Fundación GOODJOB

#aliadaSEC

PRINCIPIOS DE CIBERACCESIBILIDAD

Avancemos hacia sistemas digitales seguros, accesibles y cognitivamente sostenibles

INTRODUCCIÓN

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

Objetivo común

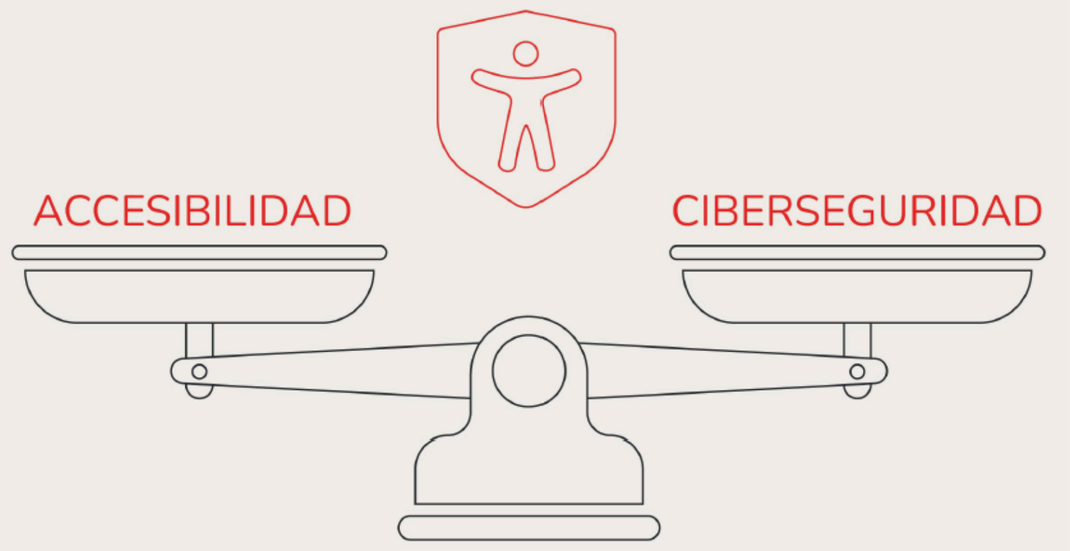
La accesibilidad digital y la ciberseguridad suelen abordarse como áreas independientes, pero en realidad comparten un objetivo común: reducir riesgos y mejorar la experiencia del usuario.

Este documento forma parte de la Guía de Buenas Prácticas en Ciberaccesibilidad elaborada por la Fundación GoodJob, con el objetivo de integrarse en todo Plan Director de Ciberseguridad.

¿QUÉ ES LA CIBERACCESIBILIDAD?

La ciberaccesibilidad es el **balance entre la accesibilidad y la ciberseguridad** de cada activo digital.
Consiste en aplicar principios y buenas prácticas para diseñar **sistemas digitales seguros e inclusivos**, garantizando que las medidas de seguridad no generen barreras adicionales y que las soluciones mantengan el nivel de protección adecuado.

Un entorno digital no accesible es más vulnerable

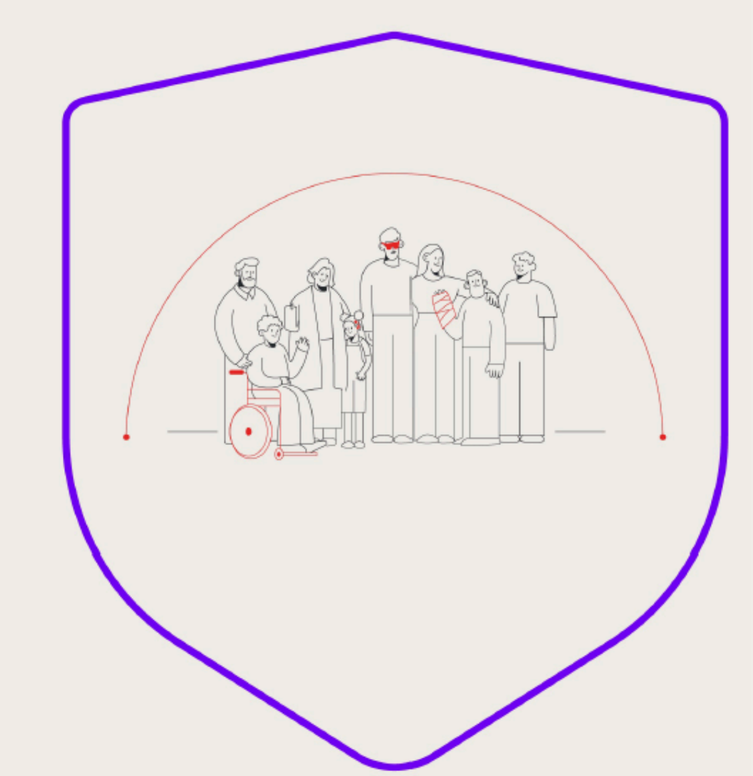


Beneficios clave de ciberaccesibilidad

1. **Reducción de vulnerabilidades:** Eliminación de puntos ciegos en el diseño digital.
2. **Cumplimiento normativo.**
3. **Concienciación ética:** Promoción de la accesibilidad como valor de seguridad.
4. **Inclusión real:** Participación activa de profesionales con discapacidad.
5. **Reputación reforzada:** Mejora de imagen ante clientes, usuarios y reguladores.

EL VALOR DE LA CIBERACCESIBILIDAD

El balance de ciberaccesibilidad depende del activo digital.
Cada sistema, aplicación o web requiere un enfoque adaptado para garantizar que la seguridad y la accesibilidad convivan sin generar barreras ni vulnerabilidades. No existe una solución única: el equilibrio varía según la naturaleza y criticidad del activo.



La falta de accesibilidad comporta riesgos de seguridad.

La ciberaccesibilidad es un componente estratégico de la seguridad digital, no solo una cuestión de inclusión.

Todo plan director de ciberseguridad debe contener un capítulo con el vector de accesibilidad digital = ciberaccesibilidad.

DISEÑO INCLUSIVO

Las personas con discapacidad ofrecen una perspectiva clave para mejorar la ciberaccesibilidad.

Porque lo que es accesible y seguro para ellas, lo es para el 90% de la población.

Diseñar sistemas que sean comprensibles, usables y seguros para todas las personas para que las medidas de protección no generen barreras de acceso.

Principios del diseño inclusivo aplicado a ciberaccesibilidad

- **Participación activa:** incluir personas con discapacidad en pruebas y validaciones.
- **Universalidad:** soluciones que funcionen para todos sin adaptaciones complejas.
- **Claridad y simplicidad:** interfaces y procesos comprensibles que minimicen errores críticos.
- **Compatibilidad tecnológica:** asegurar que las medidas de seguridad sean operables con tecnologías asistivas.

CUMPLIMIENTO NORMATIVO

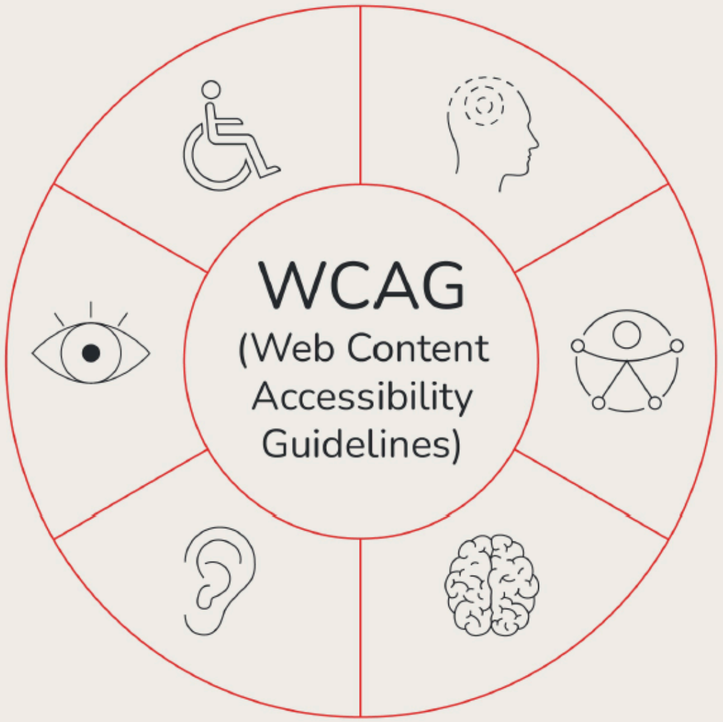
La ciberaccesibilidad está alineada con las **normas nacionales e internacionales** que establecen criterios para que plataformas, aplicaciones, sitios web y servicios digitales sean accesibles y seguros.

Pautas nacionales

- **ENS (Esquema Nacional de Seguridad):** Principios y requisitos mínimos de seguridad de los sistemas TIC en el sector público.
- **CCN-STIC 817:** Guía sobre desarrollo seguro de software.
- **CCN-STIC 823:** Guía sobre cumplimiento del ENS.

Pautas internacionales

- **WCAG 2.2 (W3C):** Accesibilidad para contenidos web.
- **UNE-EN 301 549:2021:** Accesibilidad para TIC.
- **OWASP Top 10:** Vulnerabilidades más comunes en aplicaciones web.
- **Acta Europea de Accesibilidad:** Garantiza que productos y servicios sean accesibles para las personas con discapacidad y las personas mayores en la UE.



ÁREAS CRÍTICAS EN CIBERACCESIBILIDAD

Las WCAG se organizan en 4 principios: **Perceptible, Operable, Comprensible y Robusto**. Cada uno incluye pautas que impactan en la accesibilidad y, por extensión, en la seguridad.

En este documento presentamos **10 bloques temáticos** relevantes para la ciberaccesibilidad, estableciendo la **correspondencia entre los criterios WCAG, objetivos de accesibilidad y objetivos de ciberseguridad**.

Estos criterios son clave para evitar brechas en la seguridad y garantizar entornos digitales inclusivos y confiables.

01

COLOR
Percepción confiable

02

IMÁGENES
Integridad semántica visual

03

TECLADO
Control del foco

04

PUNTERO
Confirmación perceptiva

05

EVENTOS
Visibilidad del estado

06

TIEMPO
Tiempo controlado

07

COMPRENSIÓN
Lenguaje como defensa

08

ERRORES
Sistemas impenetrables

09

AUTENTICACIÓN
Seguridad sostenible

10

SINTAXIS
Decisión segura

10 BLOQUES TEMÁTICOS

01 COLOR

El color no debe ser la única manera de transmitir información importante. **Usa contrastes para que todo el mundo pueda leer y entender el contenido.**

Mantener color + etiqueta fija en alertas oficiales (notificación segura del sistema) reduce riesgo de phishing visual o imitaciones.

02 IMÁGENES

Todas las imágenes importantes deben tener una **descripción de texto alternativo** (ALT) que explique su contenido.

Usar en los formularios tanto color como texto (error: campo vacío) y no solo una imagen, aumenta la comprensión y previene intentos de manipulación o engaño visual.

10 BLOQUES TEMÁTICOS

03 TECLADO

Todo lo que puedes hacer con el ratón también debe poder hacerse **usando solo el teclado**.

Con la navegación por teclado en formularios el usuario puede recorrer todos los campos con Tab, sin bloqueos ni saltos inesperados, evitando capturas del foco por scripts maliciosos.

04 PUNTERO

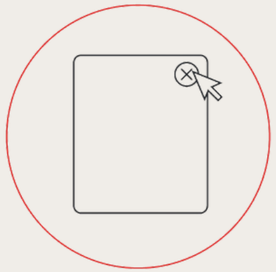
Todo evento iniciado con el puntero debe ser **visualmente confirmado, reversible y claramente delimitado**, de modo que el usuario tenga plena conciencia de su acción, su alcance y su resultado inmediato.

Los cambios claros de color o borde al pasar el puntero, mediante botones con hover/focus visible, ayuda a usuarios con visión reducida y evita clics en elementos invisibles o falsos.

10 BLOQUES TEMÁTICOS

05 EVENTOS

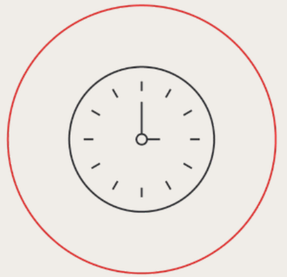
Los **elementos que aparecen al pasar el ratón** o al enfocar con el teclado (como menús desplegables o cuadros de información) deben ser **predecibles y estables**.



Una doble verificación visual en acciones críticas aumenta la conciencia del usuario y previene confirmaciones involuntarias.

06 TIEMPO

Cuando una web o aplicación tiene límites de tiempo (como sesiones que expiran), debe **avisar con antelación y permitir ampliar el tiempo fácilmente**.



Un aviso de sesión próxima a expirar que notifica con 60 segundos de antelación y ofrece “extender sesión”, evita pérdida de datos y mantiene la sesión segura.

10 BLOQUES TEMÁTICOS

07 COMPRENSIÓN Y PROPÓSITO

Los botones, enlaces y controles deben tener **etiquetas que expliquen** claramente **qué hacen**. Evita textos genéricos como "Clic aquí" o "Aceptar" sin contexto.

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.

08 ERRORES

Los mensajes de error deben ser **claros, amables y aparecer justo al lado del problema**.

Mostrar ejemplos de formato antes de rellenar campos sensibles (ej. Correo, fecha) reduce errores sin comprometer seguridad.

10 BLOQUES TEMÁTICOS

09 AUTENTICACIÓN

Los procesos de **inicio de sesión y verificación de identidad** (por ejemplo, los de tu banco) deben ser **sencillos de seguir**.

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.

10 SINTAXIS

La interfaz debe estar bien **organizada** y cada elemento debe tener un **nombre claro**.

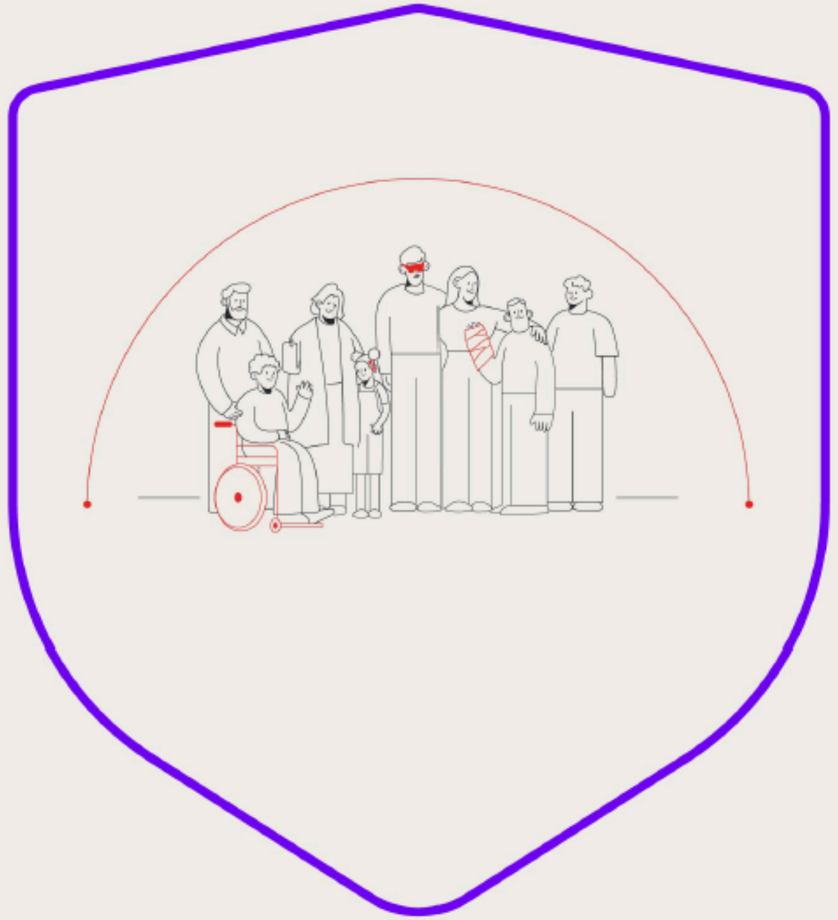
Los botones deben tener una función explícita; “eliminar archivo” en lugar de “aceptar” o “continuar”, reduce confusión y evita errores destructivos.

Fundación GOODJOB

#aliadaSEC

NUESTROS SERVICIOS

- Auditoría de ciberaccesibilidad.
- Identificación de riesgos derivados del diseño de interfaces.
- Buenas prácticas para el desarrollo seguro de servicios digitales.
- Concienciación sobre el impacto de la accesibilidad en la seguridad.

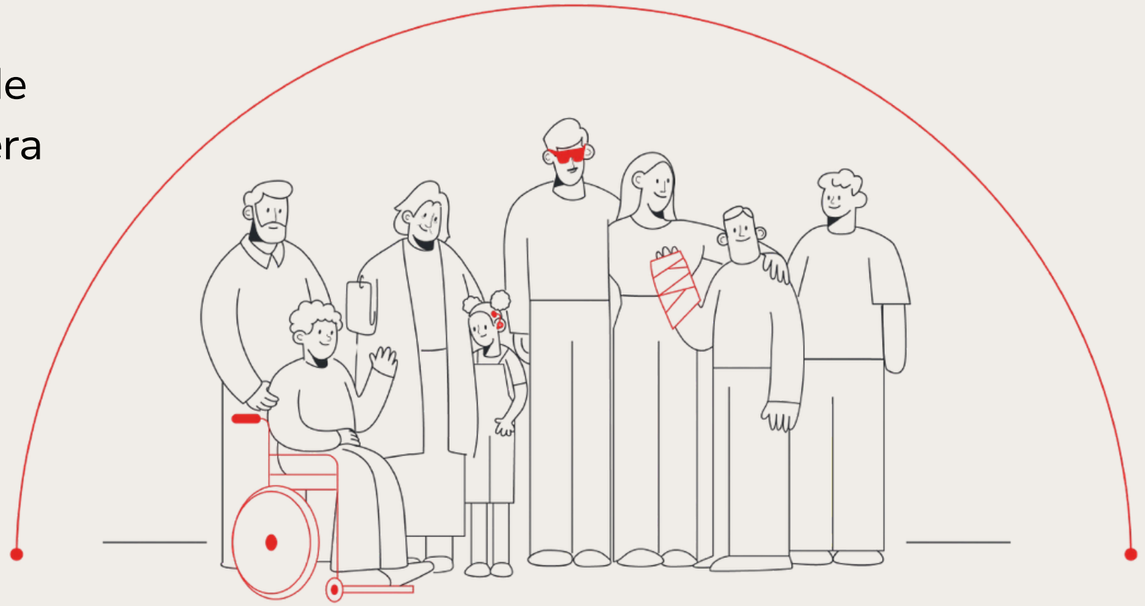


Fundación GOODJOB

#aliadaSEC

APOSTAR POR UN DISEÑO INCLUSIVO ES APOSTAR POR UN FUTURO DIGITAL PARA TODAS LAS PERSONAS

Estos principios de ciberaccesibilidad forman parte de la Guía de Buenas Prácticas del **proyecto #aliadaSEC**, una iniciativa pionera de la Fundación GoodJob para promover una **ciberseguridad inclusiva y confiable** en empresas e instituciones, integrando **accesibilidad y seguridad** como pilares de la transformación digital.



Descubre la Guía y comienza a aplicar la ciberaccesibilidad en tu organización.

Solicítala en: desarrollodeproyectos@goodjob.es

www.fundaciongoodjob.org

Con la colaboración de:

mtp DIGITAL BUSINESS ASSURANCE

CIBERSO

Revista SIC ciberseguridad, seguridad de la información y privacidad

Con el respaldo de:

CCN centro criptológico nacional