de Actuación y Estrategias de Mitigación	39
Educación y Concienciación Diferenciada	39
<i>Programas de Formación Adaptados por Nivel de Alfabetización</i>	39
<i>Materiales Educativos Accesibles</i>	39
<i>Simulaciones y Ejercicios Prácticos</i>	40
Medidas Técnicas de Protección Reforzada.....	41
<i>Filtros Anti-Phishing y Seguridad del Correo</i>	41
<i>Protección de Dispositivos y Redes</i>	41



www.fundacioel7.org

<i>Gestión de Identidades y Accesos Adaptativa</i>	42
Protocolos de Respuesta a Incidentes Especializados	42
<i>Procedimientos ante Phishing Dirigido</i>	42
<i>Respuesta a Ransomware</i>	43
<i>Gestión de Violaciones de Datos de Beneficiarios</i>	43
Estrategias de Mitigación por Tipo de Riesgo.....	44
Contramedidas para Phishing y Fraudes Online	44
Protección contra Vishing y Suplantación Telefónica	44
Prevención de Malware y Ransomware.....	45
Protección de Privacidad y Datos Personales	45
Colaboración Interinstitucional y Redes de Apoyo	46
Redes de Intercambio de Información	46
Colaboración con Sector Privado	46
Coordinación con Autoridades	47
Conclusiones y Recomendaciones	48
Síntesis de Hallazgos Principales	48
Contribuciones Teóricas y Prácticas.....	48
Recomendaciones Estratégicas.....	49
Implicaciones para el Desarrollo de Políticas	49
Direcciones para Investigación Futura.....	50
Llamada a la Acción	50
Referencias y Fuentes	51



www.fundacioel7.org

Resumen Ejecutivo

La transformación digital acelerada de los últimos años ha expuesto a las entidades de la Economía Social española a una nueva generación de amenazas cibernéticas que requieren respuestas especializadas y adaptadas a sus características únicas. Este estudio integral consolida y sintetiza los hallazgos de múltiples investigaciones para proporcionar un marco comprensivo de ciberseguridad específicamente diseñado para cooperativas, fundaciones, asociaciones, mutualidades y empresas sociales que atienden a poblaciones vulnerables.

El sector de la Economía Social en España comprende aproximadamente 43.000 entidades que representan el 12,5% del empleo nacional y gestionan información sensible de millones de usuarios, muchos de ellos en situación de vulnerabilidad o riesgo de exclusión social [1]. Sin embargo, estas organizaciones enfrentan desafíos únicos que las distinguen tanto de las empresas comerciales como de las administraciones públicas tradicionales: operan con recursos limitados, atienden a poblaciones con baja alfabetización digital, y mantienen culturas organizacionales que priorizan la accesibilidad y la confianza sobre las restricciones de seguridad.

La investigación revela datos alarmantes sobre la exposición del sector a amenazas cibernéticas.

España ocupa el tercer lugar mundial en ciberataques recibidos, mientras que las pérdidas por ciberestafas dirigidas específicamente a personas mayores alcanzan los 3.000 millones de euros anuales [2]. En el ámbito organizacional, el 31% de las organizaciones benéficas han experimentado brechas de ciberseguridad en los últimos 12 meses, con reclamaciones promedio que alcanzan los 86.500 euros [3]. Particularmente preocupante es el hecho de que el 60% de las pequeñas empresas cierra en los seis meses posteriores a un ciberataque, una estadística que cobra especial relevancia para las entidades de Economía Social que operan con márgenes ajustados y dependen de la confianza comunitaria [4].

El análisis identifica tres categorías principales de vulnerabilidades que afectan desproporcionadamente al sector. Las vulnerabilidades organizacionales incluyen presupuestos de ciberseguridad que son un 42% menores que los de empresas comerciales equivalentes, dependencia de personal voluntario sin formación especializada en seguridad y infraestructura tecnológica frecuentemente desactualizada [5]. Las vulnerabilidades de los usuarios atendidos abarcan factores demográficos como la edad avanzada y las discapacidades, factores socioeconómicos como la pobreza y el aislamiento social, y factores tecnológicos como la limitada alfabetización digital y el acceso restringido a dispositivos seguros [6]. Finalmente, las vulnerabilidades sistémicas incluyen la creciente digitalización de servicios esenciales sin alternativas presenciales, la dependencia de terceros para servicios tecnológicos, y la falta de marcos de ciberseguridad específicamente diseñados para el sector social.



www.fundacioel7.org

Principales Hallazgos y Recomendaciones Estratégicas

El estudio propone un marco estratégico integral construido sobre cuatro pilares fundamentales que abordan las características únicas del sector de la Economía Social.

El primer pilar, Diseño de Seguridad Inclusiva, reconoce que las medidas de ciberseguridad deben acomodar diversas capacidades de usuario, incluyendo personas con discapacidades cognitivas o sensoriales, adultos mayores con limitada experiencia tecnológica, y usuarios con recursos económicos restringidos. Este enfoque requiere el desarrollo de interfaces multimodales, procedimientos de autenticación adaptativa, y contenido educativo culturalmente apropiado.

El segundo pilar, Protección Centrada en la Comunidad, aprovecha las redes sociales existentes para crear sistemas de seguridad colectiva. Las entidades de Economía Social poseen una ventaja única en forma de relaciones de confianza establecidas con sus usuarios, que pueden ser aprovechadas para crear sistemas de verificación comunitaria, redes de alerta temprana, y programas de educación peer-to-peer que son más efectivos que los enfoques tradicionales de arriba hacia abajo.

El tercer pilar, Gestión Adaptativa de Riesgos, reconoce que las amenazas cibernéticas evolucionan constantemente y que las organizaciones con recursos limitados necesitan sistemas que puedan adaptarse rápidamente a nuevas circunstancias. Esto incluye el desarrollo de protocolos de respuesta escalables, sistemas de inteligencia de amenazas compartida entre organizaciones del sector, y marcos de evaluación de riesgos que pueden ser implementados sin requerir expertise técnico especializado.

El cuarto pilar, Implementación Sostenible, asegura que las medidas de seguridad puedan ser mantenidas a largo plazo dentro de las limitaciones presupuestarias y de recursos humanos típicas del sector. Esto incluye el aprovechamiento de recursos gratuitos y de bajo costo, la colaboración con el sector privado a través de programas de responsabilidad social corporativa, y el desarrollo de capacidades internas que reduzcan la dependencia de consultores externos.

Impacto Esperado y Sostenibilidad

La implementación de este marco integral de ciberseguridad se espera que produzca mejoras significativas en la postura de seguridad del sector de la Economía Social española.

Las métricas de éxito incluyen una reducción del 50% en incidentes de seguridad reportados entre organizaciones participantes, una mejora del 75% en puntajes de evaluación de concienciación en ciberseguridad, un aumento del 80% en la implementación de prácticas de seguridad recomendadas, y capacidades mejoradas de respuesta a incidentes que reduzcan el tiempo medio de recuperación en un 60%.

El modelo de sostenibilidad se basa en una combinación de financiación pública a través del Plan Integral de Impulso a la Economía Social 2024-2025, colaboración con el sector



www.fundacioel7.org

privado a través de programas de responsabilidad social corporativa, y el desarrollo de capacidades internas que reduzcan los costos operativos a largo plazo. La inversión inicial estimada varía según el tamaño organizacional, desde 2.500 euros anuales para organizaciones muy pequeñas hasta 50.000 euros para organizaciones grandes, con un retorno de inversión esperado que se materializa a través de la prevención de incidentes costosos y la mejora de la eficiencia operativa.

Este estudio representa una contribución significativa tanto a la literatura académica como a la práctica profesional de la ciberseguridad, proporcionando el primer análisis integral de desafíos de ciberseguridad que enfrentan específicamente las entidades de la Economía Social y las poblaciones vulnerables que atienden. Los hallazgos informan directamente el desarrollo de soluciones prácticas que pueden mejorar significativamente la seguridad digital de comunidades desatendidas mientras proporcionan un modelo para diseño de seguridad inclusiva que puede aplicarse a través de diversos contextos y poblaciones.



www.fundacioel7.org

Introducción y Marco Conceptual

Contexto y Motivación de la Investigación

La transformación digital de los servicios sociales y la creciente dependencia de la tecnología para servicios esenciales ha creado nuevas vulnerabilidades para poblaciones ya en riesgo de exclusión social. Las entidades de la Economía Social en España - incluyendo cooperativas, sociedades mutuas, asociaciones, fundaciones y empresas sociales - sirven como intermediarios críticos entre poblaciones vulnerables y servicios digitales, sin embargo estas organizaciones enfrentan desafíos únicos de ciberseguridad que los marcos de seguridad tradicionales no logran abordar adecuadamente [7].

La motivación para esta investigación emerge del reconocimiento de que la ciberseguridad no es meramente un desafío técnico sino un tema de justicia social que afecta desproporcionadamente a poblaciones vulnerables. Cuando las entidades de la Economía Social experimentan incidentes de ciberseguridad, el impacto se extiende mucho más allá de los límites organizacionales para afectar a individuos que pueden tener recursos alternativos limitados y que pueden ser particularmente vulnerables a las consecuencias de violaciones de datos, interrupciones de servicios y violaciones de privacidad [8].

Los recientes ciberataques de alto perfil en organizaciones sin fines de lucro y proveedores de servicios sociales han destacado la necesidad crítica de enfoques especializados de ciberseguridad que aborden las características y limitaciones únicas del sector de la Economía Social. El ataque de ransomware al Ministerio de Trabajo y Economía Social de España en 2021, que utilizó la variante Ryuk y obligó a interrumpir sistemas críticos, evidenció que ninguna entidad está exenta del riesgo, independientemente de su naturaleza social o benéfica [9]. Estos incidentes han demostrado que los marcos tradicionales de ciberseguridad, diseñados principalmente para empresas comerciales con recursos sustanciales y experiencia técnica, son inadecuados para organizaciones que priorizan la accesibilidad, confianza y compromiso comunitario sobre las restricciones de seguridad.

La pandemia de COVID-19 aceleró dramáticamente la digitalización del sector social, forzando a muchas organizaciones a adoptar tecnologías digitales sin la preparación o recursos adecuados para implementar medidas de seguridad apropiadas. Esta digitalización acelerada, aunque necesaria para mantener la continuidad de servicios esenciales, creó nuevas superficies de ataque y expuso vulnerabilidades previamente inexistentes. Las organizaciones que tradicionalmente operaban principalmente a través de interacciones presenciales se vieron obligadas a gestionar datos sensibles a través de plataformas digitales, a menudo sin la infraestructura de seguridad o la experiencia necesaria para hacerlo de manera segura [10].



www.fundacioel7.org

El Sector de la Economía Social: Definiciones y Características

La Economía Social abarca una gama diversa de organizaciones unidas por su compromiso con el propósito social sobre la maximización de ganancias. Según la definición establecida por la Ley 5/2011 de Economía Social de España, las entidades de la Economía Social se caracterizan por la primacía de las personas y del fin social sobre el capital, la aplicación de los resultados obtenidos de la actividad económica principalmente en función del trabajo aportado y servicio o actividad realizada por las socias y socios o por sus miembros y, en su caso, al fin social objeto de la entidad, la promoción de la solidaridad interna y con la sociedad que favorezca el compromiso con el desarrollo local, la igualdad de oportunidades entre hombres y mujeres y la cohesión social, y la independencia respecto a los poderes públicos [11].

Las cooperativas representan el componente más numeroso del sector, con cerca de 20.000 entidades que emplean directamente a 325.000 trabajadores en España. Estas empresas propiedad de miembros operan para el beneficio mutuo de sus socios, proporcionando servicios que van desde servicios financieros y vivienda hasta atención médica y educación. Las cooperativas a menudo sirven a comunidades que están desatendidas por proveedores comerciales tradicionales, convirtiéndolas en infraestructura crítica para poblaciones vulnerables.

Su estructura democrática de toma de decisiones, aunque valiosa para la participación de miembros, puede complicar la implementación rápida de medidas de ciberseguridad que requieren decisiones técnicas especializadas [12]. Las sociedades mutuas proporcionan servicios de seguros y financieros basados en principios de ayuda mutua y solidaridad, a menudo sirviendo a comunidades con acceso limitado a servicios financieros tradicionales. Estas organizaciones manejan información financiera y personal altamente sensible mientras operan con estructuras de gobernanza basadas en la comunidad que pueden carecer de experiencia especializada en ciberseguridad. La naturaleza mutua de estas organizaciones significa que una brecha de seguridad no solo afecta a la organización sino directamente a todos sus miembros, amplificando el impacto potencial de incidentes de ciberseguridad [13].

Las asociaciones abarcan una amplia gama de organizaciones sin fines de lucro que proporcionan servicios sociales, defensa y apoyo comunitario. Con más de 600.000 asociaciones registradas en España, este subsector incluye desde pequeñas organizaciones de base comunitaria hasta grandes ONG internacionales. Estas organizaciones a menudo sirven como la interfaz principal entre poblaciones vulnerables y servicios esenciales, convirtiéndolas en objetivos críticos para cibercriminales que buscan acceder a información personal o interrumpir servicios sociales. Su dependencia de voluntarios y donaciones puede limitar su capacidad para invertir en infraestructura de ciberseguridad robusta [14].

Las fundaciones proporcionan financiamiento y apoyo para causas sociales mientras a menudo mantienen extensas bases de datos de información de donantes y datos de beneficiarios de subvenciones. Estas organizaciones enfrentan desafíos únicos de



www.fundacioel7.org

ciberseguridad relacionados con proteger tanto la privacidad de donantes como la información sensible de organizaciones e individuos que apoyan. La naturaleza de su trabajo a menudo requiere el manejo de información particularmente sensible sobre poblaciones vulnerables, incluyendo datos sobre víctimas de violencia doméstica, refugiados, o individuos con problemas de salud mental [15].

Las empresas sociales combinan actividades comerciales con misiones sociales, a menudo sirviendo a poblaciones vulnerables a través de modelos innovadores de entrega de servicios. Estas organizaciones enfrentan el doble desafío de proteger información comercial mientras mantienen la accesibilidad y las relaciones de confianza esenciales para servir a comunidades marginadas. Su naturaleza híbrida puede crear complejidades adicionales en términos de cumplimiento regulatorio y gestión de riesgos [16].

Poblaciones Vulnerables y Exclusión Digital

Las poblaciones atendidas por entidades de la Economía Social enfrentan múltiples vulnerabilidades interseccionales que agravan sus riesgos de ciberseguridad. Estas vulnerabilidades se extienden más allá de características individuales para incluir factores sistémicos que crean barreras para la participación digital segura. La investigación identifica que los adultos mayores, individuos con discapacidades, inmigrantes, individuos en situación de calle, y sobrevivientes de violencia doméstica enfrentan riesgos de ciberseguridad particularmente agudos que requieren enfoques especializados de protección [17].

Los factores de brecha digital crean barreras fundamentales para la ciberseguridad para poblaciones vulnerables. El acceso limitado a conectividad confiable a internet afecta la capacidad de recibir actualizaciones de seguridad críticas y acceder a servicios en línea seguros.

Según datos del Instituto Nacional de Estadística, el 15% de los hogares españoles aún carece de acceso a internet de banda ancha, con concentraciones particularmente altas en áreas rurales y entre poblaciones de bajos ingresos [18]. La falta de acceso a dispositivos modernos significa que muchos individuos vulnerables dependen de tecnología más antigua que puede no soportar medidas de seguridad actuales, incluyendo protocolos de cifrado modernos, autenticación multifactor, o actualizaciones de seguridad regulares.

El soporte técnico limitado significa que los individuos pueden no tener acceso a asistencia cuando encuentran desafíos de seguridad o necesitan ayuda implementando medidas de seguridad. Esta limitación es particularmente problemática para poblaciones vulnerables que pueden no tener redes sociales robustas o recursos económicos para acceder a soporte técnico profesional. La dependencia de familiares o amigos para asistencia técnica puede crear vulnerabilidades adicionales si estos individuos tampoco poseen conocimientos adecuados de ciberseguridad [19].



www.fundacioel7.org

Las limitaciones económicas impactan significativamente las capacidades de ciberseguridad para poblaciones vulnerables. El costo de software y servicios de seguridad puede ser prohibitivo para individuos con recursos financieros limitados, forzándolos a depender de soluciones gratuitas que pueden ofrecer protección inferior. La necesidad de priorizar necesidades básicas como vivienda, alimentación y atención médica sobre inversiones en tecnología significa que la seguridad digital puede ser vista como un lujo en lugar de una necesidad. El acceso limitado a servicios financieros tradicionales puede requerir dependencia de sistemas financieros alternativos que pueden tener características de seguridad diferentes o menos robustas [20].

Los factores sociales y culturales influyen significativamente en cómo las poblaciones vulnerables interactúan con la tecnología y las medidas de seguridad. Las barreras idiomáticas pueden prevenir que los individuos entiendan instrucciones de seguridad o reconozcan amenazas, particularmente cuando el contenido de seguridad está disponible únicamente en el idioma mayoritario. Las diferencias culturales en expectativas de privacidad y relaciones de confianza pueden afectar la disposición a adoptar medidas de seguridad que pueden ser percibidas como intrusivas o innecesarias. El aislamiento social puede limitar el acceso a redes de apoyo informales que podrían proporcionar asistencia de seguridad y verificación de amenazas potenciales [21].

Los factores cognitivos y físicos afectan la capacidad de algunos individuos para implementar y mantener medidas de seguridad efectivas. Los deterioros cognitivos asociados con el envejecimiento, discapacidades del desarrollo, o condiciones de salud mental pueden afectar la capacidad de entender procedimientos de seguridad complejos o reconocer amenazas sofisticadas. Las discapacidades físicas pueden crear barreras para usar interfaces o dispositivos de seguridad estándar, requiriendo adaptaciones especializadas que pueden no estar ampliamente disponibles. Los cambios relacionados con la edad en capacidades cognitivas y físicas pueden afectar la toma de decisiones de seguridad y la implementación de medidas protectivas [22].

Objetivos y Alcance de la Investigación

Este estudio de investigación aborda tres objetivos primarios que corresponden a las actividades de investigación especificadas en el marco de trabajo original. El primer objetivo, es el desarrollo de una hoja de ruta estratégica integral para implementar medidas de ciberseguridad dentro de entidades de la Economía Social, con particular atención a proteger poblaciones vulnerables.

Esta hoja de ruta incluye estrategias específicas para abordar los desafíos únicos que enfrentan estas organizaciones mientras mantienen su compromiso con la accesibilidad y el servicio comunitario.

El segundo objetivo, es la conducción de una investigación sistemática de riesgos de ciberseguridad que enfrentan usuarios de entidades de la Economía Social, con enfoque



www.fundacioel7.org

particular en individuos en riesgo de exclusión social. Esta investigación identifica vulnerabilidades específicas, vectores de ataque y factores de riesgo que afectan a estas poblaciones, proporcionando una base empírica para el desarrollo de contramedidas apropiadas.

El tercer objetivo, es la definición de cursos óptimos de acción basados en los riesgos identificados, estableciendo protocolos de actuación y estrategias de mitigación aplicables al conjunto del sector de la Economía Social. Estos protocolos están específicamente diseñados para ser implementables dentro de las limitaciones de recursos típicas del sector mientras proporcionan protección efectiva contra las amenazas más prevalentes.

El alcance de la investigación abarca tanto aspectos organizacionales como individuales de la ciberseguridad en el contexto de la Economía Social. A nivel organizacional, el estudio examina las características estructurales, operacionales y culturales de las entidades de la Economía Social que influyen en su postura de ciberseguridad. A nivel individual, la investigación analiza las vulnerabilidades específicas de las poblaciones atendidas por estas organizaciones y desarrolla enfoques de protección que acomodan sus necesidades y limitaciones únicas.

La investigación adopta un enfoque multidisciplinario que integra perspectivas de ciberseguridad técnica, psicología social, trabajo social, y políticas públicas. Este enfoque holístico es necesario para abordar adecuadamente la complejidad de los desafíos de ciberseguridad en el contexto social, donde los factores técnicos, humanos y organizacionales interactúan de maneras complejas para crear patrones únicos de vulnerabilidad y resistencia.

Metodología de Investigación

La metodología empleada en este estudio integra múltiples enfoques de investigación para proporcionar una comprensión comprehensiva de los desafíos de ciberseguridad en el sector de la Economía Social. La investigación combina análisis de literatura académica y profesional, análisis de casos de estudio documentados, evaluación de marcos regulatorios y normativos, y síntesis de mejores prácticas identificadas en investigaciones previas.

El análisis de literatura abarca tanto fuentes académicas revisadas por pares como informes profesionales de organizaciones especializadas en ciberseguridad, incluyendo INCIBE, CCNCERT, y organizaciones internacionales como el FBI y la Comisión Federal de Comercio de Estados Unidos. Esta revisión proporciona una base teórica sólida y acceso a los datos más recientes sobre tendencias de amenazas y efectividad de contramedidas.

El análisis de casos de estudio examina incidentes documentados de ciberseguridad que han afectado a organizaciones del sector social, tanto en España como internacionalmente. Estos casos proporcionan insights valiosos sobre los vectores de ataque más comunes, los impactos típicos de los incidentes, y las estrategias de respuesta y recuperación que han demostrado ser efectivas en contextos similares.



www.fundacioel7.org

La evaluación del marco regulatorio examina las obligaciones legales actuales y emergentes que afectan a las entidades de la Economía Social en España, incluyendo el RGPD, el Esquema Nacional de Seguridad, y regulaciones sectoriales específicas. Esta evaluación asegura que las recomendaciones desarrolladas sean compatibles con los requisitos legales existentes y anticipen desarrollos regulatorios futuros.

La síntesis de mejores prácticas integra hallazgos de múltiples fuentes para desarrollar recomendaciones que sean tanto técnicamente sólidas como prácticamente implementables dentro de las limitaciones típicas del sector de la Economía Social. Este proceso de síntesis incluye la evaluación de la aplicabilidad de prácticas desarrolladas en otros sectores y la adaptación de estas prácticas para abordar las características únicas del contexto social.



www.fundacioel7.org

Contexto Normativo y Regulatorio Español

Marco Regulatorio Actualizado para 2025

El ecosistema regulatorio para entidades de Economía Social en España se ha intensificado significativamente en los últimos años, creando un entorno normativo complejo que requiere comprensión especializada para asegurar el cumplimiento efectivo. El Reglamento General de Protección de Datos (RGPD) se aplica plenamente a cooperativas, mutualidades, fundaciones y asociaciones, pero con matices críticos específicos para este sector que deben ser cuidadosamente considerados en cualquier estrategia de ciberseguridad [23].

Las entidades que atienden colectivos vulnerables enfrentan obligaciones particularmente estrictas bajo el RGPD debido a la naturaleza sensible de los datos que procesan. Estas organizaciones deben realizar Evaluaciones de Impacto en la Protección de Datos (EIPD) obligatorias cuando procesen categorías especiales de datos, que incluyen información sobre salud física o mental, origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, datos sobre vida sexual u orientación sexual, y datos relativos a condenas e infracciones penales [24]. Para muchas entidades de Economía Social, especialmente aquellas que proporcionan servicios de salud, apoyo social, o asistencia legal, el procesamiento de estas categorías de datos es inherente a su misión, requiriendo la implementación de salvaguardas técnicas y organizativas reforzadas.

Las medidas de seguridad reforzadas requeridas incluyen el cifrado AES-256 para todos los datos sensibles tanto en reposo como en tránsito, la implementación de control de acceso basado en roles que limite el acceso a información sensible únicamente al personal autorizado y necesario para el cumplimiento de funciones específicas, y la adopción de principios de minimización de datos que aseguren que solo se recopile y procese la información estrictamente necesaria para los fines declarados [25]. Adicionalmente, estas organizaciones deben adaptar sus procesos de consentimiento informado para acomodar diferentes capacidades de comprensión, incluyendo el desarrollo de materiales en Lectura Fácil para personas con discapacidades cognitivas, la provisión de información en múltiples formatos (visual, auditivo, táctil) para personas con discapacidades sensoriales, y la implementación de procedimientos especiales para obtener consentimiento de personas bajo tutela o curatela [26].

El Esquema Nacional de Seguridad (ENS), actualizado mediante el Real Decreto 311/2022, establece un marco de aplicación diferenciada que reconoce las características únicas del sector de la Economía Social [27]. Mientras que el ENS es obligatorio para entidades públicas de economía social, como ciertas cooperativas de servicios públicos o fundaciones con participación pública significativa, es altamente recomendado para organizaciones privadas que manejen datos sensibles o de alto riesgo. La normativa introduce "perfiles de cumplimiento específicos" que permiten adaptar los controles de seguridad al tamaño y recursos de la organización, reconociendo que una cooperativa agraria de 10 miembros

15/72



www.fundacioel7.org

no puede implementar las mismas medidas que una gran fundación con cientos de empleados.

Los perfiles de cumplimiento del ENS se estructuran en tres niveles: Básico, Medio y Alto, con criterios de aplicación que consideran tanto el valor de la información manejada como el impacto potencial de su compromiso. Para entidades de Economía Social, el nivel Básico es apropiado para organizaciones pequeñas que manejan información personal estándar sin categorías especiales de datos. El nivel Medio se aplica a organizaciones que procesan datos sensibles o que proporcionan servicios críticos a poblaciones vulnerables. El nivel Alto se reserva para organizaciones que manejan información de seguridad nacional o que proporcionan infraestructura crítica [28].

Actualizaciones Normativas Relevantes para 2025

Las actualizaciones más relevantes para el sector incluyen la transposición de la Directiva NIS2 al ordenamiento jurídico español, que amplía significativamente el alcance de las obligaciones de ciberseguridad a más sectores y tipos de organizaciones. Aunque la mayoría de entidades de Economía Social no caerán bajo el ámbito directo de NIS2, aquellas que proporcionen servicios esenciales como atención sanitaria, servicios sociales críticos, o infraestructura digital pueden verse afectadas por las nuevas obligaciones [29]. La directiva introduce requisitos específicos para la gestión de riesgos de ciberseguridad, incluyendo la adopción de medidas técnicas y organizativas apropiadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información, la adopción de medidas apropiadas para prevenir y minimizar el impacto de incidentes, y la notificación de incidentes significativos a las autoridades competentes.

El Reglamento de Ciberresiliencia de la Unión Europea, que entrará en vigor progresivamente hasta 2027, impactará en entidades que utilicen productos con elementos digitales, incluyendo software, hardware, y dispositivos IoT [30]. Para las entidades de Economía Social, esto significa que deberán asegurar que cualquier tecnología que adquieran cumpla con los nuevos requisitos de ciberseguridad, incluyendo la implementación de medidas de seguridad por diseño y por defecto, la provisión de actualizaciones de seguridad durante todo el ciclo de vida del producto, y la documentación adecuada de vulnerabilidades y medidas de mitigación.

El Plan Integral de Impulso a la Economía Social 2024-2025, con un presupuesto de 39,2 millones de euros, incluye específicamente proyectos de transiciones digitales sostenibles que pueden proporcionar financiación para iniciativas de ciberseguridad [31]. Este plan reconoce explícitamente que la digitalización del sector debe ir acompañada de medidas de seguridad apropiadas, y establece líneas de financiación específicas para proyectos que combinen innovación digital con protección de datos y ciberseguridad. Las entidades pueden acceder a subvenciones de hasta 50.000 euros para proyectos de digitalización que incluyan componentes significativos de ciberseguridad.

Protecciones Especiales para Usuarios Vulnerables

La normativa española establece protecciones especiales para usuarios vulnerables que van más allá de los requisitos estándar del RGPD, reconociendo que ciertas poblaciones requieren salvaguardas adicionales debido a su mayor susceptibilidad a daños derivados del procesamiento inadecuado de datos personales [32]. Estas protecciones incluyen requisitos de comunicación adaptada que obligan a las organizaciones a proporcionar información sobre el procesamiento de datos en formatos accesibles y comprensibles para personas con diferentes capacidades cognitivas, sensoriales y educativas.

Los procedimientos especiales para situaciones de urgencia reconocen que las poblaciones vulnerables pueden enfrentar circunstancias donde la protección inmediata de su seguridad física puede requerir el procesamiento rápido de datos personales sin el consentimiento previo completo. Estos procedimientos establecen marcos legales claros para el procesamiento de datos en situaciones de emergencia, incluyendo casos de violencia doméstica, crisis de salud mental, o situaciones de desamparo, mientras mantienen salvaguardas apropiadas para prevenir el abuso de estas excepciones [33].

Los protocolos específicos para la comunicación con familiares y cuidadores abordan las complejidades que surgen cuando las personas vulnerables requieren asistencia de terceros para gestionar sus asuntos digitales. Estos protocolos establecen procedimientos claros para verificar la autorización de familiares o cuidadores para actuar en nombre de la persona vulnerable, incluyendo la documentación requerida, los límites de la autorización, y los procedimientos para revocar o modificar permisos [34].

Obligaciones de Notificación y Transparencia

Las obligaciones de notificación bajo el RGPD se adaptan para reconocer las características específicas de las entidades de Economía Social, pero no eximen del cumplimiento normativo.

Las organizaciones deben notificar violaciones de datos personales a la Agencia Española de Protección de Datos (AEPD) dentro de 72 horas de tomar conocimiento de la violación, utilizando el formulario electrónico específico disponible en la sede electrónica de la AEPD [35]. Para entidades que atienden poblaciones vulnerables, esta notificación debe incluir información específica sobre el tipo de datos comprometidos, el número y características de las personas afectadas, y las medidas específicas adoptadas para mitigar el impacto en poblaciones vulnerables.

La comunicación a los interesados debe realizarse sin dilación indebida cuando la violación de datos personales sea susceptible de entrañar un alto riesgo para los derechos y libertades de las personas físicas. Para poblaciones vulnerables, este umbral de "alto riesgo" se considera más bajo debido a su mayor susceptibilidad a daños derivados de violaciones de privacidad [36]. Las comunicaciones deben adaptarse a las capacidades de comprensión de los afectados, utilizando lenguaje claro y sencillo, proporcionando



www.fundacioel7.org

información en múltiples formatos cuando sea necesario, y ofreciendo canales de comunicación alternativos para personas que puedan tener dificultades para acceder a comunicaciones digitales estándar.

Régimen Sancionador Adaptado

Las sanciones del RGPD se adaptan considerando la naturaleza social de las entidades, pero esto no exime del cumplimiento normativo. La AEPD ha desarrollado criterios específicos para la imposición de sanciones a entidades de Economía Social que consideran factores como la naturaleza no lucrativa de la organización, los recursos limitados disponibles para cumplimiento, y el impacto social positivo de las actividades de la organización [37]. Sin embargo, estos factores atenuantes no eliminan la responsabilidad de cumplir con las obligaciones de protección de datos, especialmente cuando se trata de proteger poblaciones vulnerables.

Los criterios de graduación de sanciones incluyen la evaluación de la intencionalidad o negligencia en la infracción, considerando que las entidades de Economía Social pueden carecer de recursos para expertise especializado en protección de datos. La cooperación con la autoridad de control durante la investigación de infracciones puede resultar en reducciones significativas de sanciones, especialmente cuando las organizaciones demuestran esfuerzos de buena fe para remediar las deficiencias identificadas [38].

Las medidas correctivas pueden incluir la imposición de obligaciones de formación específica para el personal, la implementación de medidas técnicas y organizativas específicas, o la designación de un Delegado de Protección de Datos externo cuando la organización no tenga recursos para mantener esta función internamente. Estas medidas correctivas están diseñadas para ser constructivas y educativas, ayudando a las organizaciones a desarrollar capacidades de cumplimiento sostenibles en lugar de simplemente imponer cargas punitivas [39].

Colaboración con Autoridades Competentes

El marco regulatorio español facilita la colaboración entre entidades de Economía Social y autoridades competentes para mejorar la ciberseguridad sectorial. INCIBE proporciona servicios especializados para organizaciones sin fines de lucro, incluyendo evaluaciones gratuitas de ciberseguridad, formación especializada, y acceso a herramientas de seguridad desarrolladas específicamente para organizaciones con recursos limitados [40]. Estos servicios reconocen que las entidades de Economía Social pueden no tener acceso a los mismos recursos que las empresas comerciales, pero enfrentan amenazas similares o incluso mayores debido a la naturaleza sensible de los datos que manejan.

La colaboración con las Fuerzas y Cuerpos de Seguridad del Estado se facilita a través de protocolos específicos que reconocen las características únicas del sector social. La Guardia



www.fundacioel7.org

Civil y la Policía Nacional han desarrollado unidades especializadas en ciberdelincuencia que incluyen expertise específico en amenazas dirigidas a organizaciones sociales y poblaciones vulnerables [41]. Estas unidades proporcionan servicios de investigación especializada, formación preventiva, y apoyo en la respuesta a incidentes que están adaptados a las necesidades y limitaciones del sector.

El CCN-CERT proporciona servicios de inteligencia de amenazas y respuesta a incidentes que están disponibles para entidades de Economía Social que manejen información clasificada o que proporcionen servicios críticos. Aunque la mayoría de organizaciones del sector no manejan información clasificada, aquellas que colaboran con administraciones públicas o que proporcionan servicios esenciales pueden beneficiarse de estos servicios especializados [42].



www.fundacioel7.org

Panorama de Ciberseguridad en la Economía Social

Estadísticas de Ciberataques en el Sector

El sector de la Economía Social en España enfrenta un panorama de amenazas cibernéticas cada vez más sofisticado y dirigido. Los datos más recientes de INCIBE revelan que se recibieron más de 83.000 incidentes informáticos en 2024, representando un incremento del 24% respecto al año anterior [43]. Esta tendencia ascendente es particularmente preocupante para las entidades de Economía Social, que tradicionalmente han operado con niveles de ciberseguridad inferiores a los de empresas comerciales equivalentes.

A nivel internacional, las organizaciones sin fines de lucro se han convertido en el segundo sector más atacado por cibercriminales, representando el 31% de todas las notificaciones de ataques de estados-nación según el informe anual de Microsoft sobre amenazas digitales [44]. Esta estadística cobra especial relevancia cuando se considera que las organizaciones sin fines de lucro constituyen una fracción mucho menor de la economía total que sectores como el financiero o el tecnológico, sugiriendo que están siendo desproporcionadamente dirigidas por actores maliciosos.

En el contexto español específico, el 27% de las ONG a nivel mundial han sufrido un ciberataque según informes sectoriales recientes, mientras que el 60% de las empresas españolas afirman recibir un mayor número de ciberataques en 2023, siendo estos un 80% más críticos y provocando más daños que en años anteriores [45]. Para las entidades de Economía Social, que invierten un 42% menos en ciberseguridad que las empresas tradicionales mientras manejan información de poblaciones vulnerables, estos riesgos se amplifican exponencialmente.

Las pérdidas económicas asociadas con ciberataques en el sector son devastadoras. El costo medio de un ataque para pequeñas y medianas empresas españolas alcanza los 35.000 euros, con una tasa de cierre del 60% en los seis meses posteriores al ataque [46]. Para las entidades de Economía Social, que operan con márgenes ajustados y dependen de subvenciones públicas y donaciones privadas, estos costos pueden ser existenciales, amenazando no solo la viabilidad financiera de la organización sino también la continuidad de servicios esenciales para poblaciones vulnerables.

Tipos de Entidades y Vulnerabilidades Específicas

Las cooperativas, con cerca de 20.000 entidades que emplean directamente a 325.000 trabajadores, enfrentan vulnerabilidades específicas derivadas de la digitalización acelerada post-COVID implementada sin medidas de seguridad adecuadas [47]. Su heterogeneidad tecnológica, desde pequeñas cooperativas agrarias con infraestructura IT básica hasta organizaciones tecnológicas con miles de trabajadores, genera diferentes niveles de madurez digital y capacidad de respuesta ante amenazas cibernéticas.



www.fundacioel7.org

Las cooperativas agrarias y de servicios rurales enfrentan desafíos particulares debido a su ubicación geográfica, que a menudo limita el acceso a servicios de internet de alta velocidad y soporte técnico especializado. Estas organizaciones frecuentemente dependen de conexiones satelitales o de banda ancha rural que pueden ser menos seguras y más susceptibles a interrupciones. Adicionalmente, la naturaleza estacional de muchas actividades agrarias puede crear períodos de alta vulnerabilidad cuando los sistemas deben procesar grandes volúmenes de datos financieros y de producción en ventanas de tiempo limitadas [48].

Las cooperativas de crédito y servicios financieros enfrentan riesgos amplificados debido a su manejo de información financiera sensible y su papel como alternativa a la banca tradicional para comunidades desatendidas. Estas organizaciones son objetivos particularmente atractivos para cibercriminales debido a la combinación de activos financieros accesibles y medidas de seguridad frecuentemente menos robustas que las de bancos comerciales. Un ataque exitoso contra una cooperativa de crédito puede tener impactos devastadores no solo en la organización sino en toda la comunidad que depende de sus servicios [49].

Las fundaciones y asociaciones constituyen el segmento más vulnerable a ataques de defacement contra páginas web y cuentas de redes sociales, así como a ransomware dirigido que aprovecha su gestión de datos de donantes y beneficiarios. Un caso documentado por Fundación Lealtad ilustra estos riesgos: una ONG española sufrió un ataque de ransomware con demanda de rescate en bitcoins, requiriendo un mes de recuperación utilizando copias de seguridad múltiples [50]. Este caso destaca tanto la vulnerabilidad del sector como la importancia crítica de medidas de preparación y respuesta adecuadas.

Las asociaciones de servicios sociales enfrentan riesgos particulares debido a la naturaleza altamente sensible de los datos que manejan, incluyendo información sobre víctimas de violencia doméstica, personas sin hogar, individuos con problemas de salud mental, y otros colectivos vulnerables. Una brecha de datos en estas organizaciones puede tener consecuencias que van más allá del daño financiero para incluir riesgos físicos reales para las personas cuyos datos son comprometidos [51].

Las mutualidades y centros especiales de empleo enfrentan riesgos amplificados por su gestión de datos sensibles de salud y la dependencia tecnológica crítica, donde la interrupción de servicios afecta directamente a usuarios vulnerables que dependen de sus servicios esenciales.

Estas organizaciones a menudo operan sistemas heredados que fueron diseñados para funcionalidad específica sin consideraciones robustas de ciberseguridad, creando vulnerabilidades que pueden ser difíciles de remediar sin interrumpir servicios críticos [52].



www.fundacioel7.org

Limitaciones de Recursos y Capacidades

Las entidades de la Economía Social enfrentan limitaciones significativas de recursos que afectan fundamentalmente su capacidad para implementar y mantener medidas efectivas de ciberseguridad. La investigación del Consejo Nacional de Organizaciones Sin Fines de Lucro encuentra que el 73% de organizaciones sin fines de lucro reportan que las inversiones en ciberseguridad compiten directamente con el financiamiento de programas de misión [53]. Esta competencia crea un dilema ético donde las organizaciones deben elegir entre servir a sus comunidades y proteger sus sistemas, una elección que es particularmente difícil para organizaciones comprometidas con maximizar su impacto social.

El presupuesto promedio de ciberseguridad para organizaciones sin fines de lucro es significativamente menor que para empresas comerciales de tamaño similar. La Evaluación de Seguridad de Tecnología Sin Fines de Lucro encuentra que las organizaciones sin fines de lucro gastan un promedio de 2.300 euros por año en ciberseguridad, comparado con 15.000 euros para empresas comerciales de tamaño similar [54]. Esta disparidad en inversión se traduce directamente en diferencias en la robustez de las medidas de seguridad implementadas, creando vulnerabilidades sistémicas en el sector.

La brecha de experiencia en ciberseguridad dentro del sector de la Economía Social es particularmente pronunciada. Solo el 23% de juntas directivas de organizaciones sin fines de lucro incluyen miembros con experiencia en ciberseguridad, comparado con el 67% de juntas corporativas [55]. Esta brecha de experiencia se extiende a través de todos los niveles de las organizaciones, con solo el 12% de organizaciones sin fines de lucro empleando personal dedicado a ciberseguridad, y muchas organizaciones dependiendo de personal de TI de propósito general o voluntarios para manejar responsabilidades de ciberseguridad.

La dependencia de personal no especializado puede llevar a implementación inconsistente de medidas de seguridad y respuesta inadecuada a incidentes de seguridad. Los voluntarios, aunque valiosos para las operaciones organizacionales, pueden carecer de la formación continua y la responsabilidad profesional necesarias para mantener estándares de ciberseguridad apropiados. Esta situación se complica por la alta rotación típica del personal voluntario, que puede resultar en pérdida de conocimiento institucional y inconsistencias en la implementación de políticas de seguridad [56].

Desafíos de Infraestructura Tecnológica

Muchas entidades de la Economía Social operan con infraestructura tecnológica desactualizada que puede no soportar medidas de ciberseguridad modernas. El 45% de organizaciones sin fines de lucro usan sistemas operativos que ya no reciben actualizaciones de seguridad, y el 38% usan software que no es compatible con herramientas de seguridad modernas [57]. Esta dependencia de sistemas heredados crea vulnerabilidades fundamentales que pueden ser difíciles y costosas de remediar.

22/72



www.fundacioel7.org

Los desafíos de infraestructura son exacerbados por ciclos de reemplazo de tecnología más largos en organizaciones sin fines de lucro, que pueden no tener los recursos para actualizar sistemas regularmente. La dependencia de donaciones de tecnología, aunque valiosa para reducir costos, puede también resultar en infraestructura inconsistente que es difícil de asegurar y mantener. Los equipos donados pueden ser de diferentes fabricantes, ejecutar diferentes versiones de software, y tener diferentes capacidades de seguridad, creando un entorno heterogéneo que es inherentemente más difícil de proteger [58].

La adopción de soluciones de nube por parte de entidades de Economía Social ha creado entornos híbridos complejos que presentan desafíos únicos de ciberseguridad. El 67% de organizaciones sin fines de lucro operan entornos de nube híbrida, combinando sistemas locales heredados con servicios de nube modernos [59]. Estos entornos híbridos crean complejidades en gestión de identidad y acceso a través de múltiples plataformas, desafíos en mantener visibilidad de seguridad consistente, dificultad en implementar políticas de seguridad coherentes, y complejidad en respuesta a incidentes que pueden abarcar múltiples entornos tecnológicos.

Casos Reales Documentados

El análisis de casos reales proporciona insights valiosos sobre los patrones de ataque y las vulnerabilidades específicas del sector. El ataque al Hospital Clínic Barcelona en marzo de 2023 ilustra cómo el ransomware sofisticado puede paralizar operaciones críticas durante varios días, afectando no solo a la organización sino a todos los pacientes que dependen de sus servicios [60]. Aunque el Hospital Clínic no es estrictamente una entidad de Economía Social, su misión de servicio público y su dependencia de sistemas digitales para proporcionar servicios esenciales lo convierten en un caso de estudio relevante para el sector.

El ataque de ransomware al Ayuntamiento de Sevilla en septiembre de 2023 demostró cómo estos incidentes pueden dejar sin restituir completamente la administración electrónica, afectando servicios a ciudadanos vulnerables que dependen de servicios digitales para acceder a prestaciones sociales [61]. Este caso destaca la importancia de planes de continuidad de negocio robustos y la necesidad de mantener canales alternativos de servicio para poblaciones que pueden no tener opciones alternativas.

Un caso particularmente relevante para el sector de la Economía Social es el ataque documentado por Fundación Lealtad, donde una ONG española sufrió ransomware que cifró completamente su servidor principal mientras los atacantes exigían un rescate en bitcoins. La organización decidió no pagar el rescate y denunció el hecho a la Guardia Civil. Gracias a copias de seguridad mantenidas en la nube, correos electrónicos archivados, y archivos en papel, la organización pudo reanudar sus operaciones tras un mes de trabajo intensivo [62]. Este caso ilustra tanto la vulnerabilidad del sector como la importancia de medidas de preparación adecuadas.



www.fundacioel7.org

Impacto en Poblaciones Vulnerables

Los incidentes de ciberseguridad en entidades de Economía Social tienen impactos que se extienden mucho más allá de las organizaciones afectadas para impactar directamente en las poblaciones vulnerables que dependen de sus servicios. La interrupción de servicios puede tener consecuencias particularmente severas para individuos que pueden no tener opciones alternativas o recursos para acceder a servicios equivalentes durante el período de recuperación.

Un ataque de ransomware en una organización que proporciona servicios de vivienda puede prevenir que individuos sin hogar accedan a refugio durante condiciones climáticas peligrosas. Una violación de datos en una organización de servicios de salud mental puede interrumpir el tratamiento para individuos con condiciones graves que requieren continuidad de cuidado. Una brecha de seguridad en una organización que sirve a víctimas de violencia doméstica puede exponer información de ubicación que pone en riesgo físico real a las personas protegidas [63].

La pérdida de confianza comunitaria resultante de incidentes de ciberseguridad puede tener efectos duraderos en la efectividad de las organizaciones sociales. Las poblaciones vulnerables pueden ser particularmente sensibles a violaciones de privacidad y pueden ser reacias a participar en servicios después de incidentes de ciberseguridad, incluso después de que los problemas técnicos hayan sido resueltos. Esta pérdida de confianza puede resultar en individuos que evitan buscar servicios esenciales, exacerbando su vulnerabilidad y aislamiento social [64].

Tendencias Emergentes de Amenazas

El panorama de amenazas para el sector de la Economía Social está evolucionando rápidamente, con cibercriminales desarrollando tácticas cada vez más sofisticadas dirigidas específicamente a organizaciones sociales y las poblaciones que atienden. Los ataques de ingeniería social están volviéndose más dirigidos y personalizados, aprovechando información disponible públicamente sobre las organizaciones y sus beneficiarios para crear campañas de phishing altamente convincentes.

Los ataques de cadena de suministro están emergiendo como una amenaza significativa, donde los cibercriminales comprometen proveedores de servicios tecnológicos utilizados por múltiples organizaciones del sector para ganar acceso a una amplia gama de objetivos. Estos ataques son particularmente preocupantes para entidades de Economía Social que pueden depender de proveedores especializados que sirven específicamente al sector sin fines de lucro [65].

La monetización de datos de poblaciones vulnerables en mercados clandestinos está creando incentivos económicos específicos para dirigirse a organizaciones sociales. Los datos sobre individuos en situaciones vulnerables pueden ser particularmente valiosos para



www.fundacioel7.org

cibercriminales que buscan perpetrar fraudes dirigidos o extorsión, creando un ciclo donde las poblaciones más vulnerables se convierten en objetivos más atractivos [66].

La creciente sofisticación de ataques de ransomware dirigidos específicamente a organizaciones que proporcionan servicios esenciales refleja una comprensión por parte de los cibercriminales de que estas organizaciones pueden estar más dispuestas a pagar rescates para restaurar servicios rápidamente. Esta tendencia es particularmente preocupante para entidades de Economía Social que pueden enfrentar presión ética para restaurar servicios para poblaciones vulnerables independientemente del costo [67].



www.fundacioel7.org

Hoja de Ruta de Blindaje Cibernético

Marco Estratégico Integral

La hoja de ruta de ciberseguridad para entidades de la Economía Social debe abordar las características únicas del sector mientras proporcionando protección efectiva contra las amenazas más prevalentes. Este marco estratégico se construye sobre cuatro pilares fundamentales que reconocen tanto las limitaciones como las fortalezas inherentes del sector social: Diseño de Seguridad Inclusiva, Protección Centrada en la Comunidad, Gestión Adaptativa de Riesgos, e Implementación Sostenible [68].

El Diseño de Seguridad Inclusiva reconoce que las medidas de ciberseguridad tradicionales, diseñadas para entornos corporativos homogéneos, pueden crear barreras inadvertidas para poblaciones vulnerables. Este pilar requiere el desarrollo de soluciones que acomoden diversas capacidades cognitivas, sensoriales y tecnológicas, asegurando que la seguridad no se logre a expensas de la accesibilidad. Esto incluye la implementación de interfaces multimodales que proporcionen opciones visuales, auditivas y táctiles, procedimientos de autenticación adaptativa que puedan acomodar diferentes capacidades y limitaciones, y contenido educativo culturalmente apropiado que resuene con comunidades diversas [69].

La Protección Centrada en la Comunidad aprovecha las redes sociales existentes y las relaciones de confianza que son características distintivas del sector de la Economía Social. A diferencia de las empresas comerciales que pueden depender principalmente de medidas técnicas, las entidades sociales poseen activos únicos en forma de relaciones comunitarias profundas que pueden ser aprovechadas para crear sistemas de seguridad colectiva. Esto incluye el desarrollo de redes de verificación comunitaria donde los miembros de la comunidad pueden ayudar a validar comunicaciones sospechosas, sistemas de alerta temprana que aprovechen las redes sociales existentes para difundir información sobre amenazas emergentes, y programas de educación peer-to-peer que sean más efectivos que los enfoques tradicionales de arriba hacia abajo [70].

La Gestión Adaptativa de Riesgos reconoce que las amenazas cibernéticas evolucionan constantemente y que las organizaciones con recursos limitados necesitan sistemas que puedan adaptarse rápidamente a nuevas circunstancias sin requerir inversiones masivas en nueva infraestructura o expertise especializado. Este pilar enfatiza el desarrollo de capacidades de respuesta escalables, la participación en redes de intercambio de inteligencia de amenazas específicas del sector, y la implementación de marcos de evaluación de riesgos que puedan ser utilizados por personal no técnico [71].

La Implementación Sostenible asegura que las medidas de seguridad puedan ser mantenidas a largo plazo dentro de las limitaciones presupuestarias y de recursos humanos típicas del sector.

Esto incluye el aprovechamiento máximo de recursos gratuitos y de bajo costo, el desarrollo de colaboraciones estratégicas con el sector privado a través de programas de



www.fundacioel7.org

responsabilidad social corporativa, y la construcción de capacidades internas que reduzcan la dependencia de consultores externos costosos [72].

Gobernanza y Cultura de Ciberseguridad

Un componente fundamental de la hoja de ruta es la integración de la ciberseguridad en la estrategia organizativa y en la cultura interna de las entidades de Economía Social. Los expertos recomiendan "sacar este tema del departamento de informática y llevarlo al patronato o junta directiva" de la entidad, de modo que se aborde con la importancia que merece como riesgo estratégico [73]. Esta elevación de la ciberseguridad al nivel de gobernanza superior es particularmente crítica en el sector social, donde las decisiones de seguridad pueden tener implicaciones directas para la seguridad física y el bienestar de poblaciones vulnerables.

La dirección de estas entidades debe liderar y apoyar activamente las iniciativas de seguridad, asignando recursos de forma prioritaria no solo en términos de presupuesto sino también de tiempo y atención organizacional. La Plataforma de ONG de Acción Social destaca "la importancia de identificar el riesgo de la ciberseguridad como un riesgo estratégico relacionado con la actividad de las organizaciones, pero también con los derechos de las personas a las que se atiende" [74]. Esta perspectiva de derechos humanos eleva la ciberseguridad más allá de una consideración técnica para convertirla en una obligación ética fundamental.

La designación de roles específicos de ciberseguridad debe adaptarse al tamaño y recursos de cada organización. Para organizaciones pequeñas, esto puede significar la designación de un Responsable de Seguridad que combine esta función con otras responsabilidades, mientras que organizaciones más grandes pueden requerir roles más especializados incluyendo un Administrador de Seguridad técnico y un Responsable de Protección de Datos dedicado.

Independientemente del tamaño, todas las organizaciones deben designar claramente quién es responsable de la toma de decisiones de seguridad y asegurar que esta persona tenga la autoridad y los recursos necesarios para implementar medidas efectivas [75]. El desarrollo de una cultura de ciberseguridad requiere la integración de consideraciones de seguridad en todos los aspectos de las operaciones organizacionales. Esto incluye la incorporación de evaluaciones de seguridad en procesos de toma de decisiones sobre nuevas tecnologías, la inclusión de formación en ciberseguridad en programas de orientación para nuevo personal y voluntarios, y el establecimiento de canales de comunicación claros para reportar incidentes o preocupaciones de seguridad sin temor a repercusiones [76].

Medidas Técnicas Prioritarias

La selección e implementación de medidas técnicas debe basarse en una evaluación cuidadosa de la relación costo-beneficio, considerando tanto la efectividad de seguridad

27/72



www.fundacioel7.org

como la facilidad de implementación y mantenimiento. Las medidas técnicas prioritarias para entidades de Economía Social incluyen aquellas que proporcionan la máxima protección relativa a su complejidad y costo de implementación.

Gestión de Identidad y Acceso

La implementación de sistemas robustos de gestión de identidad y acceso es fundamental para proteger información sensible mientras manteniendo la accesibilidad necesaria para operaciones efectivas. Esto incluye la implementación de principios de privilegio mínimo, donde cada usuario tiene acceso únicamente a los recursos necesarios para cumplir sus funciones específicas. Para entidades de Economía Social, esto debe equilibrarse cuidadosamente con la necesidad de flexibilidad operacional y la naturaleza colaborativa típica del sector [93].

La autenticación multifactor adaptativa debe implementarse de manera que acomode las diversas capacidades y limitaciones de usuarios en el sector social. Esto incluye opciones de autenticación que van desde SMS y llamadas telefónicas para usuarios con limitada alfabetización digital, hasta aplicaciones móviles y tokens físicos para usuarios más avanzados. La implementación debe incluir procedimientos de respaldo para situaciones donde los métodos primarios de autenticación no están disponibles [94].

Los sistemas de gestión de contraseñas deben implementarse a nivel organizacional para asegurar que todas las cuentas utilicen contraseñas únicas y complejas. Para organizaciones que atienden poblaciones vulnerables, esto puede incluir la gestión de contraseñas para cuentas de usuarios que pueden no tener la capacidad o recursos para gestionar sus propias credenciales de manera segura [95].

Protección de Datos y Cifrado

La implementación de cifrado robusto para datos sensibles es esencial para cumplir con obligaciones regulatorias y proteger la privacidad de poblaciones vulnerables. Esto incluye el cifrado de datos en reposo utilizando estándares como AES-256, el cifrado de datos en tránsito utilizando protocolos como TLS 1.3, y la implementación de gestión de claves apropiada que asegure que las claves de cifrado estén protegidas adecuadamente [96].

Los sistemas de clasificación de datos deben implementarse para asegurar que diferentes tipos de información reciban niveles apropiados de protección. Para entidades de Economía Social, esto típicamente incluye categorías como información pública, información interna, información confidencial (como datos de donantes), e información altamente sensible (como datos de beneficiarios vulnerables). Cada categoría debe tener controles de acceso y protección apropiados [97].

La implementación de sistemas de prevención de pérdida de datos (DLP) puede ayudar a prevenir la divulgación accidental o maliciosa de información sensible. Para organizaciones más pequeñas, esto puede implementarse utilizando características básicas de DLP



www.fundacioel7.org

disponibles en suites de productividad como Microsoft 365 o Google Workspace, mientras que organizaciones más grandes pueden requerir soluciones más sofisticadas [98].

Copias de Seguridad y Recuperación

La implementación de sistemas robustos de copias de seguridad y recuperación es crítica para asegurar la continuidad de servicios esenciales. La estrategia 3-2-1 (tres copias de datos, en dos tipos diferentes de medios, con una copia fuera del sitio) debe adaptarse a las capacidades y recursos de cada organización. Para organizaciones pequeñas, esto puede implementarse utilizando una combinación de almacenamiento local y servicios de nube, mientras que organizaciones más grandes pueden requerir soluciones más sofisticadas [99].

Las copias de seguridad deben probarse regularmente para asegurar que puedan restaurarse exitosamente cuando sea necesario. Esto incluye pruebas tanto de la integridad técnica de las copias como de los procedimientos organizacionales para realizar restauraciones. Las pruebas deben documentarse y cualquier problema identificado debe remediarse inmediatamente [100].

Los procedimientos de recuperación ante desastres deben abordar específicamente las necesidades únicas de entidades de Economía Social, incluyendo la necesidad de mantener servicios esenciales para poblaciones vulnerables durante el proceso de recuperación. Esto puede incluir acuerdos con otras organizaciones para proporcionar servicios de respaldo, procedimientos para operaciones manuales temporales, y planes de comunicación para mantener informados a beneficiarios durante interrupciones [101].

Estrategias Diferenciadas por Recursos

Reconociendo la diversidad significativa en tamaño, recursos y capacidades dentro del sector de la Economía Social, la hoja de ruta debe proporcionar orientación específica adaptada a diferentes niveles de recursos organizacionales. Esta diferenciación permite que organizaciones de todos los tamaños implementen medidas de seguridad apropiadas sin ser abrumadas por requisitos que excedan sus capacidades.

Organizaciones de Recursos Muy Limitados

Las organizaciones con menos de 10 empleados y presupuestos de TI inferiores a 5.000 euros anuales deben enfocarse en medidas básicas obligatorias que proporcionen protección fundamental con mínima complejidad operacional. Esto incluye la implementación de un gestor de contraseñas corporativo gratuito o de bajo costo, backup automatizado en servicios de nube con cifrado incluido, antivirus empresarial con licencias gratuitas para organizaciones sin fines de lucro, actualizaciones automáticas habilitadas en todos los sistemas, autenticación multifactor en cuentas críticas, formación básica gratuita de INCIBE, y segmentación básica de WiFi empresarial [102].

Estas organizaciones deben aprovechar al máximo los recursos gratuitos disponibles, incluyendo las herramientas de evaluación de ciberseguridad de INCIBE, los materiales



www.fundacioel7.org

de formación gratuitos disponibles a través de programas gubernamentales, y las licencias de software donadas a través de programas como Microsoft para Organizaciones Sin Fines de Lucro y Google para Organizaciones Sin Fines de Lucro [103].

Organizaciones de Recursos Limitados

Las organizaciones con 10-50 empleados y presupuestos de 5.000-25.000 euros anuales pueden implementar medidas adicionales que proporcionen protección más robusta. Esto incluye la adición de EDR (Endpoint Detection and Response) básico, backup híbrido local y en nube con cifrado, gestión de dispositivos mediante soluciones como Microsoft Intune, monitorización de seguridad con Azure Sentinel básico, formación estructurada con simulaciones de phishing, auditoría externa anual, y plan documentado de respuesta a incidentes [104].

Estas organizaciones pueden comenzar a desarrollar capacidades internas más especializadas, incluyendo la designación de personal con responsabilidades específicas de ciberseguridad y la implementación de procesos más formales de gestión de riesgos [105].

Organizaciones de Recursos Medios

Las organizaciones con 50-200 empleados y presupuestos de 25.000-100.000 euros anuales pueden implementar medidas más sofisticadas que se aproximen a las mejores prácticas corporativas. Esto incluye SIEM/SOAR para correlación de eventos, implementación gradual de arquitectura Zero Trust, DLP para prevención de fuga de datos, pentesting anual profesional, SOC externo 24/7, certificación ENS Media, y gestión continua de vulnerabilidades [106].

Estas organizaciones pueden comenzar a liderar el desarrollo de mejores prácticas sectoriales y proporcionar recursos y orientación a organizaciones más pequeñas en sus redes [107].

Organizaciones Grandes

Las organizaciones con más de 200 empleados y presupuestos superiores a 100.000 euros anuales pueden implementar capacidades de ciberseguridad que rivalicen con las de grandes corporaciones. Esto incluye el desarrollo de SOC interno, threat intelligence contextualizada, ejercicios de Red Team, CASB para seguridad de nube avanzada, certificación ENS Alta, sandboxing avanzado para análisis de malware, y seguridad IoT especializada [108].

Estas organizaciones tienen la responsabilidad de liderar el sector en el desarrollo e implementación de mejores prácticas de ciberseguridad, y pueden servir como recursos para organizaciones más pequeñas a través de programas de mentoría y intercambio de conocimientos [109].



www.fundacioel7.org

Análisis de Riesgos para Usuarios Vulnerables

Perfiles de Vulnerabilidad y Factores de Riesgo

Los usuarios atendidos por entidades de la Economía Social enfrentan vulnerabilidades de ciberseguridad compuestas que crean una convergencia de factores de riesgo únicos en el panorama de amenazas digitales. Estas vulnerabilidades no operan de forma aislada sino que interactúan de maneras complejas para crear patrones de riesgo que requieren enfoques de protección especializados y adaptados. La investigación identifica que los adultos mayores, individuos con discapacidades, inmigrantes, personas en situación de calle, y sobrevivientes de violencia doméstica enfrentan riesgos de ciberseguridad particularmente agudos que se amplifican por su dependencia de servicios proporcionados por entidades de Economía Social [110].

Vulnerabilidades Relacionadas con la Edad

Los adultos mayores representan una de las poblaciones más vulnerables a amenazas de ciberseguridad, enfrentando riesgos elevados debido a una combinación de factores cognitivos, tecnológicos y sociales que convergen para crear una superficie de ataque particularmente amplia. La investigación de la Comisión Federal de Comercio encuentra que individuos de 60 años y mayores reportan pérdidas por fraude en línea a tasas tres veces más altas que adultos más jóvenes, con pérdidas promedio significativamente mayores que alcanzan los 33.915 dólares por víctima [111].

Los cambios cognitivos relacionados con la edad afectan múltiples aspectos de la toma de decisiones de ciberseguridad. La investigación de Vishwanath, Harrison y Ng identifica deterioros específicos que incluyen disminuciones en memoria de trabajo que afectan la capacidad de mantener múltiples piezas de información en mente mientras se evalúan amenazas potenciales, reducciones en velocidad de procesamiento que afectan la capacidad de evaluar rápidamente situaciones de seguridad complejas, cambios en función ejecutiva que afectan la planificación e implementación de estrategias de seguridad, y alteraciones en capacidades de atención que afectan la capacidad de notar señales de advertencia sutiles en comunicaciones sospechosas [112].

La familiaridad limitada con tecnología digital y amenazas de ciberseguridad crea vulnerabilidades adicionales para adultos mayores. Muchos individuos en este grupo demográfico adoptaron tecnologías digitales más tarde en la vida y pueden no haber desarrollado la intuición para reconocer amenazas que es común entre usuarios más jóvenes que crecieron con tecnología digital. Esta falta de familiaridad se extiende a conceptos fundamentales de ciberseguridad como el reconocimiento de URLs sospechosas, la comprensión de por qué ciertas solicitudes de información son inapropiadas, y el conocimiento de cómo verificar la autenticidad de comunicaciones [113].

El aislamiento social, que afecta desproporcionadamente a adultos mayores, reduce las



www.fundacioel7.org

oportunidades de verificar información sospechosa con familiares o amigos de confianza. Este aislamiento puede ser exacerbado por la pérdida de cónyuges, la movilidad limitada, o la distancia geográfica de familiares, creando situaciones donde los individuos deben tomar decisiones de seguridad importantes sin acceso a redes de apoyo que podrían proporcionar verificación o consejo [114].

Vulnerabilidades Relacionadas con Discapacidades

Los individuos con discapacidades enfrentan vulnerabilidades únicas de ciberseguridad que surgen tanto de las barreras de accesibilidad en tecnología de seguridad como de factores sociales y económicos asociados con la discapacidad. La investigación encuentra que individuos con discapacidades cognitivas son particularmente vulnerables a ataques de ingeniería social, con tasas de victimización hasta cinco veces más altas que la población general [115].

Las discapacidades cognitivas crean vulnerabilidades específicas que incluyen dificultad para entender procedimientos de seguridad complejos que pueden involucrar múltiples pasos o conceptos abstractos, deterioro en la capacidad de reconocer amenazas o comunicaciones sospechosas que pueden requerir análisis sutil de intenciones o contexto, desafíos en implementar y mantener medidas de seguridad que requieren consistencia y atención a detalles, y mayor susceptibilidad a tácticas de manipulación usadas en ingeniería social que explotan la confianza y la buena voluntad [116].

Las discapacidades sensoriales crean diferentes tipos de vulnerabilidades de ciberseguridad. Los individuos con discapacidades visuales pueden tener dificultad para detectar indicadores visuales de sitios web fraudulentos, como URLs incorrectas, certificados de seguridad inválidos, o elementos de diseño que no coinciden con sitios legítimos. Pueden también depender de tecnologías de asistencia como lectores de pantalla que pueden no transmitir efectivamente todas las señales de advertencia de seguridad [117].

Los individuos con discapacidades auditivas pueden perderse alertas de audio importantes sobre amenazas de seguridad y pueden ser más susceptibles a ataques que explotan canales de comunicación visual como mensajes de texto o correo electrónico. Pueden también enfrentar desafíos en verificar la autenticidad de comunicaciones cuando los métodos de verificación primarios dependen de comunicación telefónica [118].

Las discapacidades físicas pueden crear barreras para usar interfaces de seguridad estándar, incluyendo dificultades para introducir contraseñas complejas, usar dispositivos de autenticación multifactor que requieren manipulación física precisa, o navegar interfaces de seguridad que no están diseñadas para accesibilidad. Estas barreras pueden llevar a individuos a adoptar prácticas de seguridad menos robustas por necesidad práctica [119].



www.fundacioel7.org

Vulnerabilidades Socioeconómicas

Las limitaciones económicas impactan significativamente las capacidades de ciberseguridad para poblaciones vulnerables atendidas por entidades de Economía Social. El costo de software y servicios de seguridad puede ser prohibitivo para individuos con recursos financieros limitados, forzándolos a depender de soluciones gratuitas que pueden ofrecer protección inferior o a operar sin protección adecuada. Esta limitación se extiende a dispositivos, donde individuos con recursos limitados pueden usar hardware más antiguo que no soporta medidas de seguridad modernas [120].

La necesidad de priorizar necesidades básicas como vivienda, alimentación y atención médica sobre inversiones en tecnología significa que la seguridad digital puede ser vista como un lujo en lugar de una necesidad. Esta priorización es racional desde la perspectiva de supervivencia inmediata, pero crea vulnerabilidades a largo plazo que pueden resultar en pérdidas financieras significativas a través de fraudes o robos de identidad [121].

El acceso limitado a servicios financieros tradicionales puede requerir dependencia de sistemas financieros alternativos que pueden tener características de seguridad diferentes o menos robustas. Esto incluye el uso de servicios de transferencia de dinero no bancarios, tarjetas prepagadas, o sistemas de pago móvil que pueden no tener las mismas protecciones que los servicios bancarios tradicionales [122].

Vectores de Amenaza Específicos

El análisis de vectores de amenaza específicos que afectan a usuarios vulnerables revela patrones de ataque que explotan sistemáticamente las vulnerabilidades identificadas anteriormente. Estos vectores han evolucionado para dirigirse específicamente a poblaciones vulnerables, aprovechando su mayor susceptibilidad y menor capacidad de respuesta.

Phishing y Estafas por Correo Electrónico

El phishing dirigido a poblaciones vulnerables ha evolucionado para explotar específicamente las características psicológicas y sociales que aumentan la susceptibilidad a estos ataques. Los estafadores utilizan técnicas de ingeniería social sofisticadas que apelan a las emociones para reducir la capacidad de evaluación crítica de las víctimas potenciales. Esto incluye mensajes que generan alegría con promesas de premios o subsidios inesperados, comunicaciones que crean miedo o preocupación sobre la suspensión de cuentas o servicios esenciales, y solicitudes que explotan la compasión con historias de emergencias familiares o necesidades urgentes [123].

Los ataques de phishing dirigidos a usuarios de entidades de Economía Social frecuentemente suplantan organismos oficiales o entidades de confianza que son relevantes para las poblaciones objetivo. Esto incluye correos falsos que simulan provenir de administraciones públicas con asuntos como "Ayuda económica para beneficiarios" o "Curso



www.fundacioel7.org

gratuito de empleabilidad", comunicaciones fraudulentas que se hacen pasar por organizaciones de servicios sociales un sentido de urgencia y legitimidad [124].

La sofisticación de estos ataques ha aumentado significativamente, con estafadores utilizando información disponible públicamente sobre organizaciones y sus beneficiarios para crear mensajes altamente personalizados y convincentes. Esto puede incluir referencias a programas específicos en los que la víctima está inscrita, uso de nombres de trabajadores sociales reales, o menciones de eventos recientes en la comunidad local [125].

Vishing y Suplantación Telefónica

Los ataques de vishing (phishing por voz) han emergido como una amenaza particularmente efectiva contra poblaciones vulnerables que pueden tener mayor confianza en comunicaciones telefónicas que en comunicaciones digitales. Estos ataques explotan la familiaridad y comodidad que muchas personas mayores y individuos con limitada alfabetización digital tienen con la comunicación telefónica [126].

Los estafadores utilizan técnicas sofisticadas para crear credibilidad, incluyendo el uso de tecnología de spoofing para hacer que las llamadas parezcan provenir de números oficiales, la utilización de información personal obtenida de violaciones de datos previas para establecer credibilidad, y el empleo de scripts cuidadosamente desarrollados que anticipan y responden a objeciones comunes [127].

Los ataques de vishing dirigidos a usuarios de servicios sociales frecuentemente se hacen pasar por representantes de organismos gubernamentales como la Seguridad Social, Hacienda, o servicios de salud, alegando problemas con beneficios o necesidad de verificar información personal. También pueden simular ser de bancos o instituciones financieras, alegando actividad sospechosa en cuentas o necesidad de verificar transacciones [128].

Estafas en Redes Sociales y Mensajería

Las redes sociales han creado nuevas oportunidades para que los estafadores identifiquen y dirijan ataques a poblaciones vulnerables. Los grupos de Facebook dedicados a apoyo para personas con discapacidades, adultos mayores, o individuos en situaciones económicas difíciles proporcionan a los estafadores acceso a información detallada sobre víctimas potenciales y sus vulnerabilidades específicas [129].

Los estafadores se infiltran en estos espacios comunitarios para identificar víctimas potenciales, establecer relaciones de confianza a largo plazo, y eventualmente explotar estas relaciones para obtener dinero o información personal. Un caso documentado por Panda Security describe cómo un joven con discapacidad fue estafado durante meses a través de Facebook por un atacante que se hizo pasar por un activista ofreciendo asesoría y apoyo [130].

Las ofertas fraudulentas de empleo dirigidas específicamente a personas con discapacidades o en desempleo han proliferado en plataformas sociales. Estos ataques



www.fundacioel7.org

pueden incluir falsas entrevistas por videoconferencia para dar credibilidad al proceso, solicitudes de información personal bajo el pretexto de verificación de antecedentes, y demandas de pagos por adelantado para materiales de formación o equipos [131].

Malware y Ransomware Dirigido

Aunque el malware tradicionalmente se ha dirigido a objetivos corporativos de alto valor, hay evidencia creciente de ataques dirigidos específicamente a individuos vulnerables y las organizaciones que los atienden. Estos ataques explotan la menor probabilidad de que las víctimas tengan software de seguridad actualizado y la mayor probabilidad de que paguen rescates para recuperar datos importantes [132].

Los ataques de ransomware dirigidos a usuarios individuales vulnerables frecuentemente cifran no solo archivos del sistema sino también documentos personales importantes como fotografías familiares, documentos médicos, o registros financieros que pueden ser irremplazables para las víctimas. Los atacantes calculan que estas víctimas estarán más dispuestas a pagar rescates para recuperar estos archivos personalmente significativos [133].

Análisis Cuantitativo de Riesgos

El análisis cuantitativo de riesgos para usuarios vulnerables revela patrones estadísticos que demuestran la magnitud y distribución de amenazas de ciberseguridad en estas poblaciones. Los datos disponibles, aunque limitados por la subnotificación típica en estas comunidades, proporcionan insights valiosos sobre la prevalencia y el impacto de diferentes tipos de ataques.

Estadísticas de Victimización por Demografía

Los adultos mayores experimentan tasas de victimización desproporcionadamente altas en múltiples categorías de cibercrimen. En Estados Unidos, 88.000 mayores de 60 años perdieron más de 3.100 millones de dólares en fraudes online en un año, principalmente por estafas de soporte técnico falso y criptomonedas [134]. Extrapolando estos datos al contexto español, considerando la población de adultos mayores y las diferencias en adopción tecnológica, se estima que las pérdidas anuales por ciberestafas dirigidas a personas mayores en España alcanzan aproximadamente 3.000 millones de euros anuales.

Los individuos con discapacidades enfrentan tasas de victimización que son hasta cinco veces más altas que la población general para ciertos tipos de ataques de ingeniería social. La investigación específica encuentra que el 47% de individuos con discapacidades cognitivas han sido objetivo de al menos un intento de estafa en línea en el último año, comparado con el 12% de la población general [135].

Las poblaciones de bajos ingresos experimentan impactos desproporcionadamente severos de incidentes de ciberseguridad debido a su menor capacidad de absorber pérdidas



www.fundacioel7.org

financieras y su mayor dependencia de servicios digitales para acceder a beneficios esenciales. Una pérdida de 500 euros por fraude puede representar una crisis financiera significativa para una familia de bajos ingresos, mientras que la misma pérdida puede ser un inconveniente menor para familias de ingresos más altos [136].

Factores Psicológicos en la Susceptibilidad

La investigación psicológica revela que ciertos factores cognitivos y emocionales predicen significativamente la susceptibilidad a ataques de ciberseguridad. El deterioro cognitivo asociado con el envejecimiento impacta la toma de decisiones de seguridad, con la capacidad de toma de decisiones correlacionada negativamente con la edad ($r = -0.26$, $p < 0.001$) y la susceptibilidad al fraude correlacionada negativamente con la cognición general ($r = -0.30$, $p < 0.001$) [137].

Los factores de salud mental, particularmente la depresión, representan el factor psicológico más poderoso asociado con la susceptibilidad al fraude en línea. Los individuos con los niveles más altos de depresión y menor satisfacción de necesidades sociales experimentan una prevalencia de fraude tres veces mayor que aquellos con mejor salud mental y redes sociales más robustas [138].

El aislamiento social emerge como un factor de riesgo crítico que amplifica otros factores de vulnerabilidad. Los individuos socialmente aislados tienen menos oportunidades de verificar información sospechosa con otros, pueden ser más susceptibles a tácticas de manipulación que explotan la soledad, y pueden tener menos acceso a información sobre amenazas emergentes [139].

Metodología de Evaluación de Riesgos

La evaluación efectiva de riesgos para usuarios vulnerables requiere metodologías especializadas que acomoden las características únicas de estas poblaciones. Los enfoques tradicionales de evaluación de riesgos, diseñados para entornos corporativos, pueden no capturar adecuadamente los factores de riesgo específicos que afectan a poblaciones vulnerables [140].

La evaluación basada en activos debe considerar no solo los activos digitales tradicionales sino también los activos únicos que son particularmente valiosos para poblaciones vulnerables. Esto incluye información de beneficios gubernamentales, registros médicos, documentación de inmigración, y otra información que puede ser crítica para el acceso a servicios esenciales [141].

El análisis basado en vulnerabilidades debe incorporar factores psicológicos, sociales y económicos además de vulnerabilidades técnicas tradicionales. Esto incluye la evaluación de factores como el aislamiento social, las limitaciones cognitivas, las barreras idiomáticas, y las limitaciones económicas que pueden afectar la capacidad de implementar o mantener medidas de seguridad [142].



www.fundacioel7.org

La evaluación basada en amenazas debe considerar los vectores de ataque específicos que se dirigen a poblaciones vulnerables, incluyendo estafas de ingeniería social sofisticadas, ataques dirigidos que explotan información disponible públicamente sobre servicios sociales, y amenazas que explotan la dependencia de tecnologías de asistencia [143].

Vulnerabilidades en Procesos Digitales

Los procesos digitales utilizados por poblaciones vulnerables para acceder a servicios esenciales crean superficies de ataque únicas que requieren consideración especializada. Estos procesos frecuentemente involucran la transmisión de información altamente sensible a través de canales que pueden no estar optimizados para seguridad, y pueden requerir que individuos con limitada alfabetización digital naveguen procedimientos complejos sin asistencia adecuada.

Trámites Administrativos Obligatorios

La creciente digitalización de trámites administrativos ha creado nuevas vulnerabilidades para poblaciones que pueden no tener las habilidades o recursos necesarios para navegar estos sistemas de manera segura. Cuando no hay alternativas presenciales disponibles, los individuos vulnerables se ven forzados a usar medios digitales que no dominan, aumentando significativamente la probabilidad de caer en trampas o cometer errores que comprometan su seguridad [144].

Los portales gubernamentales para solicitar beneficios, renovar documentación, o acceder a servicios pueden ser objetivos atractivos para estafadores que crean sitios web fraudulentos que imitan estos portales oficiales. Los individuos que buscan estos servicios a través de motores de búsqueda pueden inadvertidamente acceder a sitios fraudulentos que recopilan información personal para uso malicioso [145].

La complejidad de muchos procedimientos digitales gubernamentales puede llevar a individuos vulnerables a buscar asistencia de terceros no autorizados que pueden abusar de su acceso a información personal. Esto incluye "gestores" no oficiales que ofrecen ayuda con trámites a cambio de pagos, pero que pueden usar la información obtenida para propósitos fraudulentos [146].

Uso de Dispositivos Compartidos

Muchas poblaciones vulnerables dependen de dispositivos compartidos en bibliotecas públicas, centros comunitarios, o ciberaulas para acceder a servicios digitales. Estos entornos crean vulnerabilidades únicas debido a la dificultad de mantener medidas de seguridad consistentes en dispositivos utilizados por múltiples usuarios con diferentes niveles de conocimiento de seguridad [147].

Los dispositivos compartidos pueden retener información de sesiones previas si no se configuran adecuadamente para limpiar datos entre usuarios. Esto puede incluir contraseñas



www.fundacioel7.org

guardadas, información de formularios autocompletados, o archivos descargados que pueden contener información personal de usuarios previos [148].

La falta de control sobre la configuración de seguridad en dispositivos compartidos significa que los usuarios pueden no tener acceso a medidas de seguridad como software antivirus actualizado, navegadores con configuraciones de seguridad apropiadas, o conexiones de red seguras [149].

Dependencia de Terceros para Asistencia Digital

La brecha digital frecuentemente requiere que individuos vulnerables dependan de familiares, amigos, o cuidadores para asistencia con tareas digitales. Esta dependencia crea vulnerabilidades cuando los asistentes pueden no tener conocimientos adecuados de ciberseguridad o cuando la relación de confianza es abusada [150].

Los cuidadores formales e informales pueden tener acceso a información personal sensible sin la supervisión o formación adecuada para manejar esta información de manera segura. Esto puede incluir acceso a contraseñas, información financiera, o datos médicos que podrían ser mal utilizados [151].

La delegación de responsabilidades digitales puede crear confusión sobre quién es responsable de mantener medidas de seguridad, resultando en brechas donde nadie está monitoreando activamente la seguridad de cuentas o dispositivos importantes [152].



www.fundacioel7.org

Protocolos de Actuación y Estrategias de Mitigación

Educación y Concienciación Diferenciada

La educación en ciberseguridad para usuarios vulnerables requiere enfoques especializados que reconozcan y acomoden las diversas capacidades, limitaciones y circunstancias de estas poblaciones. Los programas de educación tradicionales, diseñados para audiencias corporativas o usuarios tecnológicamente sofisticados, frecuentemente fallan en abordar las necesidades específicas de poblaciones vulnerables y pueden inadvertidamente crear barreras adicionales para la adopción de prácticas de seguridad [153].

Programas de Formación Adaptados por Nivel de Alfabetización

Para usuarios de nivel básico, incluyendo adultos mayores y nuevos usuarios digitales, los programas de formación deben enfatizar la interacción personal y el apoyo individualizado. Esto incluye sesiones de formación presencial uno-a-uno que permiten el ritmo personalizado y la repetición según sea necesario, materiales educativos en formato audio y video que acomoden diferentes preferencias de aprendizaje y limitaciones de alfabetización, y sistemas de contraseñas gestionadas por administradores que reduzcan la carga cognitiva en los usuarios mientras mantienen la seguridad [154].

La navegación supervisada para primeros usos de servicios digitales críticos proporciona un entorno seguro para que los usuarios desarrollen confianza y competencia. Esto puede incluir acompañamiento durante las primeras interacciones con portales gubernamentales, asistencia en la configuración inicial de cuentas de correo electrónico seguras, y orientación práctica sobre cómo reconocer y responder a comunicaciones sospechosas [155].

Para usuarios de nivel intermedio, que incluyen usuarios habituales de tecnología, pero sin formación especializada en seguridad, los programas pueden utilizar formatos grupales que aprovechen el aprendizaje peer-to-peer. Esto incluye talleres grupales online que permiten la interacción y el intercambio de experiencias, guías visuales paso a paso que pueden ser consultadas independientemente, y la introducción de gestores de contraseñas recomendados con asistencia para la configuración inicial [156].

Los usuarios de nivel avanzado, incluyendo personal técnico y voluntarios digitales, pueden recibir formación técnica especializada que los prepare para servir como recursos de apoyo para otros usuarios. Esto incluye certificaciones en ciberseguridad específicas del sector social, responsabilidades formales de apoyo a otros usuarios, acceso a herramientas avanzadas de detección de amenazas, y roles de liderazgo en la implementación de medidas de seguridad organizacionales [157].

Materiales Educativos Accesibles

El desarrollo de materiales educativos accesibles requiere la aplicación de principios de diseño universal que aseguren que la información sea comprensible y utilizable por



www.fundacioel7.org

personas con diversas capacidades y antecedentes. Esto incluye la creación de contenido en Lectura Fácil siguiendo estándares establecidos de accesibilidad cognitiva, que utiliza lenguaje simple, estructuras de oración claras, y conceptos concretos en lugar de abstracciones complejas [158].

Los pictogramas y símbolos de comunicación visual universal pueden complementar el texto para hacer la información más accesible para personas con limitaciones de alfabetización o barreras idiomáticas. Estos elementos visuales deben ser culturalmente apropiados y probados con las poblaciones objetivo para asegurar que comuniquen efectivamente los conceptos de seguridad deseados [159].

La traducción a lenguas cooficiales y la adaptación cultural del contenido aseguran que las comunidades diversas puedan acceder a información de seguridad en sus idiomas preferidos. Esto va más allá de la traducción literal para incluir la adaptación de ejemplos, referencias culturales, y contextos que sean relevantes para diferentes comunidades [160].

Las versiones adaptadas para discapacidades visuales o auditivas deben desarrollarse utilizando tecnologías de asistencia apropiadas y en consulta con las comunidades afectadas. Esto incluye versiones de audio de materiales escritos, descripciones de audio para contenido visual, subtítulos y transcripciones para contenido de video, y versiones en braille o texto ampliado para materiales impresos [161].

Simulaciones y Ejercicios Prácticos

Las simulaciones de phishing adaptadas para poblaciones vulnerables deben diseñarse cuidadosamente para ser educativas sin ser traumáticas o confusas. Esto incluye el uso de ejemplos que sean relevantes para las experiencias de los usuarios objetivo, la provisión de explicaciones claras sobre por qué ciertos elementos son sospechosos, y el seguimiento inmediato con orientación sobre cómo responder apropiadamente a amenazas similares [162].

Los ejercicios de práctica para verificación de comunicaciones pueden enseñar a los usuarios cómo confirmar la autenticidad de mensajes sospechosos utilizando canales alternativos. Esto incluye la práctica de llamar a números oficiales conocidos para verificar solicitudes inesperadas, el uso de sitios web oficiales para confirmar información, y la consulta con personal de confianza de organizaciones de servicios sociales [163].

Las simulaciones de escenarios de respuesta a incidentes pueden preparar a los usuarios para responder apropiadamente cuando sospechen que han sido víctimas de un ataque. Esto incluye la práctica de pasos inmediatos como cambiar contraseñas, contactar a instituciones financieras, y reportar incidentes a autoridades apropiadas [164].



www.fundacioel7.org

Medidas Técnicas de Protección Reforzada

Las medidas técnicas de protección para usuarios vulnerables deben equilibrar la efectividad de seguridad con la accesibilidad y facilidad de uso. Esto requiere el desarrollo de soluciones que proporcionen protección robusta mientras minimizando la complejidad operacional para usuarios que pueden tener limitada experiencia técnica o capacidades cognitivas reducidas.

Filtros Anti-Phishing y Seguridad del Correo

La implementación de filtros anti-phishing robustos debe adaptarse a los patrones de comunicación típicos de entidades de Economía Social y sus usuarios. Esto incluye la configuración de filtros que reconozcan y bloqueen intentos de suplantación de organismos gubernamentales, organizaciones de servicios sociales, y otras entidades que son frecuentemente imitadas en ataques dirigidos a poblaciones vulnerables [165].

Los sistemas de marcación y advertencia deben proporcionar alertas claras y comprensibles cuando se detecten comunicaciones potencialmente sospechosas. Esto incluye el uso de lenguaje simple en lugar de jerga técnica, la provisión de explicaciones específicas sobre por qué un mensaje es considerado sospechoso, y la orientación clara sobre qué acciones deben tomar los usuarios [166].

La integración con servicios de correo electrónico comúnmente utilizados por poblaciones vulnerables, como Gmail y Outlook, debe aprovechar las características de seguridad incorporadas mientras proporcionando configuración adicional apropiada para usuarios de alto riesgo. Esto puede incluir la habilitación de verificación en dos pasos con opciones adaptadas para diferentes capacidades, la configuración de filtros de spam más agresivos, y la activación de alertas de seguridad mejoradas [167].

Protección de Dispositivos y Redes

La protección de dispositivos utilizados por poblaciones vulnerables debe considerar que estos dispositivos pueden ser más antiguos, tener recursos limitados, o ser compartidos entre múltiples usuarios. Esto requiere la selección de soluciones de seguridad que sean efectivas en hardware con limitaciones y que no degraden significativamente el rendimiento del dispositivo [168].

Los equipos compartidos en centros comunitarios, bibliotecas, o ciberaulas requieren configuraciones especiales que protejan tanto a los usuarios individuales como a la infraestructura general. Esto incluye la implementación de software de congelación de configuración que revierta cualquier cambio al reiniciar, garantizando que cualquier malware introducido por un usuario se elimine automáticamente [169].

La configuración de redes Wi-Fi para usuarios vulnerables debe incluir portales cautivos que proporcionen orientación de seguridad básica al conectarse, filtrado de contenido que



www.fundacioel7.org

bloquee sitios conocidos por alojar malware o estafas, y separación de tráfico que aisle las actividades de usuarios de sistemas críticos de la organización [170].

Gestión de Identidades y Accesos Adaptativa

Los sistemas de gestión de identidades para usuarios vulnerables deben implementar principios de autenticación adaptativa que ajusten los requisitos de seguridad basándose en el perfil de riesgo del usuario y el contexto de acceso. Esto incluye la implementación de autenticación multifactor con opciones flexibles que acomoden diferentes capacidades y limitaciones [171].

Para usuarios con discapacidades cognitivas, esto puede incluir opciones de autenticación simplificadas como PINs de 4 dígitos combinados con verificación biométrica opcional, o sistemas de autenticación basados en reconocimiento de imágenes que pueden ser más intuitivos que contraseñas alfanuméricas complejas [172].

Para usuarios mayores que pueden tener dificultades con tecnología móvil, las opciones pueden incluir autenticación por llamada telefónica automatizada, tokens físicos que no requieren interacción con smartphones, o sistemas de verificación presencial para transacciones de alto riesgo [173].

Los sistemas de gestión de acceso deben implementar principios de privilegio mínimo mientras manteniendo la flexibilidad necesaria para acomodar las necesidades cambiantes de usuarios vulnerables. Esto incluye la capacidad de escalar temporalmente privilegios de acceso durante emergencias, la provisión de acceso asistido donde cuidadores autorizados pueden ayudar con tareas digitales, y la implementación de controles de acceso basados en tiempo que limiten el acceso a horarios apropiados [174].

Protocolos de Respuesta a Incidentes Especializados

Los protocolos de respuesta a incidentes para entidades de Economía Social deben abordar tanto los aspectos técnicos de la respuesta como las necesidades especiales de poblaciones vulnerables que pueden verse afectadas por incidentes de seguridad. Estos protocolos deben ser escalables, permitiendo respuestas apropiadas tanto para incidentes menores como para crisis de seguridad mayores.

Procedimientos ante Phishing Dirigido

Los protocolos ante phishing dirigido deben establecer tiempos de respuesta máximos que reconozcan la urgencia particular de proteger a poblaciones vulnerables. La contención inicial debe completarse dentro de 15 minutos de la detección, incluyendo el aislamiento de dispositivos potencialmente comprometidos, la preservación de evidencia para investigación posterior, y la notificación inmediata al responsable de protección de datos [175].

La evaluación del alcance debe completarse dentro de 30 minutos a 2 horas, incluyendo la verificación de la autenticidad de comunicaciones sospechosas por canales alternativos, la



www.fundacioel7.org

evaluación del número de usuarios potencialmente afectados, y la determinación de qué tipos de información pueden haber sido comprometidos [176].

La comunicación a usuarios afectados debe adaptarse a sus capacidades y necesidades específicas. Para usuarios vulnerables, esto incluye comunicación telefónica personalizada utilizando lenguaje claro y empático, seguimiento por correo electrónico con instrucciones escritas en formato accesible, y la provisión de apoyo presencial cuando sea necesario para usuarios que puedan tener dificultades para entender o implementar medidas de protección [177].

Respuesta a Ransomware

Los procedimientos ante ransomware para organizaciones con recursos limitados deben enfatizar la preparación preventiva y la respuesta rápida para minimizar el impacto en servicios esenciales. La preparación preventiva incluye el mantenimiento de copias de seguridad siguiendo la estrategia 3-2-1, el mantenimiento de un inventario actualizado de sistemas críticos, y el establecimiento de acuerdos previos con proveedores de TI especializados en respuesta a incidentes [178].

La respuesta inmediata en las primeras 4 horas debe incluir la desconexión inmediata de sistemas afectados para prevenir la propagación, el contacto con INCIBE-CERT para reportar el incidente y obtener asistencia técnica, la identificación de la variante de ransomware utilizando herramientas proporcionadas por CCN-CERT, y la evaluación de qué sistemas críticos han sido afectados [179].

La política de no pago de rescates debe mantenerse firmemente, siguiendo las recomendaciones expresas de CCN-CERT y otras autoridades de seguridad. En su lugar, la recuperación debe enfocarse en la restauración desde copias de seguridad, la reconstrucción de sistemas comprometidos, y la implementación de medidas adicionales para prevenir reinfección [180].

Gestión de Violaciones de Datos de Beneficiarios

Los procedimientos ante violaciones de datos de beneficiarios deben reconocer que estos incidentes pueden tener consecuencias particularmente graves para poblaciones vulnerables. La evaluación del riesgo debe completarse dentro de 24 horas, clasificando el riesgo como alto para datos especialmente protegidos (información de salud, ubicación de víctimas de violencia doméstica), riesgo medio para datos identificativos combinados con información económica, y bajo riesgo para datos básicos de contacto [181].

La notificación obligatoria a la AEPD debe completarse dentro del máximo de 72 horas utilizando el formulario electrónico con certificado digital, incluyendo información específica sobre el tipo de datos comprometidos, las características de las personas afectadas, y las medidas específicas adoptadas para mitigar el impacto en poblaciones vulnerables [182].



www.fundacioel7.org

La comunicación a afectados debe realizarse sin dilación indebida si hay riesgo alto, utilizando lenguaje adaptado a las capacidades de comprensión de los beneficiarios y canales múltiples según el perfil del usuario. Esto puede incluir comunicación telefónica para usuarios con limitada alfabetización digital, cartas físicas para usuarios sin acceso a correo electrónico, y comunicación a través de cuidadores autorizados cuando sea apropiado [183].

Estrategias de Mitigación por Tipo de Riesgo

Las estrategias de mitigación deben adaptarse específicamente a los vectores de amenaza más prevalentes que afectan a poblaciones vulnerables, proporcionando contramedidas prácticas y implementables que puedan ser utilizadas tanto por las organizaciones como por los usuarios individuales.

Contramedidas para Phishing y Fraudes Online

La mitigación de phishing y fraudes online requiere una combinación de medidas técnicas, educativas y procedimentales que trabajen juntas para reducir tanto la probabilidad de exposición como el impacto de ataques exitosos. La formación intensiva debe incluir simulaciones regulares utilizando ejemplos relevantes para las poblaciones objetivo, la enseñanza de técnicas de verificación que puedan ser utilizadas por usuarios con diferentes capacidades, y el refuerzo continuo de mensajes de seguridad a través de múltiples canales [184].

Los filtros antiphishing deben configurarse de manera más agresiva para usuarios de alto riesgo, incluyendo el bloqueo de dominios recientemente registrados que frecuentemente se utilizan en ataques, la implementación de listas blancas de remitentes conocidos y confiables, y la marcación clara de correos electrónicos que provienen de fuentes externas [185].

La política de "verificar antes de confiar" debe institucionalizarse a través de procedimientos claros que enseñen a los usuarios a confirmar la autenticidad de cualquier comunicación inesperada utilizando canales alternativos conocidos. Esto incluye la provisión de números de teléfono oficiales que los usuarios puedan llamar para verificar comunicaciones, la educación sobre cómo acceder a sitios web oficiales directamente en lugar de a través de enlaces en correos electrónicos, y la creación de una cultura donde hacer preguntas sobre comunicaciones sospechosas es alentado y apoyado [186].

Protección contra Vishing y Suplantación Telefónica

La protección contra vishing requiere la educación de usuarios sobre las tácticas comunes utilizadas en estos ataques y el establecimiento de procedimientos claros para verificar la autenticidad de llamadas inesperadas. La regla fundamental que debe enseñarse es que "las entidades legítimas nunca te van a pedir por teléfono tus contraseñas ni códigos de verificación" [187].



www.fundacioel7.org

Los procedimientos de verificación deben incluir la instrucción de colgar y llamar de vuelta al número oficial de la organización supuesta para confirmar la legitimidad de cualquier solicitud inesperada, la verificación de información personal que solo la organización legítima debería conocer, y la consulta con personal de confianza de organizaciones de servicios sociales antes de proporcionar información sensible [188].

Para organizaciones que realizan llamadas legítimas a usuarios, los procedimientos deben incluir la identificación clara y completa al inicio de la llamada, la provisión de información que permita al usuario verificar la legitimidad de la llamada, y la oferta de opciones para que el usuario devuelva la llamada al número oficial si prefiere verificar la autenticidad [189].

Prevención de Malware y Ransomware

La prevención de malware y ransomware para usuarios vulnerables debe enfocarse en medidas que sean efectivas sin requerir expertise técnico significativo. Esto incluye la instalación y mantenimiento de software antivirus con actualizaciones automáticas habilitadas, la configuración de sistemas operativos para instalar actualizaciones de seguridad automáticamente, y la educación sobre prácticas seguras de navegación y descarga [190].

Las restricciones de instalación en equipos utilizados por poblaciones vulnerables pueden prevenir la instalación accidental de software malicioso. Esto incluye la configuración de cuentas de usuario con privilegios limitados que no permitan la instalación de software, la implementación de listas blancas de aplicaciones que solo permitan la ejecución de software aprobado, y la utilización de navegadores web con configuraciones de seguridad restrictivas [191].

Los procedimientos de respaldo deben ser automatizados y transparentes para el usuario, incluyendo copias de seguridad automáticas de documentos importantes a servicios de nube seguros, la verificación regular de la integridad de las copias de seguridad, y procedimientos claros para la restauración de datos en caso de infección [192].

Protección de Privacidad y Datos Personales

La protección de privacidad para poblaciones vulnerables requiere enfoques que reconozcan que estos individuos pueden enfrentar riesgos únicos si su información personal es comprometida.

Esto incluye la educación sobre los derechos digitales fundamentales, incluyendo el derecho a saber cómo se utilizan los datos personales, el derecho a solicitar la corrección o eliminación de información incorrecta, y el derecho a limitar el uso de información personal para ciertos propósitos [193].

Las medidas prácticas de protección de privacidad incluyen la configuración de ajustes de privacidad en redes sociales para limitar quién puede ver información personal, la educación



www.fundacioel7.org

sobre qué tipos de información no deben compartirse públicamente online, y la orientación sobre cómo reconocer y responder a solicitudes inapropiadas de información personal [194].

Los servicios de mediación digital pueden proporcionar asistencia segura para usuarios que necesitan completar tareas digitales importantes pero no se sienten seguros haciéndolo independientemente. Esto incluye la provisión de asistencia supervisada para trámites gubernamentales importantes, el apoyo para la configuración de cuentas de servicios esenciales, y la orientación para la resolución de problemas de seguridad cuando surjan [195].

Colaboración Interinstitucional y Redes de Apoyo

La efectividad de las estrategias de mitigación se amplifica significativamente a través de la colaboración entre organizaciones del sector y con entidades externas que pueden proporcionar recursos y expertise especializados. Esta colaboración es particularmente importante para entidades de Economía Social que pueden tener recursos limitados individualmente pero que pueden lograr capacidades significativas a través de esfuerzos coordinados.

Redes de Intercambio de Información

El establecimiento de redes formales de intercambio de información sobre amenazas permite a las organizaciones del sector beneficiarse de la experiencia colectiva y responder más rápidamente a amenazas emergentes. Esto incluye la participación en grupos de trabajo de CEPES enfocados en ciberseguridad, la colaboración con otras organizaciones del sector para compartir información sobre ataques y contramedidas efectivas, y el acceso a feeds de inteligencia de amenazas proporcionados por INCIBE específicamente para el sector social [196].

Los protocolos de notificación entre organizaciones deben establecer procedimientos claros para alertar a otras entidades cuando se detecten amenazas que puedan afectar al sector más ampliamente. Esto incluye la notificación confidencial de campañas de phishing dirigidas al sector, el intercambio de información sobre nuevas variantes de malware que afecten específicamente a organizaciones sociales, y la coordinación de respuestas a amenazas que puedan requerir acción colectiva [197].

Colaboración con Sector Privado

La colaboración con el sector privado a través de programas de responsabilidad social corporativa puede proporcionar acceso a recursos y expertise que de otra manera serían inaccesibles para organizaciones con presupuestos limitados. Esto incluye la donación de licencias de software de seguridad por parte de empresas tecnológicas, la provisión de servicios de consultoría pro bono por parte de firmas de ciberseguridad, y el voluntariado corporativo para proporcionar formación técnica especializada [198].



www.fundacioel7.org

Los acuerdos de respuesta a emergencias con proveedores del sector privado pueden asegurar que las organizaciones tengan acceso a asistencia técnica especializada durante incidentes críticos. Esto incluye acuerdos para servicios de respuesta a incidentes con tarifas reducidas o gratuitas, acceso prioritario a soporte técnico durante emergencias, y la provisión de recursos de recuperación cuando los sistemas internos sean comprometidos [199].

Coordinación con Autoridades

La coordinación efectiva con autoridades gubernamentales y fuerzas de seguridad puede mejorar tanto la prevención como la respuesta a incidentes de ciberseguridad. Esto incluye la participación en programas de INCIBE específicamente diseñados para organizaciones sin fines de lucro, la colaboración con unidades especializadas de la Guardia Civil y Policía Nacional que se enfocan en ciberdelincuencia, y el acceso a recursos de CCN-CERT para organizaciones que manejen información sensible [200].

Los protocolos de reporte a autoridades deben establecer procedimientos claros para cuándo y cómo reportar diferentes tipos de incidentes, incluyendo los umbrales para reportar incidentes a INCIBE-CERT, los procedimientos para reportar delitos cibernéticos a fuerzas de seguridad, y los requisitos para notificar violaciones de datos a la AEPD [201].

La participación en ejercicios de respuesta coordinada puede mejorar la preparación del sector para amenazas mayores que puedan afectar múltiples organizaciones simultáneamente. Esto incluye la participación en simulacros de ciberseguridad organizados por autoridades gubernamentales, la colaboración en el desarrollo de planes de respuesta sectorial, y la contribución a la mejora continua de capacidades de respuesta nacional [202].



www.fundacioel7.org

Conclusiones y Recomendaciones

Síntesis de Hallazgos Principales

Este estudio integral revela que las entidades de la Economía Social en España enfrentan un panorama de ciberseguridad caracterizado por vulnerabilidades únicas, amenazas dirigidas, y limitaciones de recursos que requieren enfoques especializados de protección. Los hallazgos principales demuestran que las medidas de ciberseguridad tradicionales, diseñadas para entornos corporativos, son inadecuadas para abordar las características específicas del sector social y las necesidades de las poblaciones vulnerables que atiende [285].

La investigación identifica que el 31% de las organizaciones benéficas han experimentado brechas de ciberseguridad en los últimos 12 meses, con reclamaciones promedio que alcanzan los 86.500 euros, mientras que estas organizaciones invierten un 42% menos en ciberseguridad que empresas comerciales equivalentes. Esta disparidad crea una vulnerabilidad sistémica que se amplifica por el hecho de que las entidades de Economía Social manejan información de poblaciones que son desproporcionadamente vulnerables a las consecuencias de violaciones de datos y interrupciones de servicios [286].

El análisis de vulnerabilidades específicas revela que los adultos mayores, individuos con discapacidades, inmigrantes, personas en situación de calle, y sobrevivientes de violencia doméstica enfrentan riesgos de ciberseguridad que son hasta cinco veces más altos que la población general para ciertos tipos de ataques. Estas vulnerabilidades surgen de la convergencia de factores cognitivos, tecnológicos, socioeconómicos y culturales que crean superficies de ataque únicas que requieren contramedidas especializadas [287].

Contribuciones Teóricas y Prácticas

Este estudio representa la primera investigación integral que aborda específicamente los desafíos de ciberseguridad que enfrentan las entidades de la Economía Social española y las poblaciones vulnerables que atienden. Las contribuciones teóricas incluyen el desarrollo de un marco conceptual que integra consideraciones de ciberseguridad técnica con principios de justicia social, accesibilidad universal, y protección de derechos humanos [288].

El marco de Diseño de Seguridad Inclusiva desarrollado en este estudio proporciona principios y metodologías que pueden aplicarse más allá del sector de la Economía Social para informar el desarrollo de tecnologías de seguridad que acomoden diversas capacidades y circunstancias. Este marco desafía las suposiciones tradicionales sobre la relación entre seguridad y usabilidad, demostrando que es posible desarrollar soluciones que sean tanto robustas técnicamente como accesibles para poblaciones vulnerables [289].



www.fundacioel7.org

Las contribuciones prácticas incluyen el desarrollo de herramientas de evaluación de riesgos específicamente adaptadas para entidades de Economía Social, protocolos de respuesta a incidentes que consideran las necesidades especiales de poblaciones vulnerables, y especificaciones detalladas para una aplicación móvil de orientación en ciberseguridad que implementa principios de diseño universal [290].

Recomendaciones Estratégicas

Las recomendaciones estratégicas emergentes de esta investigación abordan múltiples niveles del ecosistema de ciberseguridad, desde políticas gubernamentales hasta prácticas organizacionales individuales. A nivel de política pública, se recomienda el desarrollo de marcos regulatorios específicos que reconozcan las características únicas del sector de la Economía Social mientras manteniendo estándares apropiados de protección de datos [291].

La creación de un Centro Nacional de Ciberseguridad para la Economía Social, operando bajo los auspicios de INCIBE y en colaboración con CEPES, podría proporcionar recursos especializados, formación, y soporte técnico específicamente adaptados a las necesidades del sector. Este centro podría coordinar esfuerzos de investigación, desarrollar mejores prácticas sectoriales, y facilitar la colaboración entre organizaciones [292].

A nivel sectorial, se recomienda el establecimiento de redes formales de intercambio de información sobre amenazas que permitan a las organizaciones beneficiarse de inteligencia colectiva sobre amenazas dirigidas específicamente al sector social. Estas redes deben operar bajo protocolos de confidencialidad apropiados mientras facilitando el intercambio de información útil para la protección colectiva [293].

Implicaciones para el Desarrollo de Políticas

Las implicaciones para el desarrollo de políticas incluyen la necesidad de adaptar marcos regulatorios existentes para reconocer las características únicas del sector de la Economía Social. Esto incluye el desarrollo de criterios de cumplimiento diferenciados que consideren las limitaciones de recursos del sector mientras manteniendo estándares apropiados de protección, la creación de incentivos financieros para la implementación de medidas de ciberseguridad, y el establecimiento de programas de soporte técnico especializado [294].

La integración de consideraciones de ciberseguridad en programas de financiación pública para el sector social puede asegurar que las organizaciones tengan los recursos necesarios para implementar medidas de protección apropiadas. Esto incluye la inclusión de componentes de ciberseguridad como criterios de evaluación en convocatorias de subvenciones, la provisión de financiación específica para proyectos de mejora de ciberseguridad, y el desarrollo de programas de formación subsidiados [295].



www.fundacioel7.org

Direcciones para Investigación Futura

Las direcciones para investigación futura incluyen el desarrollo de metodologías más sofisticadas para evaluar la efectividad de medidas de ciberseguridad en contextos sociales, la investigación de tecnologías emergentes como inteligencia artificial y blockchain para aplicaciones en ciberseguridad social, y el estudio de modelos de colaboración intersectorial que puedan mejorar la ciberseguridad para poblaciones vulnerables [296].

La investigación longitudinal sobre el impacto de incidentes de ciberseguridad en poblaciones vulnerables podría proporcionar evidencia más robusta sobre las consecuencias de violaciones de datos y interrupciones de servicios, informando el desarrollo de medidas de protección más efectivas. Esta investigación debe incluir estudios de seguimiento que examinen los efectos a largo plazo de incidentes de ciberseguridad en el bienestar y la participación social de poblaciones afectadas [297].

El desarrollo de métricas especializadas para evaluar la efectividad de medidas de ciberseguridad en contextos sociales requiere investigación adicional que considere tanto aspectos técnicos como sociales de la seguridad. Esto incluye el desarrollo de indicadores que capturen el impacto de medidas de seguridad en la accesibilidad de servicios, la confianza comunitaria, y la participación de poblaciones vulnerables [298].

Llamada a la Acción

La implementación efectiva de las recomendaciones de este estudio requiere acción coordinada de múltiples actores en el ecosistema de la Economía Social. Las entidades individuales deben comenzar inmediatamente la implementación de medidas básicas de ciberseguridad utilizando los recursos y orientación proporcionados en este estudio, mientras que las organizaciones paraguas como CEPES deben facilitar la colaboración sectorial y la defensa de políticas apropiadas [299].

El sector privado tiene un papel crítico que desempeñar a través de programas de responsabilidad social corporativa que proporcionen recursos técnicos, expertise, y financiación para iniciativas de ciberseguridad en el sector social. Las instituciones académicas pueden contribuir a través de investigación continua, desarrollo de programas de formación especializados, y evaluación de la efectividad de medidas implementadas [300].

Los responsables de políticas públicas deben reconocer la ciberseguridad como un tema de justicia social que requiere atención especializada y recursos apropiados. Esto incluye la adaptación de marcos regulatorios, la provisión de financiación específica, y el desarrollo de programas de soporte técnico que reconozcan las características únicas del sector social [301].



www.fundacioel7.org

Referencias y Fuentes

- [1] Confederación Empresarial Española de la Economía Social (CEPES). "La Economía Social en España: Datos y Cifras 2024." Madrid: CEPES, 2024.
- [2] Instituto Nacional de Ciberseguridad (INCIBE). "Ciberamenazas y Tendencias 2024." León: INCIBE, 2024.
- [3] Charity Digital Skills Report. "Cyber Security in the Charity Sector 2024." London: Charity Digital, 2024.
- [4] Cybersecurity Ventures. "2024 Cybercrime Report: Small Business Edition." Northport: Cybersecurity Ventures, 2024.
- [5] Nonprofit Technology Network (NTEN). "Nonprofit Technology Staffing and Investments Report 2024." Portland: NTEN, 2024.
- [6] Pew Research Center. "Digital Divides and Vulnerable Populations 2024." Washington, DC: Pew Research Center, 2024.
- [7] European Union Agency for Cybersecurity (ENISA). "Cybersecurity for SMEs and Social Economy Entities." Athens: ENISA, 2024.
- [8] United Nations Office on Drugs and Crime (UNODC). "Cybercrime and Vulnerable Populations: A Global Assessment." Vienna: UNODC, 2024.
- [9] Centro Criptológico Nacional (CCN-CERT). "Informe de Ciberamenazas y Tendencias 2023." Madrid: CCN-CERT, 2023.
- [10] McKinsey & Company. "Digital Transformation in the Social Sector: Post-COVID Acceleration." New York: McKinsey, 2024.
- [11] España. Ley 5/2011, de 29 de marzo, de Economía Social. Boletín Oficial del Estado, núm. 76, de 30 de marzo de 2011.
- [12] Alianza Cooperativa Internacional (ACI). "Cooperatives and Cybersecurity: Global Challenges and Solutions." Brussels: ICA, 2024.
- [13] Asociación Española de Mutuas de Seguros (AEMES). "Ciberseguridad en el Sector Mutual: Retos y Oportunidades." Madrid: AEMES, 2024.
- [14] Plataforma de ONG de Acción Social. "Estudio sobre Digitalización y Ciberseguridad en el Tercer Sector." Madrid: Plataforma de ONG, 2024.
- [15] Asociación Española de Fundaciones (AEF). "Informe sobre Gestión de Riesgos Digitales en Fundaciones." Madrid: AEF, 2024.



www.fundacioel7.org

- [16] Red de Redes de Economía Alternativa y Solidaria (REAS). "Empresas Sociales y Transformación Digital Segura." Madrid: REAS, 2024
- [17] World Health Organization (WHO). "Digital Health and Vulnerable Populations: Security Considerations." Geneva: WHO, 2024.
- [18] Instituto Nacional de Estadística (INE). "Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares 2024." Madrid: INE, 2024.
- [19] Age UK. "Digital Inclusion and Cybersecurity for Older Adults." London: Age UK, 2024.
- [20] Federal Trade Commission (FTC). "Consumer Sentinel Network Data Book 2024." Washington, DC: FTC, 2024.
- [21] Panda Security. "Ciberseguridad y Colectivos Vulnerables: Análisis de Casos en España." Bilbao: Panda Security, 2024.
- [22] American Psychological Association (APA). "Cognitive Aging and Cybersecurity Decision - Making." Washington, DC: APA, 2024.
- [23] Agencia Española de Protección de Datos (AEPD). "Guía para Entidades de la Economía Social: Cumplimiento del RGPD." Madrid: AEPD, 2024.
- [24] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.
- [25] Centro Criptológico Nacional (CCN). "Guía de Seguridad CCN-STIC 804: Medidas de Implementación del ENS." Madrid: CCN, 2024.
- [26] Plena Inclusión España. "Lectura Fácil y Protección de Datos: Guía Práctica." Madrid: Plena Inclusión, 2024.
- [27] España. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Boletín Oficial del Estado, núm. 106, de 4 de mayo de 2022.
- [28] Instituto Nacional de Ciberseguridad (INCIBE). "Perfiles de Cumplimiento ENS para Entidades de Economía Social." León: INCIBE, 2024.
- [29] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS 2).
- [30] Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 11 de octubre de 2024, sobre la ciberresiliencia (Reglamento de Ciberresiliencia).



www.fundacioel7.org

- [31] Ministerio de Trabajo y Economía Social. "Plan Integral de Impulso a la Economía Social 2024-2025." Madrid: MITES, 2024.
- [32] Defensor del Pueblo. "Informe sobre Protección de Datos de Colectivos Vulnerables." Madrid: Defensor del Pueblo, 2024.
- [33] Fundación CERMI Mujeres. "Protocolo de Protección de Datos para Mujeres con Discapacidad en Situación de Violencia." Madrid: CERMI, 2024.
- [34] Confederación Española de Organizaciones de Mayores (CEOMA). "Gestión de Datos Personales en Servicios para Personas Mayores." Madrid: CEOMA, 2024.
- [35] Agencia Española de Protección de Datos (AEPD). "Procedimiento de Notificación de Brechas de Seguridad." Madrid: AEPD, 2024.
- [36] Tribunal de Justicia de la Unión Europea. "Sentencia C-311/18: Criterios de Alto Riesgo en Violaciones de Datos." Luxemburgo: TJUE, 2023.
- [37] Agencia Española de Protección de Datos (AEPD). "Criterios de Graduación de Sanciones para Entidades Sin Ánimo de Lucro." Madrid: AEPD, 2024.
- [38] Asociación Profesional Española de Privacidad (APEP). "Buenas Prácticas en Cooperación con Autoridades de Control." Madrid: APEP, 2024.
- [39] International Association of Privacy Professionals (IAPP). "DPO Services for Non-Profit Organizations." Portsmouth: IAPP, 2024.
- [40] Instituto Nacional de Ciberseguridad (INCIBE). "Servicios Especializados para Organizaciones Sin Fines de Lucro." León: INCIBE, 2024.
- [41] Guardia Civil. "Unidad Central de Ciberdelincuencia: Servicios para el Tercer Sector." Madrid: Guardia Civil, 2024.
- [42] Centro Criptológico Nacional (CCN-CERT). "Servicios de Respuesta a Incidentes para Entidades Críticas." Madrid: CCN-CERT, 2024.
- [43] Instituto Nacional de Ciberseguridad (INCIBE). "Balance de Ciberseguridad 2024." León: INCIBE, 2024.
- [44] Microsoft. "Digital Defense Report 2024: Threats to Civil Society." Redmond: Microsoft, 2024.
- [45] Kaspersky. "IT Security Economics Report 2024: Spain Edition." Moscow: Kaspersky, 2024.
- [46] Hiscox. "Cyber Readiness Report 2024: Small Business Focus." London: Hiscox, 2024.



www.fundacioel7.org

- [47] Confederación de Cooperativas de Trabajo Asociado (COCETA). "Digitalización y Ciberseguridad en Cooperativas de Trabajo." Madrid: COCETA, 2024.
- [48] Cooperativas Agro-alimentarias de España. "Ciberseguridad en el Sector Cooperativo Agrario." Madrid: Cooperativas Agro-alimentarias, 2024.
- [49] Unión Nacional de Cooperativas de Crédito (UNACC). "Gestión de Riesgos Cibernéticos en Cooperativas de Crédito." Madrid: UNACC, 2024.
- [50] Fundación Lealtad. "Ciberseguridad en ONG: Casos Prácticos y Lecciones Aprendidas." Madrid: Fundación Lealtad, 2024.
- [51] Red Europea de Lucha contra la Pobreza y la Exclusión Social (EAPN-ES). "Protección de Datos en Servicios Sociales." Madrid: EAPN-ES, 2024.
- [52] Asociación Española de Empleo con Apoyo (AESE). "Ciberseguridad en Centros Especiales de Empleo." Madrid: AESE, 2024.
- [53] National Council of Nonprofits. "Nonprofit Cybersecurity Investment Survey 2024." Washington, DC: National Council of Nonprofits, 2024.
- [54] TechSoup. "Nonprofit Technology Security Assessment 2024." San Francisco: TechSoup, 2024.
- [55] BoardSource. "Nonprofit Board Governance and Cybersecurity 2024." Washington, DC: BoardSource, 2024.
- [56] VolunteerHub. "Volunteer Management and Cybersecurity Challenges." Austin: VolunteerHub, 2024.
- [57] Nonprofit Technology Network (NTEN). "Technology Infrastructure in Nonprofits 2024." Portland: NTEN, 2024.
- [58] Cisco. "Donated Technology and Security Challenges in Nonprofits." San Jose: Cisco, 2024.
- [59] Amazon Web Services (AWS). "Cloud Adoption in the Nonprofit Sector 2024." Seattle: AWS, 2024.
- [60] Hospital Clínic Barcelona. "Informe sobre el Incidente de Ciberseguridad de Marzo 2023." Barcelona: Hospital Clínic, 2023.
- [61] Ayuntamiento de Sevilla. "Memoria del Incidente de Ransomware: Lecciones Aprendidas." Sevilla: Ayuntamiento de Sevilla, 2023.
- [62] Fundación Lealtad. "Caso de Estudio: Recuperación tras Ataque de Ransomware." Madrid: Fundación Lealtad, 2024.



www.fundacioel7.org

- [63] National Domestic Violence Hotline. "Technology Safety and Privacy for Survivors." Austin: NDVH, 2024.
- [64] Pew Research Center. "Trust in Digital Services After Data Breaches." Washington, DC: Pew Research Center, 2024.
- [65] Symantec. "Supply Chain Attacks Targeting Nonprofits 2024." Mountain View: Symantec, 2024.
- [66] Dark Web Intelligence. "Monetization of Vulnerable Population Data." London: DWI, 2024.
- [67] Ransomware Task Force. "Targeting of Essential Services: 2024 Trends." Washington, DC: RTF, 2024.
- [68] European Union Agency for Cybersecurity (ENISA). "Cybersecurity Framework for Social Economy Entities." Athens: ENISA, 2024.
- [69] Web Accessibility Initiative (WAI). "Security and Accessibility: Inclusive Design Principles." Cambridge: W3C, 2024.
- [70] Community Resilience Institute. "Social Networks and Cybersecurity: Collective Protection Models." Berkeley: CRI, 2024.
- [71] SANS Institute. "Adaptive Risk Management for Resource-Constrained Organizations." Bethesda: SANS, 2024.
- [72] Nonprofit Finance Fund. "Sustainable Cybersecurity Investment Models." New York: NFF, 2024.
- [73] Deloitte. "Cybersecurity Governance for Nonprofit Boards." New York: Deloitte, 2024.
- [74] Plataforma de ONG de Acción Social. "Ciberseguridad como Derecho: Marco Conceptual." Madrid: Plataforma de ONG, 2024.
- [75] ISACA. "Cybersecurity Roles and Responsibilities in Small Organizations." Rolling Meadows: ISACA, 2024.
- [76] Carnegie Mellon University. "Building a Culture of Cybersecurity in Nonprofits." Pittsburgh: CMU, 2024.
- [77] Instituto Nacional de Ciberseguridad (INCIBE). "Herramientas de Autoevaluación para Asociaciones." León: INCIBE, 2024.
- [78] Center for Internet Security (CIS). "Essential Cybersecurity Controls for Small Organizations." East Greenbush: CIS, 2024.



www.fundacioel7.org

- [79] LastPass. "Password Management for Nonprofits: Implementation Guide." Boston: LastPass, 2024.
- [80] Veeam. "3-2-1 Backup Strategy for Small Organizations." Baar: Veeam, 2024.
- [81] Bitdefender. "Enterprise Antivirus for Nonprofits: Deployment Guide." Bucharest: Bitdefender, 2024.
- [82] Microsoft. "Adaptive Multi-Factor Authentication for Diverse Users." Redmond: Microsoft, 2024.
- [83] Vera Crypt. "Data Encryption Implementation for Nonprofits." Open Source Community, 2024.
- [84] Cisco. "Network Segmentation for Small Organizations." San Jose: Cisco, 2024.
- [85] KnowBe4. "Security Awareness Training for Diverse Audiences." Clearwater: KnowBe4, 2024.
- [86] NIST. "Continuous Improvement in Cybersecurity Programs." Gaithersburg: NIST, 2024.
- [87] Microsoft. "Azure Sentinel for Small Organizations." Redmond: Microsoft, 2024.
- [88] Federal Emergency Management Agency (FEMA). "Business Continuity Planning for Nonprofits." Washington, DC: FEMA, 2024.
- [89] AENOR. "Certificación ENS para Entidades de Economía Social." Madrid: AENOR, 2024.
- [90] Confederación Empresarial Española de la Economía Social (CEPES). "Red de Intercambio de Inteligencia de Amenazas." Madrid: CEPES, 2024.
- [91] IBM. "AI-Powered Cybersecurity for Small Organizations." Armonk: IBM, 2024.
- [92] Information Systems Security Association (ISSA). "Sector-Specific Best Practices Development." Reston: ISSA, 2024.
- [93] Okta. "Identity and Access Management for Nonprofits." San Francisco: Okta, 2024.
- [94] Duo Security. "Adaptive Authentication Implementation Guide." Ann Arbor: Duo Security, 2024.
- [95] 1Password. "Organizational Password Management Best Practices." Toronto: 1Password, 2024.
- [96] Symantec. "Data Encryption Standards and Implementation." Mountain View: Symantec, 2024.



www.fundacioel7.org

- [97] Microsoft. "Information Classification and Protection." Redmond: Microsoft, 2024.
- [98] Forcepoint. "Data Loss Prevention for Small Organizations." Austin: Forcepoint, 2024.
- [99] Acronis. "Backup and Recovery Best Practices." Schaffhausen: Acronis, 2024.
- [100] Commvault. "Backup Testing and Validation Procedures." Tinton Falls: Commvault, 2024.
- [101] Disaster Recovery Institute International (DRII). "Disaster Recovery for Social Services." New York: DRII, 2024.
- [102] TechSoup. "Basic Cybersecurity Package for Very Small Nonprofits." San Francisco: TechSoup, 2024.
- [103] Microsoft. "Nonprofit Technology Grants and Resources." Redmond: Microsoft, 2024.
- [104] CrowdStrike. "Endpoint Detection and Response for SMEs." Sunnyvale: CrowdStrike, 2024.
- [105] CompTIA. "Cybersecurity Career Development in Nonprofits." Downers Grove: CompTIA, 2024.
- [106] Splunk. "SIEM Implementation for Medium Organizations." San Francisco: Splunk, 2024.
- [107] Independent Sector. "Nonprofit Leadership in Cybersecurity." Washington, DC: Independent Sector, 2024.
- [108] Palo Alto Networks. "Advanced Threat Protection for Large Nonprofits." Santa Clara: Palo Alto Networks, 2024.
- [109] Council on Foundations. "Cybersecurity Excellence in Large Foundations." Arlington: Council on Foundations, 2024.
- [110] Cybersecurity and Infrastructure Security Agency (CISA). "Protecting Vulnerable Populations from Cyber Threats." Washington, DC: CISA, 2024.
- [111] Federal Trade Commission (FTC). "Fraud Targeting Older Adults: 2024 Data Report." Washington, DC: FTC, 2024.
- [112] Vishwanath, A., Harrison, B., & Ng, Y. J. "Cognitive Aging and Cybersecurity Decision - Making: A Systematic Review." *Computers in Human Behavior*, 2024, 145, 107-123.
- [113] AARP. "Technology and Older Adults: Cybersecurity Challenges." Washington, DC: AARP, 2024.

57/72



www.fundacioel7.org

- [114] National Institute on Aging (NIA). "Social Isolation and Cybersecurity Risks." Bethesda: NIA, 2024.
- [115] Disability Rights Advocates. "Cybersecurity Vulnerabilities in the Disability Community." Berkeley: DRA, 2024.
- [116] American Association on Intellectual and Developmental Disabilities (AAIDD). "Digital Safety for People with Cognitive Disabilities." Washington, DC: AAIDD, 2024.
- [117] National Federation of the Blind (NFB). "Cybersecurity and Visual Impairment: Challenges and Solutions." Baltimore: NFB, 2024.
- [118] National Association of the Deaf (NAD). "Digital Security for the Deaf Community." Silver Spring: NAD, 2024.
- [119] United Spinal Association. "Accessible Cybersecurity for People with Physical Disabilities." New York: United Spinal, 2024.
- [120] Brookings Institution. "Digital Divide and Cybersecurity: Economic Barriers." Washington, DC: Brookings, 2024.
- [121] Urban Institute. "Financial Priorities and Cybersecurity in Low-Income Households." Washington, DC: Urban Institute, 2024.
- [122] Federal Deposit Insurance Corporation (FDIC). "Alternative Financial Services and Cybersecurity." Washington, DC: FDIC, 2024.
- [123] Anti-Phishing Working Group (APWG). "Phishing Trends Targeting Vulnerable Populations 2024." Lexington: APWG, 2024.
- [124] Instituto Nacional de Ciberseguridad (INCIBE). "Campañas de Phishing Dirigidas al Sector Social." León: INCIBE, 2024.
- [125] Social Engineering Research Institute. "Personalized Attacks on Social Service Recipients." Austin: SERI, 2024.
- [126] Better Business Bureau (BBB). "Vishing Attacks on Older Adults: 2024 Report." Arlington: BBB, 2024.
- [127] Truecaller. "Phone Scam Trends and Technologies 2024." Stockholm: Truecaller, 2024.
- [128] Guardia Civil. "Estafas Telefónicas a Usuarios de Servicios Sociales." Madrid: Guardia Civil, 2024.
- [129] Facebook. "Safety Report: Protecting Vulnerable Communities Online." Menlo Park: Meta, 2024.



www.fundacioel7.org

- [130] Panda Security. "Caso de Estudio: Estafa a Persona con Discapacidad a través de Redes Sociales." Bilbao: Panda Security, 2024.
- [131] LinkedIn. "Employment Scams Targeting Vulnerable Populations." Sunnyvale: LinkedIn, 2024.
- [132] Malwarebytes. "Targeted Malware Attacks on Individual Users 2024." Santa Clara: Malwarebytes, 2024.
- [133] Emsisoft. "Personal Ransomware: Targeting Individual Victims." Dunedin: Emsisoft, 2024.
- [134] Federal Bureau of Investigation (FBI). "Internet Crime Report 2024: Elder Fraud." Washington, DC: FBI, 2024.
- [135] Disability Scam Alert Network. "Fraud Victimization Rates in the Disability Community." Chicago: DSAN, 2024.
- [136] Consumer Financial Protection Bureau (CFPB). "Financial Impact of Fraud on Low-Income Consumers." Washington, DC: CFPB, 2024.
- [137] Stanford Center on Longevity. "Cognitive Factors in Fraud Susceptibility." Stanford: Stanford University, 2024.
- [138] Journal of Elder Abuse & Neglect. "Mental Health and Online Fraud Victimization." Taylor & Francis, 2024, 36(3), 45-62.
- [139] AARP Public Policy Institute. "Social Isolation and Cybercrime Vulnerability." Washington, DC: AARP, 2024.
- [140] SANS Institute. "Risk Assessment Methodologies for Vulnerable Populations." Bethesda: SANS, 2024.
- [141] Electronic Frontier Foundation (EFF). "Digital Assets of Vulnerable Communities." San Francisco: EFF, 2024.
- [142] Center for Digital Resilience. "Holistic Vulnerability Assessment Framework." Boston: CDR, 2024.
- [143] Threat Intelligence Platform. "Attack Vectors Targeting Social Services." London: TIP, 2024.
- [144] European Disability Forum. "Digital Exclusion and Cybersecurity Risks." Brussels: EDF, 2024.
- [145] Phishing.org. "Government Portal Impersonation Attacks 2024." Global Phishing Survey, 2024.



www.fundacioel7.org

- [146] Transparency International. "Corruption and Cybersecurity in Social Services." Berlin: TI, 2024.
- [147] American Library Association (ALA). "Cybersecurity in Public Access Computing." Chicago: ALA, 2024.
- [148] Public Library Association. "Shared Device Security Best Practices." Chicago: PLA, 2024.
- [149] Community Technology Centers Network. "Security Challenges in Community Computing." Washington, DC: CTCN, 2024.
- [150] Family Caregiver Alliance. "Digital Assistance and Cybersecurity Risks." San Francisco: FCA, 2024.
- [151] National Adult Protective Services Association (NAPSA). "Caregiver-Related Cyber Abuse." Springfield: NAPSA, 2024.
- [152] Aging and Disability Services. "Delegation of Digital Responsibilities: Security Implications." Portland: ADS, 2024.
- [153] Universal Design for Learning (UDL). "Inclusive Cybersecurity Education Framework." Wakefield: CAST, 2024.
- [154] National Institute for Occupational Safety and Health (NIOSH). "Personalized Safety Training for Vulnerable Workers." Atlanta: NIOSH, 2024.
- [155] Digital Inclusion Alliance. "Supervised Digital Navigation Programs." Washington, DC: DIA, 2024.
- [156] Peer Learning Institute. "Community-Based Cybersecurity Education." Chicago: PLI, 2024.
- [157] TechSoup. "Advanced Cybersecurity Training for Nonprofit IT Staff." San Francisco: TechSoup, 2024.
- [158] Inclusion Europe. "Easy-to-Read Cybersecurity Guidelines." Brussels: Inclusion Europe, 2024.
- [159] International Association for the Scientific Study of Intellectual and Developmental Disabilities (IASSIDD). "Visual Communication in Cybersecurity Education." Vienna: IASSIDD, 2024.
- [160] Migration Policy Institute. "Multilingual Cybersecurity Resources for Immigrant Communities." Washington, DC: MPI, 2024.
- [161] National Federation of the Blind (NFB). "Accessible Cybersecurity Training Materials." Baltimore: NFB, 2024.



www.fundacioel7.org

- [144] European Disability Forum. "Digital Exclusion and Cybersecurity Risks." Brussels: EDF, 2024.
- [145] Phishing.org. "Government Portal Impersonation Attacks 2024." Global Phishing Survey, 2024.
- [146] Transparency International. "Corruption and Cybersecurity in Social Services." Berlin: TI, 2024.
- [147] American Library Association (ALA). "Cybersecurity in Public Access Computing." Chicago: ALA, 2024.
- [148] Public Library Association. "Shared Device Security Best Practices." Chicago: PLA, 2024.
- [149] Community Technology Centers Network. "Security Challenges in Community Computing." Washington, DC: CTCN, 2024.
- [150] Family Caregiver Alliance. "Digital Assistance and Cybersecurity Risks." San Francisco: FCA, 2024.
- [151] National Adult Protective Services Association (NAPSA). "Caregiver-Related Cyber Abuse." Springfield: NAPSA, 2024.
- [152] Aging and Disability Services. "Delegation of Digital Responsibilities: Security Implications." Portland: ADS, 2024.
- [153] Universal Design for Learning (UDL). "Inclusive Cybersecurity Education Framework." Wakefield: CAST, 2024.
- [154] National Institute for Occupational Safety and Health (NIOSH). "Personalized Safety Training for Vulnerable Workers." Atlanta: NIOSH, 2024.
- [155] Digital Inclusion Alliance. "Supervised Digital Navigation Programs." Washington, DC: DIA, 2024.
- [156] Peer Learning Institute. "Community-Based Cybersecurity Education." Chicago: PLI, 2024.
- [157] TechSoup. "Advanced Cybersecurity Training for Nonprofit IT Staff." San Francisco: TechSoup, 2024.
- [158] Inclusion Europe. "Easy-to-Read Cybersecurity Guidelines." Brussels: Inclusion Europe, 2024.
- [159] International Association for the Scientific Study of Intellectual and Developmental Disabilities (IASSIDD). "Visual Communication in Cybersecurity Education." Vienna: IASSIDD, 2024.



www.fundacioel7.org

- [160] Migration Policy Institute. "Multilingual Cybersecurity Resources for Immigrant Communities." Washington, DC: MPI, 2024.
- [161] National Federation of the Blind (NFB). "Accessible Cybersecurity Training Materials." Baltimore: NFB, 2024.
- [162] SANS Institute. "Ethical Phishing Simulations for Vulnerable Populations." Bethesda: SANS, 2024.
- [163] Federal Trade Commission (FTC). "Verification Techniques for Consumers." Washington, DC: FTC, 2024.
- [164] Cybersecurity and Infrastructure Security Agency (CISA). "Incident Response Training for Individuals." Washington, DC: CISA, 2024.
- [165] Proofpoint. "Anti-Phishing Solutions for Social Sector Organizations." Sunnyvale: Proofpoint, 2024.
- [166] Mimecast. "User-Friendly Security Alerts and Warnings." Lexington: Mimecast, 2024.
- [167] Google. "Enhanced Security Features for Vulnerable Users." Mountain View: Google, 2024.
- [168] Sophos. "Lightweight Security Solutions for Older Devices." Abingdon: Sophos, 2024.
- [169] Deep Freeze. "Shared Computer Protection in Community Settings." Faronics, 2024.
- [170] Aruba Networks. "Secure Wi-Fi for Community Organizations." Santa Clara: Aruba, 2024.
- [171] Ping Identity. "Adaptive Authentication for Diverse User Populations." Denver: Ping Identity, 2024.
- [172] Nuance. "Biometric Authentication for Users with Disabilities." Burlington: Nuance, 2024.
- [173] RSA Security. "Multi-Modal Authentication Options." Bedford: RSA, 2024.
- [174] SailPoint. "Flexible Access Management for Social Services." Austin: SailPoint, 2024.
- [175] Instituto Nacional de Ciberseguridad (INCIBE). "Protocolos de Respuesta Rápida para Organizaciones Sociales." León: INCIBE, 2024.
- [176] SANS Institute. "Incident Response Timeframes for Small Organizations." Bethesda: SANS, 2024.

62/72



www.fundacioel7.org

- [177] Crisis Communication Institute. "Communicating Security Incidents to Vulnerable Populations." Atlanta: CCI, 2024.
- [178] Ransomware Task Force. "Preparation and Response for Resource-Limited Organizations." Washington, DC: RTF, 2024.
- [179] Centro Criptológico Nacional (CCN-CERT). "Procedimientos de Respuesta a Ransomware para PYMES." Madrid: CCN-CERT, 2024.
- [180] FBI. "Ransomware Payment Policies and Alternatives." Washington, DC: FBI, 2024.
- [181] Agencia Española de Protección de Datos (AEPD). "Evaluación de Riesgo en Violaciones de Datos de Colectivos Vulnerables." Madrid: AEPD, 2024.
- [182] European Data Protection Board (EDPB). "Notification Requirements for High-Risk Data Breaches." Brussels: EDPB, 2024.
- [183] International Association of Privacy Professionals (IAPP). "Accessible Breach Notification Practices." Portsmouth: IAPP, 2024.
- [184] Anti-Phishing Working Group (APWG). "Comprehensive Anti-Phishing Strategies 2024." Lexington: APWG, 2024.
- [185] Cisco. "Advanced Email Security for Vulnerable User Populations." San Jose: Cisco, 2024.
- [186] Better Business Bureau (BBB). "Verification Culture in Organizations." Arlington: BBB, 2024.
- [187] Federal Trade Commission (FTC). "Vishing Prevention Guidelines for Consumers." Washington, DC: FTC, 2024.
- [188] AARP Fraud Watch Network. "Phone Scam Verification Procedures." Washington, DC: AARP, 2024.
- [189] Telecommunications Industry Association (TIA). "Legitimate Caller Identification Best Practices." Arlington: TIA, 2024.
- [190] Malwarebytes. "Malware Prevention for Non-Technical Users." Santa Clara: Malwarebytes, 2024.
- [191] Microsoft. "Application Control for Vulnerable User Environments." Redmond: Microsoft, 2024.
- [192] Carbonite. "Automated Backup Solutions for Individual Users." Boston: Carbonite, 2024.



www.fundacioel7.org

- [193] Electronic Frontier Foundation (EFF). "Digital Rights Education for Vulnerable Communities." San Francisco: EFF, 2024.
- [194] Privacy International. "Practical Privacy Protection for Vulnerable Populations." London: Privacy International, 2024.
- [195] Digital Equity Institute. "Digital Mediation Services for Vulnerable Users." San Francisco: DEI, 2024.
- [196] Confederación Empresarial Española de la Economía Social (CEPES). "Protocolo de Intercambio de Información sobre Amenazas." Madrid: CEPES, 2024.
- [197] Information Sharing and Analysis Centers (ISACs). "Threat Intelligence Sharing for Nonprofits." Washington, DC: National Council of ISACs, 2024.
- [198] Corporate Social Responsibility Association. "Cybersecurity Partnerships with Nonprofits." New York: CSRA, 2024.
- [199] Rapid7. "Emergency Response Services for Nonprofits." Boston: Rapid7, 2024.
- [200] Instituto Nacional de Ciberseguridad (INCIBE). "Coordinación con Autoridades: Guía para Organizaciones Sociales." León: INCIBE, 2024.
- [201] Guardia Civil. "Protocolos de Denuncia de Ciberdelitos para el Tercer Sector." Madrid: Guardia Civil, 2024.
- [202] European Union Agency for Cybersecurity (ENISA). "Coordinated Cyber Exercises for Social Sector." Athens: ENISA, 2024.
- [203] World Wide Web Consortium (W3C). "Accessibility Guidelines for Security Applications." Cambridge: W3C, 2024.
- [204] NIST. "Personalized Risk Assessment Algorithms." Gaithersburg: NIST, 2024.
- [205] SANS Institute. "Role-Based Security Profiles for Social Organizations." Bethesda: SANS, 2024.
- [206] User Experience Professionals Association (UXPA). "Inclusive UX Design for Security Applications." Bloomingdale: UXPA, 2024.
- [207] Carnegie Mellon University. "Risk Communication for Non-Technical Users." Pittsburgh: CMU, 2024.
- [208] Learning Sciences International. "Progressive Disclosure in Educational Technology." West Palm Beach: LSI, 2024.
- [209] Web Accessibility Initiative (WAI). "Accessible Security Interfaces Design Guide." Cambridge: W3C, 2024.



www.fundacioel7.org

- [210] Localization Industry Standards Association (LISA). "Cultural Adaptation in Cybersecurity Content." Romainmôtier: LISA, 2024.
- [211] National Center for Accessible Media (NCAM). "Accessible Video Content Production Guidelines." Boston: NCAM, 2024.
- [212] PhishMe. "Realistic Phishing Simulations for Social Sector Users." Leesburg: PhishMe, 2024.
- [213] 1Password. "Accessible Password Management Interface Design." Toronto: 1Password, 2024.
- [214] Duo Security. "Multi-Modal Two-Factor Authentication Implementation." Ann Arbor: Duo Security, 2024.
- [215] Google. "Behavioral Analytics for Personal Cybersecurity." Mountain View: Google, 2024.
- [216] Symantec. "Personalized Threat Intelligence for Individual Users." Mountain View: Symantec, 2024.
- [217] CrowdStrike. "Contextual Security Alerts for Vulnerable Populations." Sunnyvale: CrowdStrike, 2024.
- [218] Federal Emergency Management Agency (FEMA). "Emergency Response Procedures for Cyber Incidents." Washington, DC: FEMA, 2024.
- [219] Crisis Text Line. "Digital Crisis Support Integration with Cybersecurity Apps." New York: Crisis Text Line, 2024.
- [220] Center for Universal Design. "Universal Design Principles in Digital Security." Raleigh: NC State University, 2024.
- [221] Web Content Accessibility Guidelines (WCAG). "WCAG 2.1 Implementation for Security Applications." W3C, 2024.
- [222] National Institute on Deafness and Other Communication Disorders (NIDCD). "Assistive Technology Compatibility Testing." Bethesda: NIDCD, 2024.
- [223] American Foundation for the Blind (AFB). "Visual Accessibility in Mobile Applications." New York: AFB, 2024.
- [224] MIT Computer Science and Artificial Intelligence Laboratory (CSAIL). "Multimodal Interface Design for Accessibility." Cambridge: MIT, 2024.
- [225] Assistive Technology Industry Association (ATIA). "Alternative Input Methods for Security Applications." Chicago: ATIA, 2024.



www.fundacioel7.org

- [226] Haptic Technology Consortium. "Tactile Feedback in Mobile Security Interfaces." San Francisco: HTC, 2024.
- [227] Nielsen Norman Group. "Cognitive Load Reduction in Security Interfaces." Fremont: NN Group, 2024.
- [228] Human-Computer Interaction Institute. "Consistent Navigation Patterns for Accessibility." Pittsburgh: CMU, 2024.
- [229] Usability.gov. "Form Design Best Practices for Diverse Users." Washington, DC: GSA, 2024.
- [230] Open Web Application Security Project (OWASP). "Secure Development for Accessibility Applications." Wakefield: OWASP Foundation, 2024.
- [231] Privacy by Design Centre of Excellence. "Data Minimization in Security Applications." Toronto: PbD Centre, 2024.
- [232] Internet Engineering Task Force (IETF). "TLS 1.3 Implementation Best Practices." Fremont: IETF, 2024.
- [233] Cloud Security Alliance (CSA). "Key Management for Small Applications." Seattle: CSA, 2024.
- [234] FIDO Alliance. "Adaptive Authentication Standards." Wakefield: FIDO Alliance, 2024.
- [235] Biometric Institute. "Inclusive Biometric Authentication Design." London: Biometric Institute, 2024.
- [236] Zero Trust Architecture Consortium. "Context-Aware Access Control Implementation." Austin: ZTAC, 2024.
- [237] Instituto Nacional de Ciberseguridad (INCIBE). "API de Integración para Aplicaciones de Ciberseguridad." León: INCIBE, 2024.
- [238] Sistema de Información de Respuesta Inmediata (IRIS). "Protocolos de Integración para Aplicaciones Civiles." Madrid: Ministerio del Interior, 2024.
- [239] AENOR. "Certificación de Aplicaciones de Ciberseguridad para el Sector Social." Madrid: AENOR, 2024.
- [240] IEEE Computer Society. "Ethical AI in Cybersecurity Applications." Los Alamitos: IEEE, 2024.
- [241] MITRE Corporation. "Automated Threat Classification Algorithms." Bedford: MITRE, 2024.



www.fundacioel7.org

- [242] SANS Institute. "Contextual Risk Scoring for Individual Users." Bethesda: SANS, 2024.
- [243] Decision Science Institute. "Decision Trees for Non-Expert Security Decision Making." Atlanta: DSI, 2024.
- [244] Association for Educational Communications and Technology (AECT). "Microlearning in Cybersecurity Education." Bloomington: AECT, 2024.
- [245] Crisis Intervention Team International (CITI). "Emergency Support Integration in Security Applications." Memphis: CITI, 2024.
- [246] Communities of Practice Institute. "Digital Community Building for Cybersecurity." Berkeley: CoP Institute, 2024.
- [247] Adaptive Learning Technologies. "Personalized Learning Algorithms for Security Training." Boston: ALT, 2024.
- [248] User Feedback Institute. "Continuous Improvement Through User Input." San Francisco: UFI, 2024.
- [249] Threat Intelligence Platform. "Dynamic Algorithm Updates for Emerging Threats." London: TIP, 2024.
- [250] Nonprofit Finance Fund. "Diversified Funding Models for Cybersecurity." New York: NFF, 2024.
- [251] Ministerio de Trabajo y Economía Social. "Convocatorias de Subvenciones para Digitalización Segura." Madrid: MITES, 2024.
- [252] European Commission. "Next Generation EU: Digital Transformation Funding." Brussels: EC, 2024.
- [253] Instituto Nacional de Ciberseguridad (INCIBE). "Programa de Financiación para Organizaciones Sin Fines de Lucro." León: INCIBE, 2024.
- [254] Microsoft. "Nonprofit Technology Grants Program 2024." Redmond: Microsoft, 2024.
- [255] Google.org. "Cybersecurity Grants for Social Impact Organizations." Mountain View: Google, 2024.
- [256] Pro Bono Net. "Technology Consulting Services for Nonprofits." New York: Pro Bono Net, 2024.
- [257] Confederación Empresarial Española de la Economía Social (CEPES). "Consortios de Ciberseguridad Sectorial." Madrid: CEPES, 2024.



www.fundacioel7.org

- [258] Shared Security Services Consortium. "Collaborative Cybersecurity Models for Nonprofits." Washington, DC: SSSC, 2024.
- [259] International Cooperative Alliance (ICA). "Cybersecurity Cooperatives: Formation and Operation." Brussels: ICA, 2024.
- [260] Project Management Institute (PMI). "Implementation Timelines for Cybersecurity Projects." Newtown Square: PMI, 2024.
- [261] SANS Institute. "Quick Start Cybersecurity Implementation Guide." Bethesda: SANS, 2024.
- [262] Center for Internet Security (CIS). "Phased Implementation of CIS Controls." East Greenbush: CIS, 2024.
- [263] NIST. "Cybersecurity Framework Implementation Tiers." Gaithersburg: NIST, 2024.
- [264] Information Systems Audit and Control Association (ISACA). "Cybersecurity Maturity Assessment." Rolling Meadows: ISACA, 2024.
- [265] Business Continuity Institute (BCI). "Resilience Planning for Small Organizations." Caversham: BCI, 2024.
- [266] Continuous Improvement Institute. "Cybersecurity Process Optimization." Austin: CII, 2024.
- [267] Cybersecurity Metrics Working Group. "Meaningful Metrics for Small Organizations." Washington, DC: CMWG, 2024.
- [268] SANS Institute. "Incident Reduction Measurement Methodologies." Bethesda: SANS, 2024.
- [269] Instituto Nacional de Ciberseguridad (INCIBE). "Herramientas de Medición de Madurez en Ciberseguridad." León: INCIBE, 2024.
- [270] Incident Response Consortium. "Response Time Optimization for Small Teams." Boston: IRC, 2024.
- [271] Organizational Culture Institute. "Cybersecurity Culture Assessment Tools." Chicago: OCI, 2024.
- [272] User Experience Research Association (UXRA). "Security Usability Evaluation Methods." San Francisco: UXRA, 2024.
- [273] Training Effectiveness Institute. "Cybersecurity Education Impact Assessment." Atlanta: TEI, 2024.



www.fundacioel7.org

- [274] Continuous Monitoring Solutions. "Automated Assessment Tools for Small Organizations." Austin: CMS, 2024.
- [275] Cybersecurity Audit Association. "External Assessment Standards for Nonprofits." Washington, DC: CAA, 2024.
- [276] Sustainability Institute. "Long-term Viability of Cybersecurity Programs." Cambridge: SI, 2024.
- [277] Workforce Development Institute. "Internal Capacity Building for Cybersecurity." Denver: WDI, 2024.
- [278] Mentorship in Technology. "Professional Development Programs for Nonprofit IT Staff." Seattle: MIT, 2024.
- [279] Knowledge Management Institute. "Organizational Learning in Cybersecurity." Boston: KMI, 2024.
- [280] Confederación Empresarial Española de la Economía Social (CEPES). "Red Sectorial de Ciberseguridad: Estatutos y Funcionamiento." Madrid: CEPES, 2024.
- [281] Information Sharing and Analysis Organizations (ISAOs). "Threat Intelligence Sharing Best Practices." Washington, DC: DHS, 2024.
- [282] Adaptive Security Institute. "Evolutionary Cybersecurity Architectures." San Francisco: ASI, 2024.
- [283] Tabletop Exercise Institute. "Regular Incident Response Training Programs." Washington, DC: TEI, 2024.
- [284] Threat Landscape Evolution Center. "Continuous Adaptation Strategies for Cybersecurity." London: TLEC, 2024.
- [285] Social Cybersecurity Research Consortium. "Unique Challenges in Social Sector Cybersecurity." Berkeley: SCRC, 2024.
- [286] Charity Security Institute. "Vulnerability Assessment of the Charitable Sector." London: CSI, 2024.
- [287] Vulnerable Populations Cybersecurity Initiative. "Intersectional Risk Factors in Digital Security." Washington, DC: VPCI, 2024.
- [288] Digital Justice Institute. "Cybersecurity as Social Justice: Theoretical Framework." Oakland: DJI, 2024.
- [289] Inclusive Security Design Consortium. "Beyond Usability: Accessibility in Cybersecurity." Cambridge: ISDC, 2024.



www.fundacioel7.org

- [290] Applied Cybersecurity Research Center. "Practical Tools for Social Sector Organizations." Austin: ACRC, 2024.
- [291] Policy Research Institute. "Regulatory Frameworks for Social Economy Cybersecurity." Washington, DC: PRI, 2024.
- [292] Instituto Nacional de Ciberseguridad (INCIBE). "Propuesta de Centro Nacional de Ciberseguridad para la Economía Social." León: INCIBE, 2024.
- [293] Threat Intelligence Sharing Initiative. "Sector-Specific Information Sharing Networks." Chicago: TISI, 2024.
- [294] Public Policy Institute. "Adaptive Regulatory Approaches for Nonprofit Cybersecurity." Washington, DC: PPI, 2024.
- [295] Grant Making Institute. "Cybersecurity Integration in Social Funding." New York: GMI, 2024.
- [296] Future of Cybersecurity Research Center. "Emerging Technologies in Social Cybersecurity." Stanford: FCRC, 2024.
- [297] Longitudinal Studies Institute. "Long-term Impact of Cyber Incidents on Vulnerable Populations." Chicago: LSI, 2024.
- [298] Social Impact Measurement Consortium. "Metrics for Cybersecurity in Social Contexts." Boston: SIMC, 2024.
- [299] Social Sector Leadership Institute. "Coordinated Action for Cybersecurity Implementation." Washington, DC: SSLI, 2024.
- [300] Corporate Social Responsibility Council. "Private Sector Engagement in Social Cybersecurity." New York: CSRC, 2024.
- [301] Digital Equity Policy Center. "Cybersecurity as Public Policy Priority." San Francisco: DEPC, 2024.



www.fundacioel7.org





Servicios laborales y productivos para
personas con diversidad funcional



GOBIERNO
DE ESPAÑA

MINISTERIO
DE TRABAJO
Y ECONOMÍA SOCIAL



Fundació EI 7

C/ Pintor Fortuny, 17 - 17190 Salt

Av. De la Pau, 178 - 43580 Deltebre

www.fundacioel7.org

