Accesibilidad, la vulnerabilidad invisible en ciberseguridad

La ciberaccesibilidad, entendida como la falta de accesibilidad digital en entornos seguros, es una realidad que ha constituido el punto de partida de una iniciativa pionera liderada por Fundación GoodJob, en colaboración con RootedCON, MTP-Ciberso, con el respaldo del Centro Criptológico Nacional del Centro Nacional de Inteligencia y el acompañamiento de la Revista SIC, que propone un cambio de paradigma: la accesibilidad como componente esencial de la seguridad digital.

César López / Javier de la Plaza

#aliadaSEC

En el ámbito de la ciberseguridad, donde cada día se perfeccionan los mecanismos de defensa frente a amenazas externas, persiste una vulnerabilidad silenciosa que todavía no se aborda con la profundidad que merece: **la ciberaccesibilidad, entendida como la falta de accesibilidad digital en entornos seguros**.

Interfaces que no pueden ser interpretadas por lectores de pantalla, sistemas de autenticación que excluyen a determinados perfiles de usuario o alertas codificadas únicamente por color son solo algunos ejemplos de cómo el mal diseño puede convertirse en una puerta abierta al riesgo. Esta vulnerabilidad, que nace de la desconexión entre accesibilidad y seguridad, es precisamente lo que aborda el concepto de **ciberaccesibilidad**: la necesidad de diseñar sistemas digitales que sean simultáneamente seguros e inclusivos.

Esta realidad ha sido el punto de partida de una iniciativa pionera liderada por **Fundación GoodJob**, en colaboración con **RootedCON**, **MTP-Ciberso**, con el respaldo del **Centro Criptológico Nacional** del **Centro Nacional de Inteligencia** y el acompañamiento de la **Revista SIC**, que propone un cambio de paradigma: la accesibilidad como componente esencial de la seguridad digital.

En 2022, usuarios con discapacidad visual denunciaron que no podían acceder a servicios bancarios *online* debido a CAPTCHAs sin alternativas sonoras funcionales. Al no poder completar el proceso de verificación, algunos optaron por compartir sus credenciales con familiares o asistentes, lo que comprometió la seguridad de sus cuentas. Este caso evidencia cómo una medida de seguridad mal implementada puede excluir y vulnerar simultáneamente.

El proyecto no se limita a una solución técnica, sino que plantea una estrategia integral que combina auditoría, formación, buenas prácticas y sensibilización sectorial. Su objetivo es doble: **reducir riesgos y generar conciencia sobre cómo la accesibilidad impacta directamente en la seguridad de los sistemas.**

UN PROYECTO QUE UNE INCLUSIÓN, TECNOLOGÍA Y ESTRATEGIA

La propuesta parte de una premisa clara: la falta de accesibilidad genera riesgos de ciberseguridad. Y lo hace desde una perspectiva estratégica, alineada con el nuevo marco normativo europeo, donde la European Accessibility Act (EAA), el Reglamento de Inteligencia Artificial y la futura PSD3 obligan a las organizaciones a repensar el diseño de sus productos y servicios digitales.

En el ecosistema digital actual, la accesibilidad web y la ciberseguridad no deben considerarse disciplinas aisladas. Las Pautas de Accesibilidad para el Contenido Web (WCAG 2.1), desarrolladas por el W3C, establecen criterios técnicos para garantizar que los sitios web sean utilizables por personas con discapacidad. Sin embargo, el incumplimiento de ciertos criterios puede derivar en vulnerabilidades que comprometen la seguridad informática de los usuarios y de las organizaciones.

En 2022, usuarios con discapacidad visual denunciaron que no podían acceder a servicios bancarios *online* debido a CAPTCHAs sin alternativas sonoras funcionales. Al no poder completar el proceso de verificación, algunos optaron por compartir sus credenciales con familiares o asistentes, lo que comprometió la seguridad de sus cuentas. Este caso evidencia cómo una medida de seguridad mal implementada puede excluir y vulnerar simultáneamente.

CRITERIOS WCAG 2.1 CON IMPACTO EN LA CIBERSEGURIDAD

El primer paso es seleccionar qué criterios de las pautas de accesibilidad (WCAG 2.1), tienen un posible impacto en ciberseguridad que puedan comprometer la seguridad en caso de incumplimiento. Algunos ejemplos de los criterios a identificar son los siguientes:

- **Criterio 2.2.1 – Tiempo ajustable**: Este criterio exige que los usuarios tengan suficiente tiempo para leer y utilizar el contenido. Si hay límites de tiempo, deben poder extenderse o desactivarse.

Impacto en ciberseguridad: En procesos de autenticación o firma digital, los usuarios con discapacidad motora o cognitiva pueden no completar la acción a tiempo. Esto puede llevarlos a usar gestores de contraseñas inseguros, compartir credenciales o desactivar medidas de seguridad como el cierre automático de sesión, exponiendo el sistema a accesos no autorizados.

• **Criterio 3.3.4 – Ayuda en la prevención de errores**: En formularios que implican transacciones legales, financieras o de datos sensibles se debe proporcionar ayuda para evitar errores, como validaciones, revisiones y confirmaciones.

> Impacto en ciberseguridad: La ausencia de validación clara puede provocar que el usuario introduzca datos erróneos, como enviar información personal al destinatario equivocado. Esto puede facilitar ataques de *phishing*, suplantación de identidad o pérdida de datos confidenciales.

• **Criterio 1.1.1 – Contenido no textual**: Todo contenido no textual (imágenes, iconos, botones) debe tener una alternativa textual que describa su función.

> Impacto en ciberseguridad: Si un botón de "Enviar" o "Aceptar términos" no tiene texto alternativo, los lectores de pantalla no lo detectan. Esto impide que usuarios con discapacidad visual completen procesos críticos como el *login* o la aceptación de políticas de privacidad, lo que puede llevar a exclusión o a que deleguen el acceso a terceros, comprometiendo la confidencialidad.

• **Criterio 2.1.1 – Acceso por teclado**: Todo contenido debe ser operable mediante teclado, sin requerir el uso de ratón.

> Impacto en ciberseguridad: Si un usuario no puede navegar por teclado, puede verse obligado a instalar herramientas externas o *scripts* personalizados para interactuar con el sitio. Estas soluciones pueden no ser seguras y abrir la puerta a *malware* o robo de información.

• **Criterio 4.1.1 – Procesamiento correcto del marcado**. El contenido debe estar correctamente estructurado en HTML, con etiquetas bien cerradas y sin errores de sintaxis.

> Impacto en ciberseguridad: Un marcado incorrecto puede interferir con tecnologías de asistencia, pero también con mecanismos de validación y autenticación. Esto puede facilitar ataques como inyecciones de código, manipulación de formularios o fallos en la lógica de seguridad del lado cliente.

• **Criterio 4.1.2 – Nombre, función y valor de los componentes.** Los elementos de la interfaz deben exponer correctamente su nombre, función y valor a las tecnologías de asistencia

> Impacto en ciberseguridad: Si un campo de entrada no está correctamente etiquetado, el usuario puede introducir datos en el lugar equivocado (por ejemplo, una contraseña en un campo visible). Esto puede exponer credenciales o provocar errores en procesos de autenticación.

Identificados todos los criterios de accesibilidad que pueden impactar en la ciberseguridad, el proceso de **análisis de ciberaccesibilidad** consiste en auditar aquellas páginas web críticas desde el punto de vista de la seguridad. Se incluyen, entre otras, las que contienen formularios, sistemas de *login*, *captchas* o cualquier componente que gestione datos personales o autenticación de usuarios.

Una vez identificada la muestra de pantallas, se analiza el cumplimiento de los criterios de ciberaccesibilidad en cada una de las páginas seleccionadas. Por cada incumplimiento, el consultor de accesibilidad detalla el motivo, el impacto en accesibilidad y las acciones de corrección, mientras que el consultor de ciberseguridad evalúa el riesgo asociado y determina su impacto desde la perspectiva de la protección del sistema.

Los resultados de la auditoría se integran en un Informe de Ciberaccesibilidad, que permite al cliente corregir los defectos detectados y reforzar simultáneamente la seguridad y la experiencia del usuario.

Este enfoque cobra especial relevancia tras el ciberataque registrado el 3 de junio de 2024 contra varios hospitales de Londres —entre ellos King's College Hospital, Guy's and St Thomas', Royal Brompton y Evelina London Children's Hospital—. En aquel incidente, los atacantes aprovecharon una vulnerabilidad en un sistema CAPTCHA adaptado para personas con discapacidad visual, lo que permitió automatizar accesos y comprometer servicios críticos. El caso evidenció que la accesibilidad mal implementada puede derivar en un riesgo real de ciberseguridad y refuerza la necesidad de diseñar sistemas donde inclusión y protección evolucionen conjuntamente.

En definitiva, un sistema que no contempla las necesidades de todos los usuarios puede inducir prácticas inseguras, generar frustración y abrir brechas de seguridad. Integrar los criterios WCAG 2.1 en el diseño seguro de interfaces es una estrategia imprescindible para construir entornos digitales resilientes, inclusivos y confiables. La convergencia entre accesibilidad y ciberseguridad debe ser una prioridad estratégica para cualquier organización que aspire a ofrecer servicios digitales seguros, inclusivos y resilientes.

UNA ALIANZA CON IMPACTO REAL

La alianza entre Fundación GoodJob, MTP-Ciberso y RootedCON permite combinar la experiencia en accesibilidad, el conocimiento técnico y la visión de negocio inclusiva. El respaldo del Centro Criptológico Nacional del Centro Nacional de Inteligencia refuerza la legitimidad de la propuesta y facilita su integración en entornos críticos tanto de la Administración Pública como del sector privado. Asimismo, Revista SIC acompaña esta propuesta, impulsando su difusión entre los actores clave del ecosistema tecnológico.

Los beneficios de esta solución son múltiples:

- **Reducción de riesgos**: Eliminación de puntos ciegos en el diseño digital.
- **Cumplimiento normativo**: Alineación con EAA y regulaciones emergentes.
- **Concienciación ética**: Promoción de la accesibilidad como valor de seguridad.
- **Inclusión real**: Participación activa de profesionales con discapacidad.
- **Reputación reforzada**: Mejora de imagen ante clientes, usuarios y reguladores.

Este proyecto no solo propone una solución técnica, sino además una transformación cultural en la forma de entender la seguridad digital. Al integrar la ciberaccesibilidad como factor crítico, se construyen sistemas más seguros, éticos y sostenibles. La Fundación GoodJob invita al sector a sumarse a esta evolución necesaria. ■

César López
Director General
FUNDACIÓN GOODJOB

Javier de la Plaza
Responsable del área de UX y Accesibilidad
MTP