

# Guía de Seguridad de las TIC

## CCN-STIC 465

# Guía Ciberaccesibilidad



## Mayo 2026



Catálogo de Publicaciones de la Administración General del Estado  
[cpage.mpr.gob.es](http://cpage.mpr.gob.es)

Edita:



CCN  
c=ES, l=MADRID, o=CCN, ou=SELLO  
ELECTRONICO, 2.5.4.97=VATES-S2800155J,  
serialNumber=S2800155J, cn=CCN  
2026.05.18 13:01:55 +02'00'

[cpage.mpr.gob.es](http://cpage.mpr.gob.es)

#### LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

#### AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

## Contenido

|                                                                                      |           |
|--------------------------------------------------------------------------------------|-----------|
| <b>1. Introducción .....</b>                                                         | <b>5</b>  |
| 1.1 Objetivo del documento .....                                                     | 5         |
| 1.1.1 Contexto .....                                                                 | 5         |
| 1.1.2 Alcance .....                                                                  | 6         |
| 1.1.3 Propósito .....                                                                | 6         |
| 1.1.4 Estructura del documento .....                                                 | 7         |
| <b>2. Bloque 1 color .....</b>                                                       | <b>8</b>  |
| 2.1 Categoría .....                                                                  | 8         |
| 2.1.1 Criterios wcag relacionados .....                                              | 8         |
| 2.1.2 Objetivo de accesibilidad .....                                                | 8         |
| 2.1.3 Objetivo de ciberaccesibilidad .....                                           | 8         |
| 2.1.4 Punto de convergencia “percepción confiable” .....                             | 9         |
| 2.1.5 Ejemplos prácticos y aplicables .....                                          | 10        |
| <b>3. Bloque 2 imágenes .....</b>                                                    | <b>11</b> |
| 3.1 Categoría .....                                                                  | 11        |
| 3.1.1 Criterios wcag relacionados .....                                              | 11        |
| 3.1.2 Objetivo de accesibilidad .....                                                | 11        |
| 3.1.3 Objetivo de ciberaccesibilidad .....                                           | 12        |
| 3.1.4 Punto de convergencia “integridad semántica visual” .....                      | 12        |
| 3.1.5 Ejemplos prácticos y aplicables .....                                          | 13        |
| <b>4. Bloque 3 teclado .....</b>                                                     | <b>14</b> |
| 4.1 Categoría .....                                                                  | 14        |
| 4.1.1 Criterios wcag relacionados .....                                              | 14        |
| 4.1.2 Objetivo de accesibilidad .....                                                | 14        |
| 4.1.3 Objetivo de ciberaccesibilidad .....                                           | 15        |
| 4.1.4 Punto de convergencia “control y verificación del foco” .....                  | 15        |
| 4.1.5 Ejemplos prácticos y aplicables .....                                          | 16        |
| <b>5. Bloque 4 puntero .....</b>                                                     | <b>17</b> |
| 5.1 Categoría .....                                                                  | 17        |
| 5.1.1 Criterios wcag relacionados .....                                              | 17        |
| 5.1.2 Objetivo de accesibilidad .....                                                | 17        |
| 5.1.3 Objetivo de ciberaccesibilidad .....                                           | 18        |
| 5.1.4 Punto de convergencia “confirmación perceptiva y control de interacción” ..... | 18        |
| 5.1.5 Ejemplos prácticos y aplicables .....                                          | 19        |
| <b>6. Bloque 5 eventos .....</b>                                                     | <b>20</b> |
| 6.1 Categoría .....                                                                  | 20        |
| 6.1.1 Criterios wcag relacionados .....                                              | 20        |
| 6.1.2 Objetivo de accesibilidad .....                                                | 20        |
| 6.1.3 Objetivo de ciberaccesibilidad .....                                           | 21        |
| 6.1.4 Punto de convergencia “visibilidad y control del estado interactivo” .....     | 21        |
| 6.1.5 Ejemplos prácticos y aplicables .....                                          | 22        |
| <b>7. Bloque 6 tiempo .....</b>                                                      | <b>24</b> |
| 7.1 Categoría .....                                                                  | 24        |

|            |                                                                                |           |
|------------|--------------------------------------------------------------------------------|-----------|
| 7.1.1      | Criterios wcag relacionados .....                                              | 24        |
| 7.1.2      | Objetivo de accesibilidad .....                                                | 24        |
| 7.1.3      | Objetivo de ciberaccesibilidad .....                                           | 25        |
| 7.1.4      | Punto de convergencia “tiempo controlado, no impuesto” .....                   | 25        |
| 7.1.5      | Ejemplos prácticos y aplicables .....                                          | 26        |
| <b>8.</b>  | <b>Bloque 7 comprensión y propósito .....</b>                                  | <b>28</b> |
| 8.1        | Categoría .....                                                                | 28        |
| 8.1.1      | Criterios wcag relacionados .....                                              | 28        |
| 8.1.2      | Objetivo de accesibilidad .....                                                | 28        |
| 8.1.3      | Objetivo de ciberaccesibilidad .....                                           | 29        |
| 8.1.4      | Punto de convergencia “comprensión como defensa y como inclusión” .....        | 30        |
| 8.1.5      | Ejemplos prácticos y aplicables .....                                          | 30        |
| <b>9.</b>  | <b>Bloque 8 errores, validación y retroalimentación.....</b>                   | <b>32</b> |
| 9.1        | Categoría .....                                                                | 32        |
| 9.1.1      | Criterios wcag relacionados .....                                              | 32        |
| 9.1.2      | Objetivo de accesibilidad .....                                                | 32        |
| 9.1.3      | Objetivo de ciberaccesibilidad .....                                           | 33        |
| 9.1.4      | Punto de convergencia “errores comprensibles, sistemas impenetrables” .....    | 34        |
| 9.1.5      | Ejemplos prácticos y aplicables .....                                          | 34        |
| <b>10.</b> | <b>Bloque 9 autenticación .....</b>                                            | <b>36</b> |
| 10.1       | Categoría .....                                                                | 36        |
| 10.1.1     | Criterios wcag relacionados .....                                              | 36        |
| 10.1.2     | Objetivo de accesibilidad .....                                                | 36        |
| 10.1.3     | Objetivo de ciberaccesibilidad .....                                           | 37        |
| 10.1.4     | Punto de convergencia “autenticación comprensible, seguridad sostenible” ..... | 38        |
| 10.1.5     | Ejemplos prácticos y aplicables .....                                          | 38        |
| <b>11.</b> | <b>Bloque 10 sintaxis y semántica .....</b>                                    | <b>40</b> |
| 11.1       | Categoría .....                                                                | 40        |
| 11.1.1     | Criterios wcag relacionados .....                                              | 40        |
| 11.1.2     | Objetivo de accesibilidad .....                                                | 40        |
| 11.1.3     | Objetivo de ciberaccesibilidad .....                                           | 41        |
| 11.1.4     | Punto de convergencia “lenguaje claro igual a decisión segura” .....           | 41        |
| 11.1.5     | Ejemplos prácticos y aplicables .....                                          | 42        |
| <b>12.</b> | <b>Anexo.....</b>                                                              | <b>43</b> |
| 12.1       | Glosario de términos.....                                                      | 43        |
| 12.2       | Referencias normativas y técnicas.....                                         | 44        |

## 1. Introducción

### 1.1 Objetivo del documento

El objetivo de este documento es establecer las bases conceptuales, metodológicas y operativas de la Guía de Ciberaccesibilidad, definiendo su propósito, alcance y marco normativo de referencia.

Esta guía tiene como finalidad proporcionar un conjunto estructurado de principios, criterios y recomendaciones prácticas que integren la accesibilidad digital y la ciberseguridad inclusiva en el diseño, desarrollo y mantenimiento de sistemas y servicios TIC.

El documento pretende orientar tanto a equipos técnicos como a responsables de seguridad, diseño y cumplimiento normativo, fomentando la creación de entornos digitales seguros, usables y accesibles para todas las personas, con independencia de sus capacidades, limitaciones o contexto de uso.

#### 1.1.1 Contexto

La transformación digital y la aplicación del Esquema Nacional de Seguridad (ENS) obligan a considerar no sólo la protección de la información y los servicios, sino también la accesibilidad universal de los usuarios que los utilizan.

En este sentido, la ciberaccesibilidad surge como una disciplina transversal que une las buenas prácticas de ciberseguridad, accesibilidad y diseño inclusivo, garantizando que las medidas de seguridad no generen barreras adicionales y que las soluciones accesibles mantengan el nivel de protección adecuado.

### 1.1.2 Alcance

Esta guía es aplicable a:

- a) Sitios web, aplicaciones, plataformas y servicios electrónicos de organismos públicos y entidades privadas que se rijan por el ENS o por los principios del CCN-STIC.
- b) Procesos de diseño, desarrollo, auditoría y mantenimiento de sistemas TIC donde la interacción con el usuario implique factores de accesibilidad o de seguridad cognitiva.
- c) Equipos de trabajo multidisciplinares que integren roles de accesibilidad, ciberseguridad, diseño UX/UI y cumplimiento normativo.
- d) Cualesquiera que sean los sitios web, aplicaciones, plataformas y servicios electrónicos de organismos públicos y entidades privadas, aunque no caigan bajo principios de ENS o CCN-STIC.

### 1.1.3 Propósito

El propósito último de esta guía es ofrecer un marco metodológico de convergencia entre accesibilidad y ciberseguridad, permitiendo diseñar sistemas digitales:

- a) Accesibles, siguiendo estándares como WCAG 2.2 y UNE-EN 301 549.
- b) Seguros, conforme a los principios del CCN-STIC y las buenas prácticas de OWASP.
- c) Cognitivamente sostenibles, es decir, comprensibles y previsibles para todos los usuarios, reduciendo el riesgo de error o manipulación.
- d) Diseñados con una premisa de menor propensión a vulnerabilidades por comportamientos inadvertidos de los usuarios.

#### 1.1.4 Estructura del documento

La guía se organiza en diez bloques técnicos temáticos (Color, Imágenes, Teclado, Puntero, Eventos, Tiempo, Comprensión y Propósito, Errores, Autenticación y Sintaxis/Semántica), acompañados de secciones conceptuales, recomendaciones transversales y conclusiones.

Cada bloque establece la correspondencia entre los criterios WCAG, los objetivos de accesibilidad, los objetivos de ciberseguridad y el punto de convergencia entre ambos, complementado con ejemplos prácticos aplicables a entornos reales.

## 2. Bloque 1 color

### 2.1 Categoría

Color

#### 2.1.1 Criterios WCAG relacionados

- a) 1.4.1 Uso del color
- b) 1.4.3 Contraste (mínimo)
- c) 1.4.6 Contraste (mejorado – AAA)
- d) 1.4.11 Contraste de contenido no textual

#### 2.1.2 Objetivo de accesibilidad

Garantizar que el color no sea el único medio visual para transmitir información, indicar acciones o distinguir elementos.

El diseño debe mantener una relación de contraste mínima (4.5:1 AA / 7:1 AAA) entre texto, imágenes y fondo, y asegurar que los elementos interactivos sean perceptibles también mediante texto, iconos o patrones.

Ejemplos de incumplimiento:

- a) Usar solo color para marcar errores o campos obligatorios.
- b) Enlaces no distinguibles sin color.
- c) Texto o iconos con bajo contraste sobre fondos decorativos o imágenes.
- d) Bordes invisibles o indicadores de foco perdidos por falta de contraste.

#### 2.1.3 Objetivo de ciberaccesibilidad

Asegurar que el uso del color sea coherente, comprensible y verificable, evitando ambigüedades que puedan explotarse mediante técnicas de ingeniería social o manipulación visual.

Los colores deben estar acompañados de mensajes explícitos y límites visuales claros que delimiten zonas activas y avisos legítimos.

Ejemplos de vulnerabilidad:

- a) Cambiar el color de los avisos de error (por ejemplo, usar violeta en lugar de rojo) sin explicación puede inducir a errores repetidos. Si el usuario no llega a la comprensión completa de un error, al sufrir algún tipo de disonancia cognitiva entre el código de error y los colores, podría querer repetir una misma solicitud generando resultados impredecibles y, naturalmente, aumentando la probabilidad de caer en potenciales errores o vulnerabilidades.
- b) La falta de límites visibles permite superposición de elementos (clickjacking) al dificultar la capacidad del usuario en la diferenciación de dónde termina un elemento y dónde empieza el siguiente.
- c) Un atacante puede crear falsos avisos o formularios simulando colores del sistema.

#### 2.1.4 Punto de convergencia “percepción confiable”

Todo elemento visual que comunique una acción, estado o aviso debe ser perceptible, inequívoco y verificable por todos los usuarios, evitando que diferencias de color o contraste generen confusión, inaccesibilidad o vulnerabilidad.

Tanto la accesibilidad como la ciberseguridad buscan garantizar que el usuario interprete correctamente la interfaz, sin depender únicamente del color ni de interpretaciones subjetivas (utilizar ambos mecanismos: el de color y el de texto de apoyo que deje claro el significado específico de ese color).

Un color mal aplicado puede ser una barrera perceptiva o un vector de ataque visual.

### 2.1.5 Ejemplos prácticos y aplicables

| Escenario                   | Descripción                                                                                                                       | Beneficio convergente                                                    |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Captcha accesible           | Sustituir captchas basados en color por alternativas táctiles o auditivas.<br>Ejemplo: respuesta háptica por vibración o presión. | Permite verificación sin visión ni color y evita automatismos inseguros. |
| Mensajes de error           | Combinar color (rojo/verde) con texto e icono explicativo.                                                                        | Evita confusión cromática y mejora la interpretación segura del estado.  |
| Alertas de seguridad falsas | Mantener esquema de color + etiqueta fija en alertas oficiales (“Notificación segura del sistema”).                               | Reduce riesgo de phishing visual o imitaciones.                          |
| Botones activos             | Destacar límites mediante hover/focus y contraste 3:1 con entorno.                                                                | Mejora navegación y evita ataques de superposición.                      |
| Validación de acciones      | Mantener coherencia entre color, texto y estructura tras operaciones (login, envío de datos).                                     | El usuario reconoce mensajes auténticos y evita manipulaciones.          |

Cuadro: Ejemplos prácticos y aplicables.

## 3. Bloque 2 imágenes

### 3.1 Categoría

Imágenes

#### 3.1.1 Criterios WCAG relacionados

- a) 1.1.1 Contenido no textual (Texto alternativo)
- b) 1.4.5 Imágenes de texto (AA)
- c) 1.4.9 Imágenes de texto (sin excepción – AAA)

#### 3.1.2 Objetivo de accesibilidad

Garantizar que todo contenido no textual (imágenes, iconos, gráficos, botones, diagramas, etc.) Disponga de una alternativa textual equivalente, que comunique la misma información o función.

Cuando el texto puede cumplir el mismo propósito, se debe usar texto real en lugar de imágenes de texto, excepto cuando la presentación visual sea esencial (p. Ej., logotipos o tipografías de marca).

Ejemplos de incumplimiento:

- a) Imágenes con información importante insertadas por CSS sin alt.
- b) Alternativas textuales incompletas o genéricas (ej. Alt="imagen").
- c) Imágenes decorativas sin marcado adecuado (alt="").
- d) Falta de actualización del texto alternativo cuando el contenido visual cambia.
- e) Incoherencias entre el texto de la imagen y su descripción textual.
- f) Uso de ASCII art o texto incrustado en imágenes sin alternativa.

### 3.1.3 Objetivo de ciberaccesibilidad

Asegurar que los textos alternativos, títulos y etiquetas asociadas a imágenes sean precisos, coherentes y semánticamente consistentes con la función real del elemento.

Un texto alternativo inexacto, redundante o contradictorio puede inducir a errores, desinformación o manipulación social.

Ejemplos de vulnerabilidad:

- a) Mensajes falsos o maliciosos disfrazados de imágenes con alt engañoso.
- b) Formularios o botones críticos (login, pagos, contraseñas) que usan imágenes sin textos claros.
- c) Desajustes entre ALT, TITLE y contenido visible que confunden lectores de pantalla.
- d) Uso de imágenes para representar acciones seguras (“Enviar”, “Confirmar”) sin explicación textual clara.

Buenas prácticas:

- a) Revisar manualmente los alt y title en procesos críticos.
- b) Evitar incluir información sensible en texto alternativo (p. Ej., “Transferencia enviada correctamente a cuenta X”).
- c) Mantener la coherencia semántica entre la interfaz visual y la accesible.
- d) Evitar imágenes ambiguas o decorativas en contextos de autenticación o confirmación.

### 3.1.4 Punto de convergencia “integridad semántica visual”

Toda representación visual o textual debe mantener una correspondencia semántica exacta con la función que cumple en la interfaz, asegurando que la información sea comprensible, verificable y confiable por cualquier usuario o tecnología asistiva.

La accesibilidad busca equivalencia de comprensión, mientras que la ciberseguridad busca veracidad de la representación.

Ambas coinciden en que una imagen mal descrita puede ser una barrera o una trampa.

Garantizar que el significado percibido y el significado declarado sean idénticos es clave para una experiencia segura e inclusiva.

### 3.1.5 Ejemplos prácticos y aplicables

| Escenario              | Descripción                                                                              | Beneficio convergente                                                                              |
|------------------------|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Botones gráficos       | Botones con iconos, acompañados de texto o aria-label que explicita la acción.           | Evita malinterpretaciones por parte de lectores de pantalla y reduce el riesgo de clics inseguros. |
| Iconos de validación   | En formularios, usar tanto color como texto ("Error: campo vacío") y no solo una imagen. | Aumenta la comprensión y previene intentos de manipulación o engaño visual.                        |
| Alertas gráficas       | Las imágenes de advertencia deben incluir texto explicativo ("Este sitio no es seguro"). | Refuerza la credibilidad del aviso y evita falsos positivos de phishing.                           |
| Gráficos o infografías | Añadir descripción larga (longdesc o aria-describedby) con la información clave.         | Asegura acceso a la información sin exponer datos críticos o falsos.                               |
| Contenido decorativo   | Marcar correctamente imágenes sin valor informativo con alt="".                          | Evita ruido cognitivo y posibles inserciones maliciosas disfrazadas de decoración.                 |

Cuadro: Ejemplos prácticos y aplicables.

## 4. Bloque 3 teclado

### 4.1 Categoría

Teclado

#### 4.1.1 Criterios WCAG relacionados

- a) 2.1.1 Mecanismos de entrada
- b) 2.1.2 Sin trampas para el foco del teclado
- c) 2.1.3 Mecanismos de entrada (sin excepción – AAA)
- d) 2.1.4 Atajos con teclas de caracteres
- e) 2.4.7 Foco visible

#### 4.1.2 Objetivo de accesibilidad

Garantizar que todas las funcionalidades del contenido sean operables mediante teclado, sin necesidad de ratón ni gestos complejos.

El usuario debe poder navegar, activar y desplazarse por los elementos de la interfaz utilizando únicamente las teclas estándar (tabulación, enter, flechas, etc.).

Asimismo, los puntos de foco deben ser siempre visibles, claros y consistentes, de forma que el usuario sepa en todo momento dónde está interactuando.

Los atajos de teclado deben poder activarse, desactivarse o personalizarse para evitar conflictos con tecnologías de asistencia o accesos del sistema.

Ejemplos de incumplimiento:

Controles o menús inaccesibles sin ratón.

Elementos que atrapan el foco (sin posibilidad de salir con Esc o Tab).

- a) Falta de indicador visible de foco (sin borde o resaltado).
- b) Atajos activados por una sola tecla que interfieren con lectores de pantalla.

### 4.1.3 Objetivo de ciberaccesibilidad

Todos los atajos de teclado deben ser coherentes con la lógica funcional y de seguridad de la interfaz.

El uso inadecuado o inconsistente de combinaciones de teclas puede ser explotado por adversarios. Entre los especiales criterios de consistencia deben contemplarse la completitud del diccionario de atajos que puedan reaccionar a los eventos, no dejando “huecos” que pudieran terminar en algún tipo de comportamiento impredecible por defecto o, peor, donde un potencial Adversario pudiera ubicar su propio evento de gestión de la pulsación de teclado.

Ejemplos de vulnerabilidad:

Evasión de controles (por ejemplo, saltar una pantalla de segundo factor).

Salto en los ordinales que identifican elementos para el acceso mediante tabulador u otras opciones de avance sin ratón; puede implicar que un adversario inserte un elemento indeseado en la cadena de tabulación.

Inserción maliciosa de comandos o scripts mediante teclas especiales.

Generación de fatiga cognitiva o errores inducidos (por ejemplo, repetir Enter o Tab hasta omitir verificaciones).

Además, el foco visible y el cursor activo en campos de entrada son elementos esenciales tanto para la orientación accesible como para la seguridad operativa, ya que ayudan a:

Prevenir ataques de “focus hijacking” (robo del foco para capturar contraseñas).

Confirmar al usuario que está introduciendo datos en el campo correcto.

Evitar redirecciones invisibles o formularios superpuestos.

### 4.1.4 Punto de convergencia “control y verificación del foco”

Todo elemento controlable mediante teclado debe ofrecer retroalimentación visible, predecible y coherente, asegurando que el usuario mantenga el control de la

interacción en todo momento y que la interfaz no pueda ser manipulada para alterar el flujo lógico o la percepción de seguridad.

En accesibilidad, esto garantiza autonomía y orientación cognitiva; en ciberseguridad, garantiza integridad de la interacción y trazabilidad del foco.

Ambas dimensiones convergen en el principio de que el usuario debe saber y controlar dónde está actuando, evitando tanto la confusión como la manipulación.

#### 4.1.5 Ejemplos prácticos y aplicables

| Escenario                             | Descripción                                                                             | Beneficio convergente                                                              |
|---------------------------------------|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Navegación por teclado en formularios | El usuario puede recorrer todos los campos con Tab, sin bloqueos ni saltos inesperados. | Mejora la accesibilidad y evita capturas del foco por scripts maliciosos.          |
| Indicador de foco visible             | Borde resaltado (3:1 de contraste mínimo) o sombreado animado al cambiar de elemento.   | Permite al usuario identificar visualmente el área activa y evita el robo de foco. |
| Campos de autenticación               | El cursor parpadea en el campo activo y no se redirige automáticamente.                 | Reduce errores y previene capturas de credenciales.                                |
| Atajos personalizables                | Permitir activar/desactivar combinaciones (ej. Alt + S para “Enviar”).                  | Previene conflictos con lectores de pantalla y bloquea posibles abusos.            |
| Gestión segura del foco tras alertas  | Al cerrar un modal o alerta, el foco regresa al elemento que lo originó.                | Mantiene la lógica de navegación y evita confusión o manipulación del flujo.       |

Cuadro: Ejemplos prácticos y aplicables.

## 5. Bloque 4 Puntero

### 5.1 Categoría

Puntero

#### 5.1.1 Criterios WCAG relacionados

2.5.1 Gestos del puntero

2.5.2 Cancelación del puntero

2.5.5 Tamaño objetivo (AAA)

2.5.8 Tamaño del objetivo (mínimo – AA, WCAG 2.2)

#### 5.1.2 Objetivo de accesibilidad

Garantizar que las acciones realizadas mediante puntero (ratón, touchpad, pantalla táctil o lápiz digital) sean simples, controlables y reversibles.

Los gestos complejos o que requieran precisión milimétrica deben evitarse o complementarse con alternativas más sencillas.

Cada objetivo clicable debe tener un tamaño mínimo y área activa suficiente para facilitar su uso a personas con movilidad reducida o limitaciones motoras.

Asimismo, debe existir la posibilidad de cancelar una acción iniciada con el puntero (por ejemplo, arrastrar un archivo o hacer doble clic por error) y ofrecer una confirmación visual clara de cuál es el elemento actualmente activo o seleccionado.

Ejemplos de incumplimiento:

Elementos clicables demasiado pequeños o cercanos.

Gestos complejos (p. Ej., arrastrar y soltar) sin alternativa mediante clic simple.

Falta de indicador visual al presionar o mantener el clic.

Imposibilidad de cancelar una acción iniciada por error.

### 5.1.3 OBJETIVO DE CIBERACCESIBILIDAD

El ratón o puntero debe ser un instrumento de interacción consciente y verificable.

El usuario debe saber en todo momento dónde se encuentra su puntero y sobre qué elemento está actuando, evitando manipulaciones visuales o confusiones intencionadas.

Cuando se produzcan eventos de clic o doble clic, la interfaz debe emitir una respuesta visual inequívoca (marco, sombra, animación o cambio de color) que confirme la acción y su destino.

Esto reduce riesgos:

Clickjacking (redirigir al usuario a elementos invisibles o falsos).

Superposición de zonas activas sobre contenido legítimo.

Acciones no deseadas por error o fatiga (doble clic involuntario).

También se recomienda asegurar un tamaño de objetivo suficiente (mínimo 24x24 px) para minimizar errores de puntería y facilitar la precisión en entornos táctiles o con dispositivos alternativos.

### 5.1.4 Punto de convergencia “confirmación perceptiva y control de interacción”

Todo evento iniciado con el puntero debe ser visualmente confirmado, reversible y claramente delimitado, de modo que el usuario tenga plena conciencia de su acción, su alcance y su resultado inmediato.

La accesibilidad busca control físico y cognitivo y la ciberseguridad busca control lógico y verificación de intención.

Ambas convergen en garantizar que la interacción con el puntero sea siempre visible, inequívoca y segura, evitando tanto errores humanos como manipulaciones visuales intencionadas.

### 5.1.5 Ejemplos prácticos y aplicables

| Escenario                               | Descripción                                                           | Beneficio convergente                                                                         |
|-----------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Botones con hover/focus visibles        | Cambios claros de color o borde al pasar el puntero.                  | Ayuda a usuarios con visión reducida y evita clics en elementos invisibles o falsos.          |
| Confirmación visual del clic            | Animación o cambio de estado inmediato (botón presionado).            | Refuerza la percepción de acción legítima y evita ataques de suplantación visual.             |
| Tamaño mínimo de zona activa (24x24 px) | Mejora la precisión en clics y toques.                                | Reduce errores involuntarios y evita que el atacante aproveche zonas minúsculas superpuestas. |
| Gestos simplificados o alternativos     | Doble clic reemplazable por pulsación larga o botón "Aceptar".        | Mejora la usabilidad y evita acciones no intencionadas.                                       |
| Cancelación de acción                   | Permitir deshacer o confirmar antes de ejecutar operaciones críticas. | Previene la manipulación y protege contra la fatiga de clics.                                 |

**Cuadro:** Ejemplos prácticos y aplicables.

## 6. Bloque 5 eventos

### 6.1 Categoría

Eventos (Hover, Focus, Entradas y Cambios de Estado)

#### 6.1.1 Criterios WCAG relacionados

1.4.13 Contenido en hover o focus

3.2.1 Al recibir el foco

3.2.2 Al recibir entradas

2.4.13 – Apariencia del foco (Nivel AAA)

2.1.2 – Sin trampa de teclado (Nivel A)

#### 6.1.2 Objetivo de accesibilidad

Garantizar que cualquier contenido o acción que se active al pasar el puntero o al recibir el foco del teclado sea predecible, controlable y perceptible.

El usuario debe poder identificar claramente qué elemento está activo, qué información emergente aparece y cómo cerrarla o descartarla fácilmente sin perder contexto.

Además, los cambios de contenido o estado provocados por hover o focus no deben confundir al usuario ni generar pérdida de foco, especialmente para personas que utilizan tecnologías de asistencia.

Ejemplos de incumplimiento:

Menús desplegados que desaparecen al mover ligeramente el puntero.

Pop-ups que se abren con el foco pero sin medios claros para cerrarlos.

Cambios automáticos de página o contenido al recibir el foco.

Campos que se validan o alteran automáticamente al recibir entrada.

### 6.1.3 Objetivo de ciberaccesibilidad

Los elementos activos que reciben hover, focus o input deben delimitarse y resaltarse de forma evidente, mostrando claramente al usuario qué zona se encuentra en modo interactivo y qué impacto podría tener su acción.

Esto es especialmente importante en:

- a) Áreas que impliquen cambios de datos esenciales (p. Ej. Configuración, credenciales).
- b) Procesos de autenticación o transacción.
- c) Acciones de pago, confirmación o eliminación de información.
- d) El resaltado visible y consistente reduce riesgos de:
- e) Clickjacking (camuflar un botón bajo otro).
- f) Falsos focus (redirección del foco a un elemento malicioso).
- g) Ingeniería social visual, donde el usuario pulsa sin entender la consecuencia real.

La interfaz debe proveer feedback visual inmediato y delimitado, asegurando que:

- a) El foco no pueda ser secuestrado.
- b) El usuario sepa qué acción va a ejecutar antes de confirmarla.
- c) Los elementos críticos estén claramente marcados con color, borde o iconografía de advertencia (por ejemplo, triángulos o color ámbar para acciones sensibles).

### 6.1.4 Punto de convergencia “visibilidad y control del estado interactivo”

Todo elemento que cambie de estado o reacción mediante hover, focus o entrada debe ofrecer retroalimentación perceptible, contextual y segura, asegurando que el usuario comprende la acción que está realizando y su posible impacto.

En accesibilidad, esto permite navegación clara y predecible y en ciberseguridad, evita acciones confusas, redirecciones o confirmaciones engañosas.

Ambas perspectivas convergen en el principio de transparencia interactiva: el usuario debe ver, entender y controlar cada evento antes de que produzca efectos.

### 6.1.5 Ejemplos prácticos y aplicables

| Escenario                                      | Descripción                                                                                                                  | Beneficio convergente                                                            |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Hover sobre elementos activos                  | Botones o enlaces cambian de color, forma o sombra al pasar el puntero.                                                      | Permite identificar zonas clicables y previene engaños visuales o solapamientos. |
| Focus en campos críticos                       | Al enfocar un campo de contraseña o pago, aparece un borde destacado y un aviso discreto (“Introduzca con precaución”).      | Refuerza la atención y reduce riesgos de errores o phishing.                     |
| Pop-ups o tooltips accesibles                  | Los tooltips aparecen con foco, permanecen visibles hasta que el usuario los cierra manualmente y son accesibles al teclado. | Facilita la lectura y evita cierres accidentales o desvío del foco.              |
| Confirmación visual al escribir                | Campos que cambian de borde (verde/rojo) al validar contenido, sin mensajes engañosos o automáticos.                         | Mejora comprensión y evita falsos mensajes de éxito/errores explotables.         |
| Doble verificación visual en acciones críticas | Botones de eliminación o envío acompañados de                                                                                | Aumenta la conciencia del usuario y previene                                     |

| Escenario | Descripción                    | Beneficio convergente         |
|-----------|--------------------------------|-------------------------------|
|           | iconos y color de advertencia. | confirmaciones involuntarias. |

Cuadro: Ejemplos prácticos y aplicables.

## 7. Bloque 6 tiempo

### 7.1 Categoría

Temporizadores, expiraciones y control del tiempo de interacción.

#### 7.1.1 Criterios WCAG relacionados

- a) 2.2.1 Tiempo ajustable
- b) 2.2.3 Sin tiempo (AAA)
- c) 2.2.6 Tiempos de espera (AAA)

#### 7.1.2 Objetivo de accesibilidad

Garantizar que los usuarios puedan controlar o desactivar los límites de tiempo impuestos por una aplicación o sistema, de forma que no se vean forzados a actuar más rápido de lo que sus capacidades les permiten.

El tiempo no debe ser un factor excluyente ni un obstáculo para completar tareas, leer, comprender o interactuar con el contenido.

Se deben ofrecer opciones de ampliación, pausa o eliminación del límite temporal, salvo en contextos donde el tiempo sea esencial (por ejemplo, subastas en tiempo real).

Ejemplos de incumplimiento:

- a) Formularios que expiran automáticamente sin aviso ni posibilidad de extensión.
- b) Sesiones que se cierran sin advertencia previa, perdiendo los datos introducidos.
- c) Captchas o autenticaciones temporizadas sin alternativa accesible.
- d) Elementos interactivos que cambian automáticamente antes de que el usuario los comprenda.

### 7.1.3 Objetivo de ciberaccesibilidad

Los temporizadores y tiempos de espera en procesos sensibles deben diseñarse considerando tanto la fatiga cognitiva y motora del usuario, como el riesgo de exposición o abuso.

Un mal diseño puede:

- a) Inducir estrés y abandono prematuro, afectando la seguridad (el usuario podría reintentar con errores o usar canales menos seguros).
- b) Exponer al usuario a riesgos de ingeniería social, si busca “atajos” para evitar repetir pasos de verificación.
- c) Generar vulnerabilidades por sesiones caducadas sin control, o por mantener activas sesiones que deberían expirar.
- d) Derivar en ejecuciones incontroladas en los casos donde se utiliza JavaScript con patrones del tipo `setTimeout( () => {})`; y la gestión de los temporizadores o tiempos límites no ha sido cuidadosamente definida.

Por tanto:

- a) Las acciones críticas deben ser atómicas y transaccionales: completarse en un único flujo breve y verificable.
- b) El usuario debe recibir avisos anticipados de expiración y opciones claras para extender o confirmar la sesión.
- c) El sistema debe gestionar tiempos límite con contexto, distinguiendo entre inactividad y dificultad real de interacción.

### 7.1.4 Punto de convergencia “tiempo controlado, no impuesto”

La interfaz debe otorgar al usuario la capacidad de gestionar su propio tiempo dentro de los márgenes de seguridad, garantizando que ninguna acción crítica se vea interrumpida o forzada por un límite temporal que comprometa su comprensión o decisión.

En accesibilidad, esto asegura inclusión y autonomía temporal y en ciberseguridad, previene errores por presión, omisiones y explotación del estrés del usuario.

Ambos coinciden en el principio de autonomía temporal supervisada: permitir que el usuario controle su ritmo sin comprometer la integridad del sistema.

### 7.1.5 Ejemplos prácticos y aplicables

| Escenario                                              | Descripción                                                                                    | Beneficio convergente                                  |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Avisos de sesión próxima a expirar                     | El sistema notifica con 60 segundos de antelación y ofrece “Extender sesión”.                  | Evita pérdida de datos y mantiene la sesión segura.    |
| Formularios extensibles por el usuario                 | Opción “Necesito más tiempo” para ampliar plazos en formularios largos o de autenticación.     | Mejora accesibilidad y reduce frustración o abandono.  |
| Transacciones atómicas                                 | Operaciones críticas (pago, cambio de clave) divididas en pasos con confirmaciones inmediatas. | Minimiza riesgo de interrupción o corrupción de datos. |
| Captchas sin tiempo o adaptativos                      | Se reemplazan por mecanismos alternativos (p. Ej. Audio, háptico o pregunta de contexto).      | Evita discriminación por lentitud o discapacidad.      |
| Desconexión segura con persistencia controlada         | Al cerrar sesión, el sistema guarda el estado de trabajo y ofrece reanudación segura.          | Protege datos y reduce la frustración del usuario.     |
| Verificación de la lógica en temporizadores JavaScript | Verificar que los procesos definidos mediante setTimeout son                                   | Evita problemas de comportamiento errático e           |

| Escenario | Descripción                              | Beneficio convergente              |
|-----------|------------------------------------------|------------------------------------|
|           | consistentes y están bien implementados. | impredecible de código JavaScript. |

Cuadro: Ejemplos prácticos y aplicables.

## 8. Bloque 7 comprensión y propósito

### 8.1 Categoría

Claridad semántica, comprensión del propósito y consistencia del lenguaje

#### 8.1.1 Criterios WCAG relacionados

- a) 1.3.5 Identificar el propósito de la entrada
- b) 1.3.6 Identificar propósito (AAA)
- c) 2.4.4 Propósito de los enlaces (en contexto)
- d) 2.4.9 Propósito del enlace (solo enlace) (AAA)
- e) 3.1.3 Palabras inusuales (AAA)
- f) 3.1.4 Abreviaturas (AAA)
- g) 3.1.5 Nivel de lectura (AAA)

#### 8.1.2 Objetivo de accesibilidad

Asegurar que todas las entradas, enlaces, botones y mensajes sean comprensibles, predecibles y semánticamente claros, permitiendo que el usuario entienda qué hace cada elemento antes de interactuar con él.

El lenguaje y el propósito de cada componente deben ser evidentes sin ambigüedad, sin depender de contexto visual ni suposiciones técnicas.

Ejemplos de incumplimiento:

- a) Botones con etiquetas vagas como “Enviar” o “Aceptar” sin indicar qué acción concreta realizan.
- b) Formularios que no describen claramente el propósito de un campo (por ejemplo, no indicar si es correo personal o profesional).
- c) Enlaces con texto genérico como “Haz clic aquí” sin contexto.
- d) Uso de tecnicismos o abreviaturas sin explicación accesible.

e) Niveles de lectura excesivamente complejos o redactados con jerga innecesaria.

El contenido debe poder ser comprendido por una amplia variedad de usuarios, incluyendo aquellos con dificultades cognitivas, lingüísticas o culturales, manteniendo la consistencia en toda la interfaz.

### 8.1.3 Objetivo de ciberaccesibilidad

Desde la ciberseguridad, la claridad del propósito y la precisión del lenguaje son esenciales para evitar confusión, manipulación o errores del usuario que puedan derivar en vulnerabilidades.

Riesgos y medidas:

- a) Lenguaje ambiguo o técnico puede inducir al usuario a realizar acciones inseguras (ej. Aceptar condiciones sin entender su alcance o uso de *encriptar* en lugar de cifrar).
- b) Mensajes confusos o contradictorios pueden facilitar ataques de ingeniería social (p. Ej. Phishing dentro de la misma interfaz o imitaciones visuales).
- c) Alertas demasiado técnicas pueden revelar información sensible sobre el sistema, útil para un adversario.
- d) Mensajes excesivamente alarmistas o triviales pueden desensibilizar al usuario o inducir comportamientos automáticos.

Las interfaces deben:

- a) Ser predecibles y consistentes, sin alterar dinámicamente el propósito de los elementos.
- b) Usar lenguaje seguro y funcional, centrado en la acción del usuario y no en los detalles técnicos.
- c) Minimizar la exposición de información interna en mensajes de error o validación.

#### 8.1.4 Punto de convergencia “comprensión como defensa y como inclusión”

La comprensión del propósito de cada elemento es un principio compartido entre la accesibilidad y la ciberseguridad: un usuario que entiende lo que hace, se equivoca menos y es más difícil de engañar.

Desde la accesibilidad, la claridad favorece la inclusión y la autonomía cognitiva y desde la ciberseguridad, reduce la superficie de ataque basada en la confusión o la manipulación semántica.

Ambas perspectivas convergen en el diseño cognitivo seguro, donde el lenguaje es transparente, los propósitos son explícitos y la interacción no deja espacio a la duda ni a la interpretación maliciosa.

#### 8.1.5 Ejemplos prácticos y aplicables

| Escenario                             | Descripción                                                                                   | Beneficio convergente                                      |
|---------------------------------------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------|
| Etiquetas contextuales en formularios | Campos con indicaciones como “Correo electrónico laboral” o “Teléfono de contacto personal”.  | Reduce errores de envío y mejora comprensión de propósito. |
| Botones con propósito explícito       | En lugar de “Aceptar”, usar “Confirmar pago” o “Guardar cambios en perfil”.                   | Evita confusiones y reduce riesgo de acción indebida.      |
| Mensajes de error neutros y guiados   | “Tu contraseña no cumple los requisitos de seguridad” en lugar de mostrar criterios técnicos. | Orienta sin revelar información sensible.                  |
| Glosario de términos y abreviaturas   | Ofrecer explicaciones simples de siglas (p. Ej.                                               | Mejora comprensión y evita explotación cognitiva.          |

| Escenario                   | Descripción                                                           | Beneficio convergente                              |
|-----------------------------|-----------------------------------------------------------------------|----------------------------------------------------|
|                             | “OTP: código temporal de un solo uso”).                               |                                                    |
| Enlaces con propósito claro | “Leer más sobre políticas de privacidad” en lugar de “Haz clic aquí”. | Mejora navegación y evita redirecciones engañosas. |

Cuadro: Ejemplos prácticos y aplicables.

## 9. Bloque 8 errores, validación y retroalimentación

### 9.1 Categoría

Gestión de errores, instrucciones, prevención y confirmación de acciones

#### 9.1.1 Criterios WCAG relacionados

- a) 3.3.1 Identificación de errores
- b) 3.3.2 Etiquetas o instrucciones
- c) 3.3.3 Sugerencias para corrección de errores
- d) 3.3.4 Prevención de errores
- e) 3.3.6 Prevención de errores (Todos) (AAA)

#### 9.1.2 Objetivo de accesibilidad

Garantizar que los usuarios comprendan los errores cometidos y sepan cómo corregirlos sin perder información ni sentirse desorientados.

Los mensajes de error deben ser:

- a) Claros, concisos y comprensibles, indicando qué ha ocurrido y cómo solucionarlo.
- b) Contextuales, situados junto al elemento que provoca el error.
- c) Persistentes, no temporales o emergentes de corta duración.
- d) Compatibles con tecnologías de asistencia, de modo que lectores de pantalla o dispositivos alternativos los interpreten correctamente.

Ejemplos de incumplimiento:

- a) Formularios que muestran un error solo en color rojo sin texto asociado.
- b) Mensajes genéricos como “Error en el envío” sin indicar qué campo está afectado.
- c) Pérdida total de datos al producirse un error de validación.

- d) Ausencia de etiquetas claras o instrucciones previas que eviten errores repetitivos.
- e) Pop-ups de error que desaparecen automáticamente sin dar tiempo a su lectura.

### 9.1.3 Objetivo de ciberaccesibilidad

Los mensajes de error y de validación deben ofrecer sólo la información estrictamente necesaria para que el usuario comprenda lo ocurrido, sin exponer detalles internos del sistema o de su infraestructura.

Principios clave:

- a) Los mensajes no deben revelar información técnica sensible (nombres de campos, algoritmos, estructuras de base de datos, etc.).
- b) Los detalles de los errores en acciones críticas (autenticación, transacciones, recuperación de contraseñas, cambios de datos) deben ser escuetos y controlados.
- c) Las sugerencias de corrección deben guiar al usuario sin ofrecer pistas técnicas que puedan ser aprovechadas por adversarios.
- d) Los mensajes de confirmación deben ser claros, persistentes y verificables por el usuario, evitando notificaciones temporales o automáticas.
- e) Toda comunicación de error o éxito debe confirmarse de forma explícita por el usuario, reforzando la certeza de que ha comprendido el resultado.
- f) Todo mensaje de error o de confirmación relacionado con procesos de autenticación debe generalizarse al máximo, evitando que distintos motivos emitan mensajes distintos, lo que podría llevar al Adversario a determinar si un usuario existe (descubrimiento) o el motivo por el que se ha fallado un proceso concreto. Un ejemplo claro es la posibilidad de descubrir que existan unos u otros usuarios por mensajes de error que así lo indiquen.

### 9.1.4 Punto de convergencia “errores comprensibles, sistemas impenetrables”

Tanto en accesibilidad como en ciberseguridad, la gestión de errores debe informar al usuario sin informar al adversario.

Desde la accesibilidad, se busca que los errores sean fáciles de entender, corregir y confirmar y desde la ciberseguridad, se exige que esos mensajes no revelen datos internos ni vulnerabilidades.

La convergencia se alcanza en el principio de “retroalimentación controlada”, donde cada mensaje mantiene el equilibrio entre informar lo suficiente para guiar al usuario y ocultar lo suficiente para proteger el sistema.

### 9.1.5 Ejemplos prácticos y aplicables

| Escenario                           | Descripción                                                                                    | Beneficio convergente                                                                                                                                                                                                         |
|-------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mensajes de error neutros y guiados | “Tu contraseña no cumple los requisitos de seguridad. Revisa el formato.”                      | Guía al usuario sin revelar detalles técnicos.<br>Adicionalmente, evitando ser explícitos en si un usuario existe o no, o si se ha fallado la contraseña al autenticar (preferible “Credenciales incorrectas” como genérico). |
| Validación contextual por campo     | Indicar el error justo debajo del campo correspondiente.                                       | Facilita comprensión y evita exposición innecesaria.                                                                                                                                                                          |
| Confirmaciones persistentes         | Tras un cambio de datos, mostrar un mensaje fijo: “Tu perfil se ha actualizado correctamente.” | Refuerza confianza y reduce confusión.                                                                                                                                                                                        |

| Escenario                      | Descripción                                                                                    | Beneficio convergente                                    |
|--------------------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Instrucciones preventivas      | Mostrar ejemplos de formato antes de rellenar campos sensibles (ej. Correo, fecha).            | Reduce errores sin comprometer seguridad.                |
| Alertas accesibles y auditivas | Para usuarios con discapacidad visual o cognitiva, emitir una señal auditiva además del texto. | Aumenta comprensión y percepción del estado del sistema. |

Cuadro: Ejemplos prácticos y aplicables.

## 10. Bloque 9 autenticación

### 10.1 Categoría

Procesos de identificación, re-autenticación y validación multifactor

#### 10.1.1 Criterios WCAG relacionados

- a) 2.2.5 Re-autenticación
- b) 3.3.8 Autenticación accesible (Mínimo) (2.2. AA)
- c) 3.3.9 Autenticación accesible (Mejorada) (AAA)

#### 10.1.2 Objetivo de accesibilidad

Asegurar que los procesos de autenticación puedan ser completados por cualquier persona, independientemente de sus capacidades físicas, sensoriales o cognitivas, y sin depender exclusivamente de métodos visuales, temporizados o motrices.

Los mecanismos deben:

- a) Ofrecer alternativas perceptivas equivalentes (visual, auditiva, háptica o textual).
- b) Evitar obstáculos cognitivos o de tiempo que generen estrés o confusión.
- c) Permitir autenticarse sin tener que recordar datos complejos, priorizando la identificación basada en patrones, biometría o dispositivos confiables.
- d) Mantener consistencia y predictibilidad en el proceso (siempre los mismos pasos, en el mismo orden y diseño).

Ejemplos de incumplimiento:

- a) Formularios que cambian el orden o aspecto de los campos en cada acceso.
- b) Captchas solo visuales sin alternativa sonora o háptica.
- c) Tokens de segundo factor con tiempos excesivamente cortos.
- d) Errores de sesión sin explicación o que fuerzan a repetir todo el proceso.

El usuario debe sentir control y comprensión en todo el flujo de autenticación, no ansiedad o incertidumbre.

### 10.1.3 Objetivo de ciberaccesibilidad

Los procesos de autenticación requieren máxima claridad y previsibilidad, tanto para el usuario como para la arquitectura de seguridad.

Un diseño complejo o decorativo aumenta la probabilidad de error humano y la superficie de ataque.

Principios clave:

- a) Evitar elementos decorativos innecesarios o dinámicas visuales no funcionales en los formularios de acceso.
- b) Mantener la estructura constante y reconocible de los formularios.
- c) Si se usan captchas, identificarlos claramente como tales y mantener su patrón de aparición coherente. Cambios impredecibles generan confusión y facilitan ataques de inyección de campos falsos.

Gestionar cuidadosamente el 2FA/MFA:

- a) Evitar barras de tiempo visibles o temporizadores agresivos que generen estrés.
- b) Incluir mensajes tranquilos y claros, informando al usuario que dispone del tiempo necesario para completar el proceso.
- c) Garantizar que los tokens o mensajes OTP lleguen de forma inmediata y verificable, evitando la duda o repetición innecesaria de solicitudes.
- d) Ofrecer opciones para recordar dispositivos de confianza durante períodos limitados (15-20 días máximo) para reducir la fatiga de autenticación sin comprometer la seguridad.
- e) Prevenir el agotamiento por MFA (Multi-Factor Authentication Fatigue):  
notificar al usuario de forma explícita por qué y desde dónde se le está pidiendo autenticarse de nuevo.

### 10.1.4 Punto de convergencia “autenticación comprensible, seguridad sostenible”

Una autenticación accesible no solo permite el acceso a todos los usuarios, sino que también fortalece la seguridad al eliminar el error humano, el estrés y la confusión, principales aliados de los adversarios.

Desde la accesibilidad, se busca autonomía y comprensión total del proceso y desde la ciberseguridad, se busca consistencia, resiliencia y mínima exposición cognitiva al riesgo.

La convergencia se materializa en el principio de autenticación empática, donde el sistema entiende los límites humanos y los respeta, sin debilitar la integridad técnica.

### 10.1.5 Ejemplos prácticos y aplicables

| Escenario                         | Descripción                                                                     | Beneficio convergente                                     |
|-----------------------------------|---------------------------------------------------------------------------------|-----------------------------------------------------------|
| Captcha accesible multimodal      | Permite resolver el reto mediante audio, vibración o preguntas lógicas simples. | Garantiza acceso sin debilitar la validación humana.      |
| Mensajes calmados en MFA          | “Tómate tu tiempo, puedes abrir ahora tu app de autenticación.”                 | Reduce ansiedad, evita errores por prisa.                 |
| Diseño constante del login        | La interfaz de autenticación mantiene los mismos campos, colores y disposición. | Evita confusión y facilita detección de fraudes visuales. |
| Recordar dispositivo de confianza | Permite omitir MFA en equipos personales durante 15 días.                       | Disminuye fatiga cognitiva sin reducir seguridad.         |
| Reautenticación accesible         | Si una sesión expira, el usuario recupera su                                    | Previene frustración y pérdidas de información.           |

| Escenario | Descripción                          | Beneficio convergente |
|-----------|--------------------------------------|-----------------------|
|           | progreso tras autenticarse de nuevo. |                       |

Cuadro: Ejemplos prácticos y aplicables.

## 11. Bloque 10 sintaxis y semántica

### 11.1 Categoría

Coherencia técnica, precisión terminológica y consistencia estructural

#### 11.1.1 Criterios WCAG relacionados

- a) 4.1.1 Análisis sintáctico
- b) 4.1.2 Nombre, función, valor

#### 11.1.2 Objetivo de accesibilidad

Asegurar que todos los elementos de la interfaz —tanto visibles como subyacentes en el código— sean comprensibles, estructurados y semánticamente correctos, de modo que las tecnologías de asistencia (lectores de pantalla, navegadores adaptativos, dispositivos hápticos) puedan interpretarlos correctamente.

Principios esenciales:

- a) El contenido debe estar bien estructurado sintácticamente, cumpliendo los estándares HTML, ARIA y WAI para asegurar interoperabilidad.
- b) Todos los elementos deben tener nombre, rol y valor definidos, permitiendo identificar su función (por ejemplo, si un botón envía, cancela o confirma).
- c) La semántica textual debe ser coherente, predecible y libre de ambigüedad.
- d) El lenguaje técnico debe priorizar la claridad sobre la jerga, usando términos reconocibles y comprensibles para usuarios no especializados.

Ejemplos de incumplimiento:

- a) Botones sin etiqueta ARIA o con descripciones genéricas como “botón1”.
- b) Código HTML con etiquetas anidadas incorrectamente, provocando errores en lectores de pantalla.
- c) Formularios con roles o nombres inconsistentes (“enviar” y “guardar” en distintas pantallas para la misma acción).

- d) Uso de términos técnicos complejos o ambiguos sin explicación accesible.

### 11.1.3 Objetivo de ciberaccesibilidad

En procesos o acciones con riesgo para el usuario (autenticación, pago, cambio de datos, etc.), la claridad semántica y terminológica es un componente esencial de la seguridad.

Principios clave:

- a) Los mensajes y textos deben ser claros, precisos y consistentes, indicando de forma inequívoca qué ocurrirá cuando el usuario ejecute una acción (ej. Uso de *encriptar* en lugar de cifrar).
- b) La ambigüedad en los textos o etiquetas (por ejemplo, “continuar” sin indicar a qué paso lleva) genera confusión y abre la puerta a ataques de manipulación o engaño.
- c) La terminología debe ser correcta y universalmente comprendida, evitando tecnicismos incorrectos o confusos que deterioren la confianza del usuario.
- d) Este bloque actúa como criterio horizontal de simpleza cognitiva, conectado con todos los anteriores: un lenguaje claro es, a la vez, más accesible y más seguro.

### 11.1.4 Punto de convergencia “lenguaje claro igual a decisión segura”

La claridad sintáctica y semántica no solo mejora la accesibilidad, sino que disminuye los riesgos de error humano y manipulación.

Desde la accesibilidad, la corrección sintáctica y semántica garantiza que los usuarios —y sus tecnologías de asistencia— entiendan y ejecuten correctamente cada acción.

Desde la ciberseguridad, asegura que las instrucciones no induzcan interpretaciones erróneas ni dejen espacio a engaños cognitivos o a técnicas de ingeniería social.

Ambas dimensiones se encuentran en el principio de “transparencia operativa”: cada palabra y cada estructura deben reflejar exactamente lo que ocurre, sin adornos ni ambigüedades.

## 11.1.5 Ejemplos prácticos y aplicables

| Escenario                        | Descripción                                                      | Beneficio convergente                                               |
|----------------------------------|------------------------------------------------------------------|---------------------------------------------------------------------|
| Botones con función explícita    | “Eliminar archivo” en lugar de “Aceptar” o “Continuar”.          | Reduce confusión y evita errores destructivos.                      |
| Terminología técnica correcta    | “Cifrar” y “Descifrar” en lugar de “Encriptar” o “Desencriptar”. | Clarifica propósito y refuerza confianza.                           |
| Roles ARIA coherentes            | Cada elemento interactivo tiene nombre y rol definidos.          | Mejora interpretación por lectores de pantalla y reduce ambigüedad. |
| Estructura HTML válida           | Código limpio, bien anidado, con etiquetas coherentes.           | Previene errores funcionales y de interpretación.                   |
| Mensajes de acción comprensibles | “Al pulsar este botón, tu sesión se cerrará.”                    | Reduce la incertidumbre y mejora seguridad cognitiva.               |

Cuadro: Ejemplos prácticos y aplicables.

## 12. Anexo

### 12.1 Glosario de términos

Este anexo recoge los términos principales utilizados en la guía, junto con su definición en el contexto de la ciberaccesibilidad y la seguridad de las TIC.

**Accesibilidad digital:** capacidad de un sistema o servicio TIC para ser utilizado por todas las personas, incluidas aquellas con discapacidad o limitaciones funcionales.

**Ciberaccesibilidad:** práctica de diseñar, desarrollar y mantener sistemas digitales que sean simultáneamente accesibles, seguros y usables para todos los usuarios.

**Ciberseguridad inclusiva:** conjunto de medidas de seguridad diseñadas para no excluir ni dificultar el acceso de personas con discapacidad o diversidad funcional.

**WCAG (Web Content Accessibility Guidelines):** normas internacionales que establecen criterios para hacer el contenido web más accesible.

**UNE-EN 301 549:** estándar europeo que define los requisitos de accesibilidad para productos y servicios TIC.

**OWASP:** proyecto comunitario que define prácticas y metodologías para el desarrollo seguro de aplicaciones.

**ENS (Esquema Nacional de Seguridad):** marco normativo español que establece los principios y requisitos mínimos de seguridad de los sistemas TIC en el sector público.

**2FA / MFA (Autenticación multifactor):** procedimientos que requieren dos o más métodos de verificación para autenticar a un usuario.

**Fatiga cognitiva:** sobrecarga mental causada por el exceso de estímulos, tareas o información que afecta la atención o la comprensión del usuario.

## 12.2 Referencias normativas y técnicas

Este anexo compila las normas, guías y estándares que sirven como base o referencia metodológica para la elaboración de la presente guía.

WCAG 2.2 (W3C): pautas internacionales de accesibilidad para contenidos web.

UNE-EN 301 549:2021: requisitos europeos de accesibilidad para TIC.

CCN-STIC 817: guía de seguridad sobre desarrollo seguro de software.

CCN-STIC 823: guía sobre cumplimiento del Esquema Nacional de Seguridad.

OWASP Top 10: listado de las vulnerabilidades más comunes en aplicaciones web.

ISO/IEC 27001:2022: sistema de gestión de seguridad de la información.

ISO 9241-210:2019: ergonomía de la interacción persona-sistema, diseño centrado en el usuario.