GUÍA DE SEGURIDAD DIGITAL

<para un sitio WordPress>

Versión para organizaciones de la sociedad civil

<K+LAB>

Fundación Karisma

Este trabajo se pudo realizar gracias al apoyo financiero de Open Society Foundation:

OPEN SOCIETY FOUNDATIONS

Se hizo en el marco de una práctica y una pasantía en alianza con la Universidad Nacional de Colombia, bajo la supervisión del profesor tutor Jorge Eduardo Ortiz Triviño.

Autora de la guía:
María Sol Botello León

Revisión y apoyo:
Stéphane Labarthe
Pilar Sáenz
Henry Zárate Ceballos
Jorge Eduardo Ortiz Triviño

Dirección Karisma:
Catalia Moreno Arocha.
Juan Diego Castañeda.

Corrección de estilo:
Laura Grisales.

Coordinación editorial:
Natalia Andrade Fajardo.

Identidad gráfica y diseño editorial:
Daniela Moreno Ramírez.

Contenido

Introducción

Las capacidades y necesidades de las Organizaciones de la Sociedad Civil (OSC) son distintas a las del sector público o privado. Muchas de ellas se financian a través de proyectos, lo que limita sus recursos operativos y dificulta la inversión en infraestructura digital o en personal especializado en tecnología. A pesar de ello, su trabajo centrado en causas sociales y su manejo de información sensible las convierte en un blanco atractivo para ataques cibernéticos.

Diversos estudios evidencian esta situación y la necesidad urgente de contar con medidas adecuadas de protección. Por ejemplo, una encuesta realizada en 2023 a organizaciones pertenecientes a International Geneva reveló que el 41 % había sido víctima de al menos un ataque digital en los últimos tres años. Además, estos incidentes no fueron aislados, sino que se presentaron de forma recurrente.

Aunque existen indicadores para medir incidentes de seguridad digital en sectores como el gubernamental y el empresarial, actualmente no hay datos específicos sobre las OSC en Colombia o América Latina. Desde Karisma hemos abogado por la creación de estos indicadores como un paso clave para diseñar respuestas más adecuadas.

Nuestra experiencia en el K+Lab, el Laboratorio de Seguridad y Privacidad de Karisma, muestra que los sitios web de las OSC suelen ser uno de los frentes más vulnerables en términos de seguridad digital. Los incidentes más comunes incluyen la caída de las páginas, la eliminación de contenidos y la suplantación de información.

En América Latina, la mayoría de las OSC utilizan sistemas de gestión de contenidos (CMS) para administrar sus sitios web, siendo WordPress lejos el más popular. Dado que muchas de estas organizaciones buscan mejorar su seguridad digital con recursos limitados, esta guía presenta recomendaciones clave para fortalecer la seguridad de sus sitios en WordPress.

Esta guía tiene un objetivo:

Definir un conjunto de buenas prácticas para el despliegue de sitios web en las Organizaciones de Sociedad Civil (OSC) latinoamericanas para optimizar su postura de seguridad digital y poder autoevaluarse.

¿Cómo lo vamos a hacer?

A través de recomendaciones generales y específicas en cuatro áreas clave para la seguridad de sitios web de organizaciones de la sociedad civil en América Latina, este documento ofrece orientaciones pensadas especialmente para sitios desarrollados en WordPress. Los temas abordados son: dominios y subdominios, copias de respaldo, actualizaciones, y gestión de permisos y accesos.

Dichas recomendaciones están dirigidas a los administradores de los sitios web de OSCs. En caso de que el sitio web de alguna organización sea gestionado externamente, esta guía también busca que los miembros de las OSC sepan qué cambios pueden pedir para asegurar su sitio web.

¿Qué herramientas, accesos y conocimientos son necesarios?

Para llevar a cabo las recomendaciones, se necesita tener acceso administrativo al CMS de WordPress y, en algunos casos, al servidor y al panel de control de dominio. Sin embargo, si no se tienen estos accesos, se pueden solicitar los cambios a la persona o empresa que maneja dichas herramientas normalmente.

¿Por qué hace falta esta metodología?

Existen diversos recursos sobre seguridad digital para las OSC, como Safetag, Security in a Box y el Manual de Ciberseguridad; aunque cubren diversos temas y niveles de complejidad, no proporcionan una guía amigable y adaptada a las necesidades de seguridad de los sitios web de las OSC.

Otro material útil para las organizaciones de la sociedad civil es el sitio web *chequea.la*, que ofrece recomendaciones valiosas sobre seguridad web en un contexto general. Es una excelente herramienta complementaria a esta guía, ya que aborda una amplia variedad de temas con un enfoque accesible. Por su parte, esta guía se centra específicamente en el gestor de contenidos WordPress, lo que nos permitió ofrecer recomendaciones más detalladas y concretas, adaptadas a un entorno que hoy es común para la mayoría de las OSC.

Menos es más

Imagina tu sitio web como un apartamento: mantenerlo ordenado y seguro implica evitar acumular objetos innecesarios o peligrosos. Igualmente, decides quién puede entrar, cuándo y qué puede hacer en su interior.

Un enfoque que facilita la gestión del sitio web es restringirlo a lo esencial. Pregúntate, ¿qué debe tener para satisfacer las necesidades de la organización? Incorpora sólo aquello que sea necesario.

Desactiva funcionalidades innecesarias o en desuso y, antes de incorporar una nueva herramienta, revisa si su mantenimiento y protección son sostenibles en el tiempo para tu organización y cuáles son los eventuales impactos en términos de protección de datos personales.

Busca por ti mismo

Esta guía es un buen punto de partida para fortalecer la seguridad de tu sitio web. Te invitamos a tomarte el tiempo para revisar las recomendaciones y evaluar cómo pueden implementarse de forma sostenible en tu organización.

Si bien no incluimos instrucciones detalladas paso a paso, nuestro objetivo es que sepas qué buscar. Con el apoyo de internet y, si lo necesitas, herramientas de traducción en línea, podrás encontrar la información necesaria para aplicar estas recomendaciones con mayor confianza.

No te abrumes… Estás dando un primer paso

Reconoce que cada pequeño avance es significativo. Comienza con lo que puedes hacer; lo esencial es que estás dando el primer paso.

La seguridad digital no es un estado final, sino un esfuerzo continuo que depende de tus necesidades y contexto. Para que tus esfuerzos sean sostenibles, pregúntate: ¿cómo puede tu organización implementar estas buenas prácticas a largo plazo?

Tu misión, si decides aceptarla, es fortalecer la seguridad de tu sitio web hasta alcanzar un nivel que responda a las necesidades de tu organización. Para la mayoría de las OSC, esto implica contar con un sitio capaz de prevenir incidentes y, en caso de que ocurran, de recuperarse de manera efectiva.

Si encuentras una gran diferencia entre las necesidades de tu organización y los recursos de los que dispone, también puedes usar esta guía para abogar por recursos de sostenimiento informático.

Esta guía busca caracterizar un sitio web que cumpla estos requerimientos. Si tu organización necesita más, recuerda que esto es solo el comienzo: hay mucho más por aprender y aplicar en el camino hacia una infraestructura digital robusta y resiliente.

Glosario

Definiciones obtenidas y adaptadas de Wikipedia

Dominio (web): Parte principal de una dirección web. Suele indicar la persona, organización o compañía que administra el sitio web o página en cuestión. Por ejemplo, en la dirección “www.ejemplo.com”, el dominio sería “ejemplo.com”.

Extensión: Última parte de una dirección web. Por ejemplo, en “ejemplo.com” la extensión es “.com” que suelen usar las empresas de uso comercial. Las extensiones que suelen usar las OSC y que son en general más adaptadas para ellas son el “.org”, “.ong” y “.ngo”.

Gestor de contenidos (CMS): Herramienta o programa que permite crear, organizar y gestionar la información de un sitio web sin necesidad de conocimientos avanzados en programación. El más usado es WordPress.

Hosting (o alojamiento web): Servicio que provee a los usuarios de Internet un espacio de almacenamiento en línea, que permite publicar todo el contenido relacionado con un sitio web. Hay muchas empresas privadas que ofrecen hosting

Panel de control de dominio: Herramienta que permite gestionar los aspectos relacionados con un nombre de dominio. Desde aquí puedes realizar tareas como renovar el dominio, configurar subdominios o definir la dirección IP del servidor web.

Principio de mínimo privilegio: Principio de seguridad según el cual un sistema debe restringir los privilegios de acceso de los usuarios al mínimo necesario para realizar las tareas asignadas. least privilege - Glossary | CSRC

Registrador de dominio o Registrar: Empresa o entidad a la cual se puede reservar o comprar un dominio de Internet. En general el individuo o la entidad paga una cuota anual a cambio de tener el nombre de dominio.

Servidor DNS: Es el sistema que traduce los servicios de un dominio web (sitio web, correo, etc.) en direcciones IP, que son necesarias para que los navegadores puedan cargar el contenido del sitio web. Sin este servicio, no podríamos acceder fácilmente a las páginas de Internet. Se suele configurar desde el panel de control de dominio.

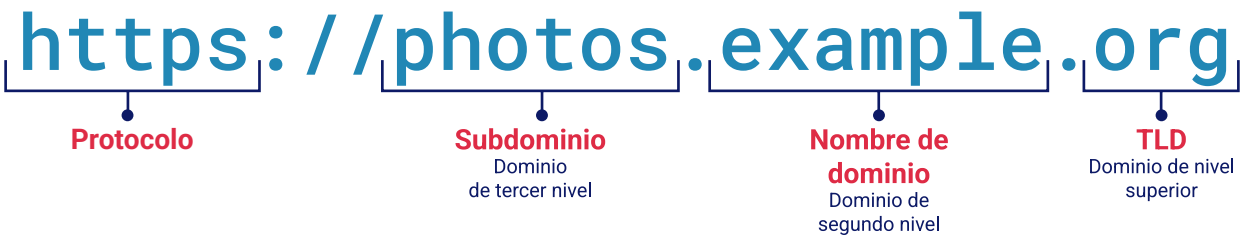
Servidor (web): Ordenador o sistema que almacena los archivos y datos de un sitio web, y los entrega a los usuarios cuando acceden a la página. Es como el "almacén" de tu sitio en Internet.

Soporte: Mantenimiento que reciben las tecnologías para garantizar su funcionamiento correcto. Esto incluye actualizaciones, resolución de problemas, implementación de parches de seguridad y compatibilidad con otras tecnologías. Sin este soporte, el uso de una tecnología puede volverse riesgoso o ineficiente.Subdominio: Subgrupo o subclasificación del nombre de dominio, que podría considerarse como un dominio de segundo nivel. Por ejemplo, en la dirección "blog.ejemplo.com", el subdominio sería "blog". Permiten separar las diferentes partes de un sitio web para organizar los contenidos.

UDRP (Política Uniforme de Solución de Controversias en materia de Nombres de Dominio): Proceso establecido por la ICANN para la resolución de disputas relacionadas con el registro de dominios de Internet.

Dominios y subdominios

Componentes de URL con subdominio



La extensión, los dominios y subdominios de tu sitio web son importantes.

Los dominios permiten que las personas encuentren tu sitio web, y los subdominios, te permiten dividirla y organizarla.

En el caso específico de las ONG, encontramos que se suelen usar nuevos dominios o subdominios para generar publicaciones asociadas a un proyecto específico, lo que se llamaremos un “micro sitio”.

Sin embargo, tener demasiados dominios o subdominios puede ser perjudicial para la organización, dado que pueden suponer una carga significativa para su mantenimiento y actualización. Y, en caso de que este no se realice, representan puntos de vulnerabilidad adicionales que pueden ser comprometidos.

Tip:

Si tu organización está en el momento de escoger un dominio.

Evita escoger uno con una extensión (TLD) no adaptada como el .com, que suele ser usado por empresas comerciales. Es ideal conseguir un dominio cuya extensión muestre que pertenece a una OSC como .org, .ong, .ngo, para aportar fiabilidad al sitio. Estas tres extensiones son gestionadas por el Public Internet Registry (PIR). La extensión org es de libre acceso, mientras que las extensiones ong o ngo , que son más recientes, necesitan demostrar cumplir ciertos criterios específicos cómo ser una entidad sin ánimo de lucro. También puedes utilizar la extensión territorial de tu país, como lo es .co u .org.co para el caso de Colombia.

Acá te proponemos una serie de acciones para simplificar su gestión y reducir riesgos.

Desactiva dominios y subdominios no usados

Es posible olvidarse de gestionar o de desactivar los dominios, especialmente cuando han sido creados para un proyecto que ya se terminó.

Revisa cuáles dominios y subdominios deben permanecer en línea. Asegúrate de que estén correctamente gestionados. Los que ya no se usen pueden desactivarse para mitigar riesgos de forma efectiva, reducir la carga de mantenimiento y eliminar posibles vulnerabilidades.

Para revisar esto, ten en cuenta que cada subdominio se muestra como una o más entradas en el servidor DNS del dominio. Primero, se debe revisar la lista de dominios y subdominios existentes, usando la parte DNS del panel de control de dominio. Si no puedes acceder, se pueden encontrar listas de estos dominios y subdominios (potencialmente no precisas) en herramientas como DNSdumpster o con ayuda de buscadores como Google.

Si identificas subdominios que deben desactivarse, el procedimiento debe hacerse desde el panel de control del dominio. Los pasos pueden variar según el panel que estés utilizando.

Planificar renovaciones de nombre de dominio

Cuando un dominio es adquirido, se registra en bases de datos públicas que almacenan información sobre los propietarios de los dominios.[1] Este registro asegura que el comprador es reconocido como el titular legítimo del dominio por un período determinado.

El registro de un dominio generalmente tiene una duración de un año. Al finalizar este período, el propietario debe renovarlo para mantener el control sobre él. Si no se realiza la renovación a tiempo, el dominio puede ser adquirido por terceros, quienes podrían utilizarlo con fines legítimos o intentar extorsionar al propietario original exigiendo una

1 https://www.colcert.gov.co/800/w3-article-198650.html

suma elevada de dinero a cambio de devolverlo, lo que se conoce como “secuestro de dominios”.

Para asegurarse de renovar el subdominio a tiempo puedes tomar las siguientes medidas:

1) Realiza seguimiento a las fechas de renovación

La fecha de vencimiento del dominio se puede revisar a través de su panel de control. Por lo general, la empresa proveedora del dominio suele enviar alertas por correo. Si no puedes acceder, revisalas ingresando el dominio en estas páginas https://lookup.icann.org/es o https://veni.chequea.la/, ya que las fechas son públicas.

Calcula el tiempo necesario para que la renovación de un dominio sea efectiva, considerando también el tiempo que pueda tomar el proceso administrativo dentro de tu organización para completar la compra.

Puedes armar un calendario propio o usar las alertas automáticas que llegan al correo electrónico registrado para acordarte. **¡Lo importante es que no se te pase la fecha!**

2) Activa la renovación automática

La renovación automática es una forma conveniente de renovar tu dominio sin necesidad de intervención manual, los cobros se realizan de forma automática en cada renovación.

Igualmente, es aconsejable verificar que el cobro se haya realizado correctamente, ya que si el pago es rechazado, no se renovará el dominio. Además, el precio del dominio puede variar, por lo que es recomendable revisar previamente la política de devolución de tu proveedor de dominios, en caso de un cobro involuntario.

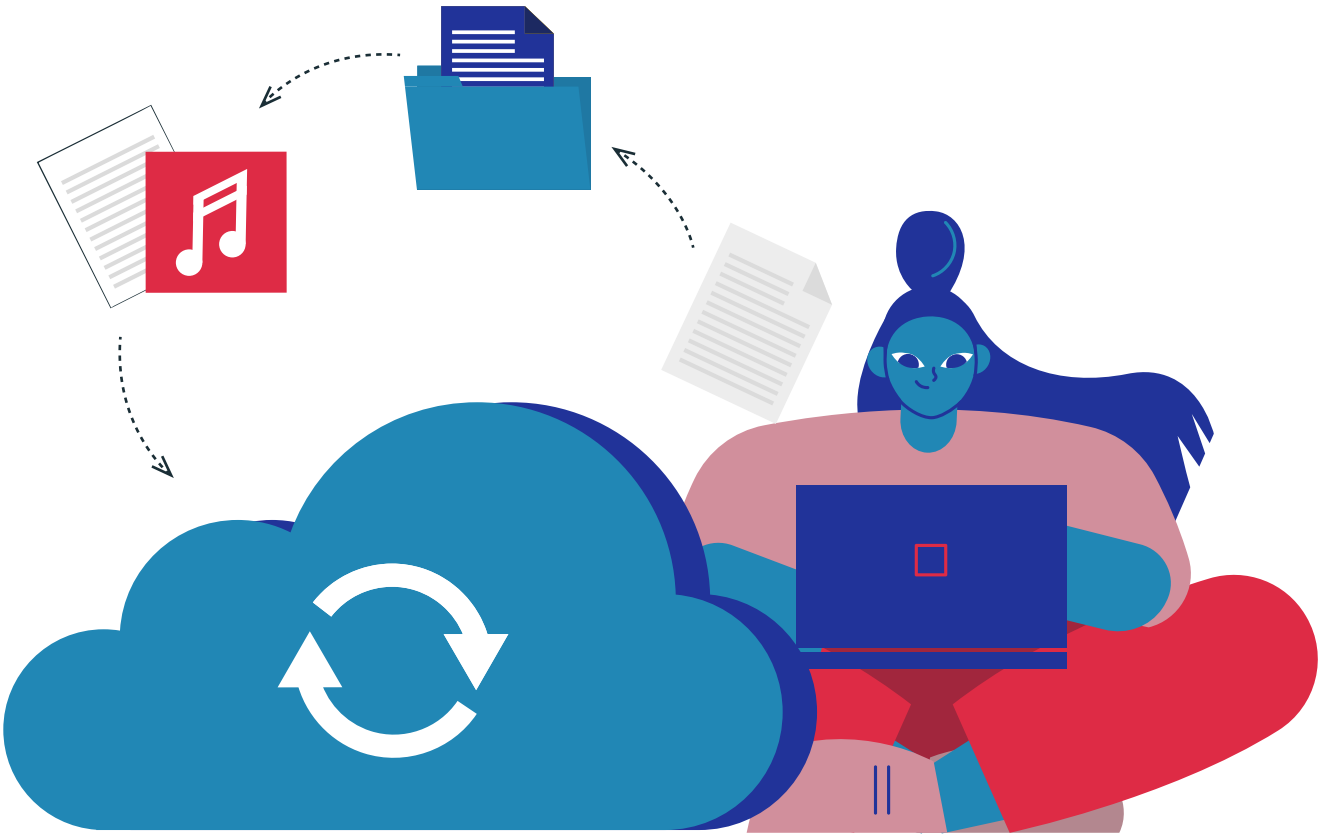
3) Monitorea tu marca

Dominios similares al dominio de tu sitio web pueden ser confundidos por tus usuarios, lo que representa una posible amenaza de suplantación.Si el presupuesto de tu organización lo permite, puedes prevenir el problema al registrar algunos dominios similares, evitando que terceros los adquieran.

En caso de detectar un sitio web que esté suplantando el tuyo, es posible recuperar los nombres de dominio mediante una demanda ante la ICANN, utilizando el Proceso Uniforme de Resolución de Disputas de Nombres de Dominio (UDRP).

Si además de esta suplantación se están incumpliendo las reglas y políticas de la extensión, por ejemplo difundiendo imágenes sexuales no consensuadas, actividades ilegales o fraudulentas, se puede denunciar directamente a la entidad que lo gestiona. En el caso del ".org", ".ong" y ".ngo", se puede denunciar con el Registrar o con el Public Internet Registry en esta dirección: abuse@pir.org

Copias de respaldo



Una **copia de respaldo** (de seguridad o *backup*) es una copia del sitio web que se usa en caso de que la información original se pierda o se dañe en caso de una falla o incidente grave..

Las copias de respaldo son esenciales para prevenir la pérdida irreversible de información y garantizar la continuidad operativa ante diversas eventualidades, como errores humanos, fallos tecnológicos o ataques informáticos, especialmente en casos de secuestro de datos o ransomware.

No obstante, la utilidad de una copia de respaldo depende de su calidad y actualización. Por ejemplo, una única copia que sea demasiado antigua o esté dañada no sirve de mucho.

¿Cómo realizar una copia de respaldo en WordPress?

Las copias de respaldo en WordPress se pueden realizar de diversas maneras:

- **Copias de respaldo manuales:** de los archivos y la base de datos de WordPress.
- **Plugins de copias de respaldo:** Permiten crear y programar copias de respaldo automáticas. Uno de los más populares es Duplicator[2].
- **Copias por los servicios de alojamiento web:** Algunos proveedores de hosting ofrecen servicios de copia de seguridad automáticos de un servidor web, la cual es ideal en conjunto con una copia de seguridad propia. Revisa que las condiciones de entrega de la copia de seguridad sean viables tanto en el tiempo de respuesta, como en el formato de la misma.
- **Máquina virtual que hospeda el servidor web:** Ciertas OSC con más capacidades alquilan o poseen un servidor físico que hospeda la máquina virtual con el servidor web. En este caso, también se pueden hacer copias de respaldo de esta máquina virtual.

En este link encontrarás instrucciones para respaldar los archivos y la base de datos de WordPress. También están algunos links recomendados para hacer la automatización de las copias de respaldo.
https://codex.WordPress.org/es:Copias_de_seguridad_de_WordPress

> **Nota:** Prueba que tus copias de respaldo funcionen, por lo menos una vez. Intenta reconstruir el sitio web a partir de una de ellas y analiza qué se podría mejorar.

2 https://es.WordPress.org/plugins/duplicator/

Protocolos de copias de respaldo

Como decíamos anteriormente, no basta con que exista una copia de seguridad si esta está desactualizada o dañada. Para que sea útil en caso de ser necesaria, esta debe ser relativamente reciente y estar en buen estado.

Para asegurarte de siempre tener una copia de seguridad útil, debes tener estrategias definidas o **protocolos** para la creación y el almacenamiento de las copias y seguirlos. Un protocolo de copias de respaldo debe definir qué datos se van a respaldar, cada cuánto, cómo y dónde. Estos protocolos dependen del tipo de sitio web y de organización.

Puedes crear diferentes protocolos que se complementen entre sí para respaldar los diferentes componentes de un sitio web. Por ejemplo, puedes copiar la base de datos todas las semanas, pero el WordPress completo, sólo cada dos meses.

Importante: ¡Es mejor tener una copia de seguridad imperfecta que no tener ninguna! Ajusta el protocolo de acuerdo a las capacidades y necesidades de tu organización.

¿Qué datos respaldar?

Una copia de seguridad debe tener la información necesaria sin ser demasiado voluminosa, por lo que se debe escoger la información que se va a respaldar. Para esto, ten en cuenta estas recomendaciones:
Prioriza datos críticos para el funcionamiento de tu organización. Por ejemplo, los datos de los usuarios o las bases de datos.

Excluye información irrelevante. Por ejemplo, algunos plugins pueden ser voluminosos e innecesarios en la copia de seguridad.

Establece límites y expectativas sobre el tiempo de conservación de los archivos respaldados, en función de su relevancia y antigüedad.

Comprime la copia de seguridad para que utilice menos espacio.

¿Cada cuánto tiempo respaldar?

La frecuencia de las copias de respaldo depende de varios factores como: el tipo de sitio web, la frecuencia de publicaciones y la gravedad de perder la información desde la última copia realizada. Además, diferentes componentes de tu sitio web pueden necesitar copias de respaldo con distintas periodicidades.

Por ejemplo, un blog con pocas publicaciones mensuales puede respaldar las carpetas de contenido una vez por semana y hacer una copia completa de WordPress cada tres meses. En estos casos, se recomienda a los editores guardar una copia personal de sus publicaciones semanalmente. Por otro lado, un sitio web con mayor actividad requeriría copias de seguridad más frecuentes.

También se puede hacer una copia de seguridad preventiva en ciertos contextos específicos, por ejemplo, en caso de publicaciones sobre temas sensibles. Desde K+Lab tuvimos que asistir varias veces a OSC cuyos sitios webs fueron atacados justo después de una publicación sobre temas sensibles.

Tips:

Asegúrate siempre de tener una copia de seguridad reciente del WordPress antes de actualizarlo, ya que este proceso puede fallar fácilmente.

Automatizar las copias de respaldo es una manera confiable de mantenerte al día.

Puede ser útil tener un **histórico** de copias de respaldo. Por ejemplo, tener una copia de hace tres meses o un año para no depender únicamente de la última copia creada, en caso de que esta esté dañada.

¿Cuántas copias y dónde las guardo?

Imagina que se daña tu sitio web y necesitas restaurarlo a partir de una copia de seguridad que tienes en tu disco duro externo. Sin querer lo dejas caer y este deja de servir. Así de fácil pueden fallar al mismo

tiempo el sitio web y una copia de seguridad. Por esto, recomendamos tener varias copias de respaldo en distintos lugares o dispositivos.

En particular, puedes aplicar la regla 3-2-1 para protegerte frente ante diferentes riesgos. Esta regla establece que:

- **3:** Mantén al menos 3 copias de tus datos: La copia principal y dos copias de respaldo.
- **2:** Almacena las copias en 2 tipos de dispositivos diferentes.
- **1:** Guarda 1 de las copias fuera de tu sitio de trabajo, para protegerte frente a desastres locales. Puedes guardarlo en una nube que no sea la de uso cotidiano de la organización o en un disco duro en tu casa.

Tip:

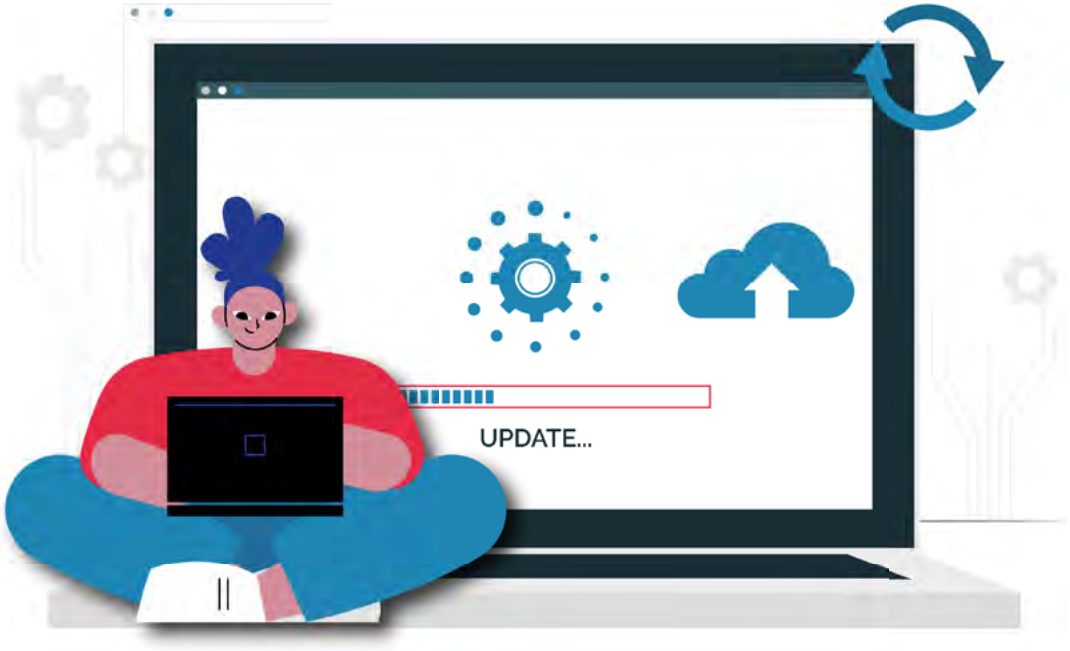
¿Qué hacer si no había hecho ninguna copia de seguridad y perdí todo el contenido de mi sitio web?

Existe un sitio que se llama “Archive.org” que hace copias automáticas de sitios webs que detecta. Por lo tanto, es probable que se hayan hecho copias de tu sitio web sin que lo sepas. Lo puedes verificar en esta url: https://web.archive.org/

Si es el caso, puedes seleccionar la última copia que hizo Archive.org y guardar manualmente las páginas. No es una copia del WordPress y de sus bases de datos sino de cada página de tu sitio una por una. Por lo tanto se necesitará un trabajo manual para reconstruir cada página, pero es mejor que nada. Además Archive también puede ser útil en el periodo de transición entre el incidente de seguridad en tu sitio web y la reconstrucción de su sitio web, ya que esta copia sigue accesible.

También puedes pedir a Archive.org de manera proactiva que copie tu página web desde esta url: https://help.archive.org/help/save-pages-in-the-wayback-machine/

Actualizaciones



Las actualizaciones no solo aportan mejoras y nuevas funcionalidades, también suelen incluir parches de seguridad que corrigen vulnerabilidades descubiertas en versiones anteriores. Además, ayudan a mantener la compatibilidad con otras tecnologías.

Por eso es importante mantener actualizadas las tecnologías de tu sitio web. Para lograrlo, tu organización puede definir un protocolo de actualización que considere sus recursos y necesidades, de modo que el proceso sea sostenible a largo plazo.

Si la carga de actualizaciones es demasiado alta, es recomendable reducir la cantidad de elementos que necesitan ser actualizados, y así evitar generar brechas de seguridad (aquí aparece de nuevo la filosofía ‘menos es más’). Otra opción, si la información es importante, es presentar este punto ante posibles financiadores de la organización.

En general, recomendamos:

- **Actualizar regularmente las distintas tecnologías**, idealmente una vez al mes y siempre que se conozca una nueva vulnerabilidad o el sistema indique una actualización disponible.

- **Mantener copias de respaldo actualizadas y seguras.**

- **Utilizar un entorno de prueba previo y/o elaborar una matriz de compatibilidad**, para asegurarte de que el sitio no se vea afectado al realizar actualizaciones importantes.

Dependiendo de la importancia de la actualización, la complejidad de la infraestructura web y de las prioridades de la organización, puede ser recomendable utilizar la actualización automática o, de lo contrario, revisar cuidadosamente la compatibilidad de las actualizaciones.

Diferentes componentes

En un sitio web de WordPress hay múltiples tecnologías que deben actualizarse, como el gestor de contenido WordPress en sí mismo, el tema y todos los plugins. Para poder utilizar las versiones actualizadas de estas, es necesario que el **servidor** en el que se está hospedado el sitio web provea a su vez PHP, MySQL y el servidor web mismo estén actualizados. Para conseguir esto, puede ser necesario comunicarse con el administrador del servidor o la empresa de hosting.

Plugins y temas

WordPress, como producto, depende en gran medida de la instalación de plugins, muchos de los cuales son desarrollados por terceros. Por eso, es fundamental asegurarse de que los plugins y temas que se utilicen cuenten con soporte activo, es decir, que sus desarrolladores publiquen actualizaciones de manera periódica.

Aquí encuentras el paso a paso oficial para realizar esas actualizaciones en tú página web:
https://WordPress.com/es/support/plugins/actualiza-un-plugin-o-tema/

Plugins y temas fuera de soporte

Cuando un plugin o tema deja de recibir soporte, es recomendable reemplazarlo debido a la ya mencionada falta de actualizaciones y de parches de seguridad. Aún más, depender de un plugin o tema sin soporte suele llevar a utilizar versiones desactualizadas de otras tecnologías, debido a problemas de compatibilidad. Esto empeora la desactualización de las tecnologías del sitio web y las consecuencias que esto tiene.

Para que esto no le ocurra a tu sitio web, es importante que los nuevos plugins que añadas reciban soporte activo por parte de los desarrolladores. Además, es necesario que revises periódicamente que tus plugins sigan bajo soporte.

WordPress

Existen múltiples formas para actualizar WordPress, aquí encuentras un paso a paso en español
https://codex.WordPress.org/es:Actualizar_WordPress

Normalmente, al acceder a la interfaz de administración de WordPress, aparecen alertas que indican si hay actualizaciones disponibles para el núcleo de WordPress, los plugins o los temas, como se muestra en este pantallazo:

Tip:

Antes de realizar cualquier actualización importante, asegúrate de hacer una copia de respaldo de tu sitio web. Si algo sale mal durante el proceso, una copia de seguridad puede ser la diferencia entre una simple restauración y la pérdida total del sitio.

Revisa compatibilidad

Un sitio web de WordPress está compuesto por una combinación de lenguajes de programación, bases de datos y plugins externos que interactúan entre sí. Si alguna de estas tecnologías no es compatible con otra después de una actualización, puede generar fallos en el funcionamiento del sitio, desde errores en la carga de las páginas hasta problemas más graves como vulnerabilidades de seguridad o pérdida de datos.

Por esto, es importante evaluar la compatibilidad entre las tecnologías existentes y las nuevas versiones que se desean implementar, antes de realizar cualquier cambio. Puedes hacer esto de diferentes maneras:

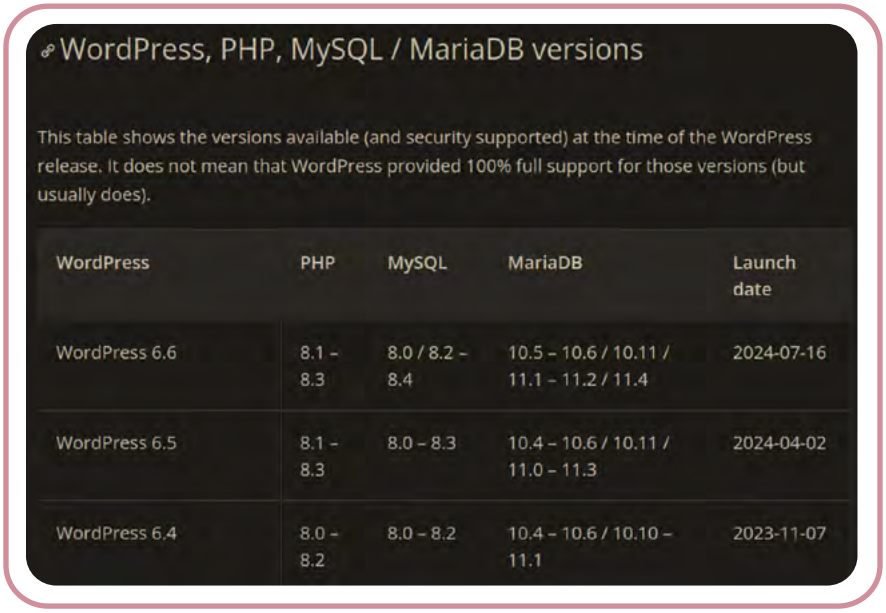
Matrices de compatibilidad

Una matriz de compatibilidad permite visualizar de manera clara las interdependencias entre las distintas tecnologías utilizadas y cómo cada versión interactúa con las demás.

Las matrices de compatibilidad ayudan a decidir a qué versiones de cada tecnología actualizar en un sitio web, ya que indican cuáles son compatibles entre sí. Esto permite evitar conflictos o errores al momento de realizar una actualización.

Puedes consultar matrices de compatibilidad en https://make.WordPress.org/hosting/handbook/compatibility/.

Por ejemplo, en la imágen podemos observar que WordPress 6.6 es compatible con PHP 8.1 a 8.3, con MySQL 8.0 y 8.2 a 8.4.



WordPress, PHP, MySQL / MariaDB versions

This table shows the versions available (and security supported) at the time of the WordPress release. It does not mean that WordPress provided 100% full support for those versions (but usually does).

WordPress	PHP	MySQL	MariaDB	Launch date
WordPress 6.6	8.1 – 8.3	8.0 / 8.2 – 8.4	10.5 – 10.6 / 10.11 / 11.1 – 11.2 / 11.4	2024-07-16
WordPress 6.5	8.1 – 8.3	8.0 – 8.3	10.4 – 10.6 / 10.11 / 11.0 – 11.3	2024-04-02
WordPress 6.4	8.0 – 8.2	8.0 – 8.2	10.4 – 10.6 / 10.10 – 11.1	2023-11-07

Otra opción es hacer tu propia matriz de compatibilidad listando todas las tecnologías claves para tu sitio web que puedan tener conflictos (plugins, WordPress, PHP, base de datos, entre otras).

Para crear una matriz de compatibilidad, se deben listar las tecnologías clave en filas y columnas, organizando cada una según su versión o variante. Luego, en cada intersección de la matriz, se indica si las versiones respectivas son compatibles, incompatibles o si requieren algún ajuste adicional. Para encontrar esta información puedes revisar la documentación técnica o consultar bases de datos de compatibilidad ya existente.

Entorno de pruebas

Para las organizaciones con más experiencia y recursos, es recomendable trabajar con un entorno de pruebas: una réplica del sitio web donde se pueden implementar y evaluar cambios sin afectar la experiencia de las personas usuarias ni comprometer el funcionamiento del sitio. Este entorno puede alojarse en un subdominio dedicado solo a esto.

El entorno de pruebas permite identificar posibles incompatibilidades, fallos de funcionalidad o problemas de rendimiento antes de que los cambios se apliquen en el entorno de producción. Aquí puedes leer sobre cómo crear y utilizar uno:

https://WordPress.com/es/support/crear-un-sitio-de-pruebas/

Actualización automática

Otra opción es configurar la actualización automática para los plugins, los temas y las versiones menores de WordPress. Esto garantiza la aplicación oportuna de parches de seguridad y mejoras de rendimiento, reduciendo así el riesgo de vulnerabilidades. Sin embargo, ten en cuenta que algunas actualizaciones pueden afectar la compatibilidad con ciertos plugins o temas y provocar fallos en el sitio. Por eso, es fundamental seguir un buen protocolo de copias de respaldo.

Tomar esta decisión dependerá de qué es lo importante para la organización: tener una página permanentemente en línea,disminuir la cantidad de recursos que consume su gestión o ambas opciones sin sacrificar la seguridad del sitio web.

Aquí tienes tutoriales para activar las actualizaciones automáticas.
https://es-mx.WordPress.org/support/article/plugins-themes-auto-updates/

https://developer.WordPress.org/advanced-administration/upgrade/upgrading/#configuring-automatic-background-updates

¿Reconstruir el sitio web para actualizarlo?

En algunos casos no es posible actualizar los componentes del sitio web, especialmente cuando la actualización tiene importantes cambios o se debe actualizar el PHP.

En este caso es posible migrar los datos del sitio a un nuevo ambiente a partir de una copia de respaldo como se explica en este enlace:

https://support.hostinger.com/es/articles/6149777-como-restaurar-un-sitio-WordPress-con-solo-una-copia-de-la-base-de-datos

Gestión de permisos y accesos

Uno de los vacíos de seguridad más importantes en las OSC son los permisos y accesos que mantienen personas que no los necesitan o que ya no pertenecen a la organización.

Mínimos permisos y accesos

Una gestión segura de los permisos y accesos en una organización se caracteriza por seguir el **principio de mínimo privilegio**: cada persona usuaria tiene únicamente los permisos y accesos necesarios para cumplir con su función.

Esto permite tener control sobre el acceso a los distintos niveles de gestión del sitio, lo cual minimiza riesgos de seguridad frente a un acceso no autorizado. Además, previene errores involuntarios por usuarios inexpertos.

En WordPress

WordPress permite asignar diferentes roles a las personas usuarias: *administrador*, *editor*, *autor*, *colaborador*, y *suscriptor*, cada uno con distintos niveles de acceso y capacidad. Puedes encontrar más información aquí Roles and Capabilities – Documentation – WordPress.org. Para modificar los roles: User Management | Learn WordPress

Por ejemplo, un pasante del área de comunicaciones no necesita permisos de administrador del sitio web. Podría tener los roles de *editor* o de *autor*.

Revisión periódica de permisos y accesos

Como el equipo de una organización cambia con el tiempo, te recomendamos añadir y eliminar los permisos y accesos del sitio web para reflejar estos movimientos de personal

Para revisar que no se hayan cometido errores u omisiones en este proceso y controlar así un acceso no autorizado, recomendamos revisar periódicamente los permisos que debería tener cada usuario. Esto requiere una comunicación fluida entre el área de talento humano y el área de tecnología . Idealmente este proceso se debería incluir en protocolos internos de entrada y de salida de la organización.

Matriz de control de permisos y accesos

Una manera de facilitar la revisión es crear una matriz de control de permisos y accesos, como la siguiente:

		WordPress				
		Suscriptor	Colaborador	Autor	Editor	Administrador
Personal	Lector	x	x	x	-	-
	Comunicador	x	x	x	x	-
	Gestión del sitio web	x	x	x	x	x

Para crear una matriz de permisos y accesos:

1. Enumera los diferentes usuarios o roles de tu organización en las filas.

2. Agrega los permisos y accesos al sitio web en las columnas.

3. Completa la matriz asignando a cada usuario o rol únicamente los permisos necesarios según su función.

Nota: Puedes listar por rol en lugar de por usuario, esto facilita asignar permisos y accesos por necesidad y adherirse al **principio de mínimos privilegios**. Además, también simplifica la tabla, lo cual es útil si tienes una cantidad considerable de usuarios.

Por último, revisa qué permisos tiene cada usuario en la práctica, discute los cambios con otros miembros de la organización y realiza los cambios necesarios al modelo de permisos y accesos.

Podrás encontrar más detalles sobre la creación de una matriz de control en este sitio: **https://blog.hackmetrix.com/matriz-de-accesos/**

¡Listo! Ahora puedes realizar la revisión de manera más sencilla:

1. Revisa que la matriz de control de permisos y accesos esté actualizada.

2. Verifica que dicha matriz se refleje correctamente en los accesos reales al sitio web.

   Nota: En la matriz de permisos y accesos puedes incluir todas las otras herramientas que use tu organización. Por ejemplo, los grupos de mensajería instantánea, bases de datos o el panel de control de dominio.

Autenticación en el panel de control y el WordPress

Es importante tener una buena gestión de los permisos de acceso, así como un método de autenticación robusto, tanto para el acceso al panel de control del dominio como para la interfaz de administración de WordPress. Por eso, recomendamos.

Tener contraseñas seguras, cambiadas periódicamente, en particular cuando se identifica un riesgo.

Activar la autenticación en dos pasos (2FA).

Puedes encontrar más detalles sobre la autenticación en dos pasos en WordPress aquí https://es.WordPress.org/2024/12/05/como-configurar-la-autenticacion-en-dos-pasos-2fa-en-WordPress/

Autonomía organizacional

En caso de que la administración de tu sitio web esté a cargo de un tercero, es fundamental que tu organización conserve una copia de los accesos de administrador. Esto garantiza autonomía sobre el sitio y evita una dependencia total del contratista, reduciendo el riesgo de perder el acceso si la relación laboral termina de forma inesperada o conflictiva.

> **Nota:** Para adherirse al principio de mínimo privilegios, tu organización puede crear una cuenta de usuario con permisos administrativos únicamente con esta función, la cual será usada solo en caso de ser necesario. Este acceso debería ser revisado periódicamente para asegurarse de su funcionamiento.

Desvinculación / Offboarding

Desvincular correctamente a una persona que ha salido de una organización es fundamental para proteger la seguridad e integridad de la infraestructura digital del sitio web. Esto implica revocar su acceso a cuentas, sistemas y documentos sensibles, asegurando que la información de la organización permanezca confidencial y no esté expuesta a accesos no autorizados.

En el caso de las OSC, donde el trabajo suele centrarse en causas sociales y el manejo de información delicada, es especialmente importante controlar quién tiene acceso a los recursos. Por ejemplo, un sitio web que incluya formularios de contacto puede recibir información sensible.

Para garantizar un proceso completo en cada ocasión, puedes establecer un protocolo de desvinculación que contemple la revocación de todos los permisos y accesos que esa persona ya no debería tener. Para ello, puede ser útil la matriz de control de permisos y accesos.

En caso de alguna omisión accidental, es posible detectar el error durante una revisión periódica de permisos y accesos, si tu organización cuenta con este tipo de controles.

Otras recomendaciones importantes

Activa un CDN

Para protegerte frente a análisis de puertos a tu sitio web y de ataques de denegación de servicio DDOS, idealmente deberías activar un CDN en todas las conexiones al servidor del sitio web. Existen CDN gratuitos para organizaciones de sociedad civil, como Deflect de eQualitie https://deflect.ca/es/ y el Proyecto Galileo de Cloudflare https://www.cloudflare.com/es-la/galileo/.

Revisa la correcta implementación del certificado SSL

Puedes hacerlo con la herramienta SSL LAB de Qualys https://www.ssllabs.com/ssltest/. Recuerda marcar la opción *Do not show the results on the boards* para que los resultados de tu sitio web no sean publicados e ingresar la dirección de tu sitio web en la casilla principal.

Los resultados A+, A o B indican una seguridad adecuada para la mayoría de OSC.[3]3

Maneja correctamente la información sensible

En particular, asegúrate de diferenciar cuidadosamente los documentos públicos y privados de tu sitio web, así como la información recolectada a través de los formularios del sitio. Es importante controlar el acceso a los documentos privados siguiendo estos pasos: https://WordPress.com/es/support/visibilidad-de-paginas-y-entradas/

3 https://www.sic.gov.co/boletin-juridico-octubre-2017/transferencia-Internacional-de-datos-personales

Elige bien el servicio / la empresa de "hosting"

Escoge cuidadosamente el servicio de *hosting* para tu sitio web, ya que cambiar de proveedor requiere tiempo y esfuerzo. Para esto, revisa sus condiciones de uso, en especial la política de copias de respaldo. Debes revisar cada cuánto son realizadas, cuánto se demoran y en qué formato son entregadas.

Además, es importante considerar la legislación aplicable respecto a la protección de datos y la privacidad, ya que tu sitio web debe cumplir con las normativas nacionales e internacionales. Esto es fundamental si tu sitio recolecta datos personales a través de formularios. En Colombia, cuando el servicio de *hosting* se ubica en "*países que no proporcionen niveles adecuados de protección de datos*" (establecida por la SIC), la transferencia de datos personales puede estar prohibida si no entra en las excepciones de la ley de protección de datos[4].

En algunos casos, el *hosting* y el servicio de registro del dominio pueden ser ofrecidos por la misma empresa (el *Registrar*), lo que facilita la gestión inicial. Sin embargo, exige una revisión de las condiciones de uso.

¿Y la privacidad en mi sitio web?

Aunque no entra en el marco de esta guía enfocada en la seguridad digital, el respeto de la privacidad de las personas usuarias de sus sitios web y de las leyes y normas de protección de datos personales es muy importante.

Debes tener una política de privacidad, cuidar los formularios que recogen datos personales y tener en cuenta el impacto de la inclusión de servicios de terceros que puedan incluir tecnologías de rastreo cómo cookies en su sitio web (analítica de datos, publicidad, botones redes sociales, etc.).

Para estos caso, pueden consultar las recomendaciones al final de nuestro informe *Datos y AdTech: ¿a dónde van los ductos del petróleo digital?* y una herramienta de análisis de sitios webs enfocada en la privacidad desarrollada por la Agencia Europea de Protección de Datos (EDPB website auditing tool).

4 https://www.sic.gov.co/boletin-juridico-octubre-2017/transferencia-Internacional-de-datos-personales

Recursos recomendados

Herramientas

https://protege.la/guias-contenido/herramientas-de-seguridad-digital/#PROTEGE_TU_SITIO_WEB

https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/edpb-website-auditing-tool_es Análiza tu sitio web con el "*EDPB website auditing tool*" de la Agencia Europea de protección de datos. Está más enfocado hacia la privacidad pero incluye funcionalidades de seguridad digital.

Kits

https://chequea.la Revisa tu sitio web y obtén pasos personalizados para mejorar la seguridad digital del sitio web. Analiza tu sitio web por medio de fuentes abiertas.

https://securityinabox.org/es/ Conoce herramientas y tácticas para todos los días.

https://ssd.eff.org/es/ Asegura tus comunicaciones online.
https://cso.cyberhandbook.org/ Empieza a crear un plan de ciberseguridad.

https://openbriefing.gitbook.io/defenders-protocol/es Protocolo de seguridad holística para defensores de derechos humanos

Cuestionarios

https://digitalfirstaid.org (*Kit de primeros auxilios digitales*) Encuentra una solución para situaciones de emergencias digitales.

https://securityplanner.consumerreports.org/es/ Obtén un plan de seguridad digital personalizado.

Cursos

https://totem-project.org/es/

https://digital-self-defense.org/

Modelos de evaluaciones

https://safetag.org/ Para grupos activistas.

https://web.karisma.org.co/nueva-guia-para-auditorias-en-seguridad-digital/ Para auditores de seguridad digital latinoamericanos.

Conclusiones

Este documento ha presentado una metodología práctica, adaptada a las necesidades de las OSC en América Latina para fortalecer la seguridad digital de sus sitios web, con énfasis en plataformas basadas en WordPress. La adaptación e implementación de estas prácticas no solo mejora la protección frente a incidentes de seguridad digital, sino que también fomenta una cultura de seguridad digital sostenible.

Aunque los desafíos técnicos pueden parecer abrumadores, los pasos propuestos son alcanzables y escalables. Cada avance, por pequeño que sea, contribuye significativamente a reducir el riesgo y la gravedad de un incidente digital y a proteger las causas que las organizaciones representan.

Estos esfuerzos deben mantenerse a lo largo del tiempo. La seguridad digital es un proceso continuo y, si se cuenta con los recursos y la disposición, es posible alcanzar un nivel de seguridad suficiente para tu propio contexto. Invitamos a las OSC a dar el primer paso adoptando estas buenas prácticas, sentando las bases para una infraestructura digital más robusta y resiliente.

<K+LAB> Fundación Karisma

GUÍA DE SEGURIDAD DIGITAL

<para un sitio Wordpress>

Versión para organizaciones de la sociedad civil

karisma.org.co