Ciberseguridad accesible: el acento en la inclusión como pilar estratégico de la Seguridad Digital

En un ecosistema digital cada vez más sofisticado –y expuesto–, donde los vectores de ataque se multiplican al ritmo de la innovación tecnológica, la accesibilidad se posiciona como un componente esencial, no solo en términos éticos o normativos, sino como un auténtico pilar estratégico de ciberseguridad. Con la entrada en vigor del Acta Europea de Accesibilidad (EAA, por sus siglas en inglés) el próximo 28 de este mes de junio, las empresas se ven obligadas a adoptar un nuevo enfoque: integrar la seguridad desde el diseño inclusivo, garantizando que sus productos y servicios digitales sean seguros y accesibles para todos desde el inicio.

César López

La EAA como palanca de seguridad

La Directiva (UE) 2019/882, más conocida como Acta Europea de Accesibilidad (EAA), obliga a que una amplia gama de productos y servicios digitales –desde *smartphones* y terminales bancarios hasta aplicaciones de transporte o banca *online*– sean accesibles para todas las personas. Sus requisitos técnicos se destacan en la **Figura 1**.

Más allá del cumplimiento: la oportunidad de innovar

Incorporar la accesibilidad como principio de diseño fortalece la postura de seguridad global.

El incumplimiento puede suponer **sanciones de hasta el 4% de la facturación anual** o la retirada del producto del mercado.

Asimismo, esta normativa se alinea con otras normativas clave, como:

• PSD3 (prevista para 2026), que exigirá accesibilidad en los métodos de pago digitales, promoviendo APIs estandarizadas para terceros proveedores (TPPs).

• Reglamento de IA (IA Act, 2024), que establece requisitos para que los algoritmos –como los de detección de fraude– no generen sesgos ni discriminen a usuarios con discapacidad.

Accesibilidad y ciberseguridad: una relación simbiótica

Durante años, la accesibilidad digital ha sido percibida como una obligación legal o una responsabilidad social. Sin embargo, los hechos demuestran que lo accesible es más seguro. Un sistema diseñado para ser utilizado por personas con capacidades diversas –permanente o temporalmente– es, por definición, más robusto frente a errores de uso, menos susceptible a *bypasses* inseguros y más eficiente a la hora de validar controles organizativos y técnicos.

La discapacidad, entendida de forma amplia, actúa como un *stress test* natural que revela las debilidades reales de un sistema.

Para los responsables técnicos, esto implica un cambio de paradigma: accesibilidad, inclusión y ciberseguridad deben abordarse de forma integrada.

Requisitos Técnicos

CATEGORÍAS	ELEMENTOS TÉCNICOS
PERCEPTIBILIDAD	• Contraste visual • Alternativas multimedia • Señales hápticas
OPERABILIDAD	• Navegación sin ratón • Tiempos ajustables
SEGURIDAD ACCESIBLE	• Autenticación reforzada (SCA)
COMPATIBILIDAD TECNOLÓGICA	• APIs abiertas • Formatos estándar

Figura 1

Diseño inclusivo: proteger mejor a más personas

La inaccesibilidad en mecanismos de autenticación, navegación o verificación excluye –y expone– a millones de personas. Lejos de ser un colectivo vulnerable en términos de seguridad, las personas con discapacidad ofrecen una perspectiva clave para mejorarla: lo que es accesible para ellas, lo es para el 90% de la población.

Además, podemos confirmar que los sistemas accesibles:

• Reducen errores humanos.

• Disminuyen desviaciones de procedimiento.

• Permiten auditar con mayor precisión la eficacia real de los controles existentes.

La solución no está en parches aislados, sino en adoptar una estrategia de diseño universal: autenticación adaptativa, interfaces multimodales, herramientas tolerantes a la diversidad y procesos inclusivos.

Incorporar el talento de personas con discapacidad en equipos técnicos y de ciberseguridad aporta una perspectiva

Lo inaccesible es inseguro

Casos reales documentados por el National Cyber Security Centre (NCSC) de Reino Unido muestran cómo la falta de accesibilidad abre grietas en la superficie de defensa:

- CAPTCHAs visuales imposibles de resolver en condiciones de baja visibilidad, llevan a usuarios a recurrir a servicios externos no auditados para sortearlos, exponiendo credenciales.
- MFA no inclusivo, que obliga a desactivar medidas de autenticación por limitaciones temporales o motoras, dejando activos críticos desprotegidos.
- Alertas de ciberseguridad codificadas exclusivamente por color, que no son identificadas en contextos visuales alterados, retrasando la respuesta a incidentes.

diferencial. Su experiencia en entornos digitales diversos permite identificar puntos ciegos en el diseño y anticipar riesgos que de otro modo pasarían desapercibidos. En este sentido, la discapacidad no es una limitación, sino una fortaleza estratégica.

La Fundación GoodJob: conectando inclusión y ciberseguridad

En este contexto, la Fundación GoodJob ha desarrollado una línea de trabajo pionera en la interseccionalidad de la discapacidad con la accesibilidad y la ciberseguridad. A través de #factory, su servicio especializado de accesibilidad digital, ayuda a las organizaciones a identificar riesgos derivados de la inaccesibilidad y a implementar soluciones que mejoran simultáneamente la experiencia de usuario y la seguridad de sus sistemas.

La Fundación GoodJob no solo promueve el cumplimiento normativo, sino que actúa como *partner* estratégico en la transformación hacia una ciberseguridad más inclusiva, resiliente y efectiva.

La iniciativa #factory de accesibilidad digital permite a empresas y entidades públicas integrar estos principios con acompañamiento técnico, metodologías probadas y una visión centrada en las personas.

Conclusión: la accesibilidad es un activo estratégico, no un complemento

Tal y como recoge el informe del National Cyber Security Centre (NCSC), la accesibilidad no es un complemento, sino una medida proactiva de seguridad que ayuda a mitigar riesgos sistémicos y construir ecosistemas digitales más robustos.

El cumplimiento de la EAA no debe entenderse como una carga regulatoria, sino como una palanca de madurez digital en la que las personas con discapacidad son agente clave para la construcción de entornos digitales más seguros. Su experiencia y perspectiva aportan un valor diferencial en el diseño de soluciones accesibles y robustas. Incorporar su talento en equipos de ciberseguridad no solo es un acto de justicia social, sino una estrategia inteligente para anticipar vulnerabilidades y reforzar la defensa digital.

Recomendaciones básicas para líderes de ciberseguridad

- Incluir un capítulo específico de accesibilidad en los planes directores de ciberseguridad.
- Auditar procesos y controles desde una perspectiva inclusiva.
- Incorporar criterios de accesibilidad en *pentests* y revisiones de arquitectura.
- Formar equipos de seguridad en normativas como EN 301 549 y diseño universal.
- Promover la inclusión de personas con discapacidad en los equipos técnicos para enriquecer la visión y anticipar riesgos.

En definitiva, **accesibilidad, discapacidad y ciberseguridad están profundamente interconectadas**. Apostar por un diseño inclusivo es apostar por un futuro digital más seguro, más justo y más innovador. ■

César López
Director
FUNDACIÓN GOODJOB

La Fundación GoodJob es una entidad sin ánimo de lucro dedicada a la integración laboral de personas con discapacidad. Nuestra labor se centra especialmente en el ámbito tecnológico, con un enfoque particular en la ciberseguridad y la accesibilidad digital.