La ciberseguridad de los principales E-Commerce de Ecuador no ha mejorado desde el 2020

Según el eccomerceday el comercio electrónico creció y se consolido como un medio de la pandemia, en Ecuador específicamente la categoría de supermercado, que ocupaba el lugar 15 dentro de las 24 categorías monitoreadas, creció un 67% seguida por medicamentos que creció un 50% y restaurantes un 42%. Esto tiene que ver con categorías de primer orden, en este mismo sentido cifras preliminares señalan que la facturación del sector de comercio electrónico paso de USD 1.900 millones en 2019, a unos USD 2.300 millones en 2020. (CyberDay, 2021)

Por ello, desde el año anterior como empresa enfocada en la seguridad de información, decidimos hacer un analisis con propósitos académicos de cuál es la postura de seguridad de información de los principales E-Commerce del país, un año mas tarde hemos decidido repetir este estudio para evaluar el progreso de las buenas practicas de seguridad en estos portales.

El analisis que realizamos es con fines académicos, corresponde a la fase inicial que cualquier cibercriminal haría de alguno de estos sitios, conocida como fase de reconocimiento en la que se evalúa los siguientes parámetros: HTTPS, Only HTTPS, servidor web dedicado, software al día, sitios de administración seguros, protección del sitio web.

Para el año anterior, se pudo verificar que de un 100 % solo el 23% tenía un E-Commerce considerado como seguro, mientras que el 87% podría ser víctima de algún ciberataque mientras que, para este año, de un total de 31 sitios involucrados, todos cuentan con al menos una mala configuración de seguridad, la misma que puede generar una brecha de seguridad bastante importante.

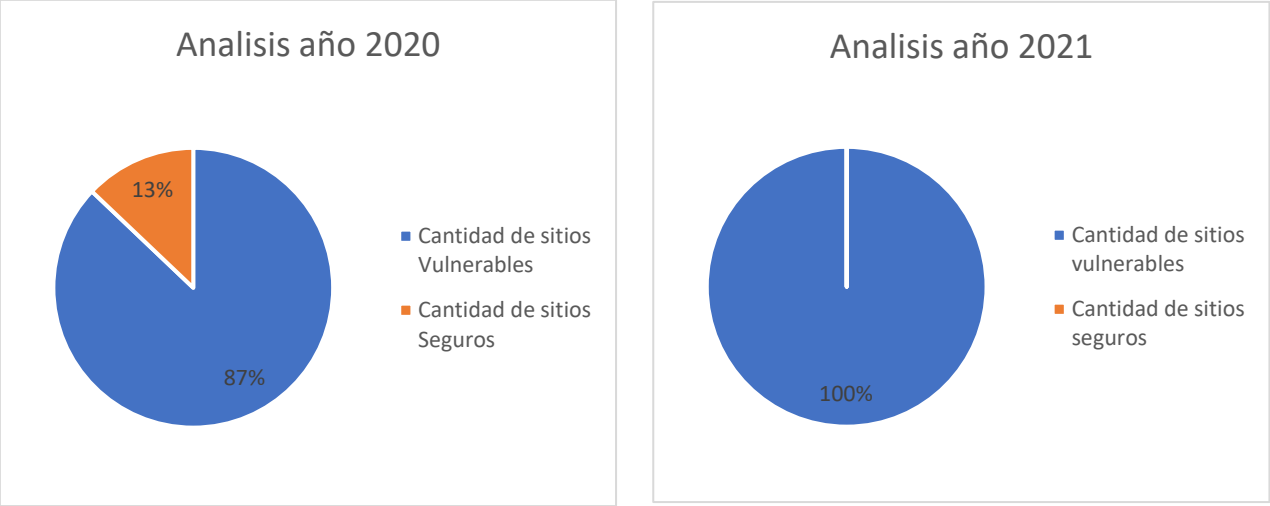


Ilustración 1: Porcentaje E-commerce que tienen configuraciones inseguras año 2020 y 2021.

Para generar el análisis se tomó como referencia la importancia de la seguridad de aplicaciones según (OWSAP, 2021), el primer aspecto son las buenas prácticas de infraestructura en donde se analizó lo siguiente:

Elaborado por: Stalin Tipán | Departamento Preventa Vialynk
Colaboradores: David Ruiz y Ricardo Romo | Departamento Preventa Vialynk
Revisado y Aprobado por: Guillermo García Granda

- **Verificación de que el sitio web tenga una cabecera de hipertexto segura (HTTPS):** Esto debido a que permite ver al usuario que la página puede tener un certificado de seguridad al abrir el enlace permitiéndole estar un poco más seguro, pero no totalmente.
- **Redireccionamiento de http a https:** Es importante tomar en cuenta este punto ya que si un sitio de internet utiliza http puede darnos muchas brechas de seguridad determinando una validación inadecuada permitiendo modificar fácilmente un sitio como lo es con "Burp Proxy" que permite interceptar peticiones y ver el tráfico, mientras que https brinda confiabilidad y seguridad a cada usuario que ha ingresado a los distintos portales de una página web, sin filtración de datos.
- **Reconocimiento de servidor web dedicado:** Varios de los sitios analizados mantienen sus servicios web compartidos con otros como FTP, SSH, DNS, etc. Lo único que se consigue con esto es la posibilidad de una mala administración en la seguridad a nivel de red.
- **Software al día:** Hay que tener claro que otra deficiencia en la seguridad es el uso de versiones de software desactualizadas, esto se midió con ayuda de una herramienta gratuita proporcionada por (Sucuri, 2021) denominada "Free website security check & malware scanner".

El segundo aspecto para tomar en cuenta fueron las buenas prácticas en seguridad, en este punto se realizó el análisis por medio de pruebas en el propio dominio de los sitios:

- **Validación de seguridad en gestores de administración:** Con el ingreso de palabras claves como **admin, wp-admin, wpadmin, cpanel, dashboard**, etc. Permiten verificar si existe una seguridad a nivel de la capa de aplicación al momento de querer tener acceso ya sea a un gestor de la página o gestor de base de datos alojada allí.
- **Verificación del uso de WAF por parte de la aplicación web:** Con ayuda de la aplicación mencionada anteriormente que brinda Sucuri, fue posible determinar que dominios cuentan con un WAF y cuáles no.

Para poder cuantificar los resultados se establecieron métricas con el fin de verificar el cumplimiento de cada uno de los puntos mencionados anteriormente de la siguiente manera:

Buenas prácticas de la infraestructura				Buenas prácticas de seguridad		Total
Cabecera HTTPS	**Redireccionamiento HTTP → HTTPS**	**Servidor Web dedicado**	**Software al día**	**Sitios de administración seguros**	**Protección del sitio web (uso de WAF)**	
1 punto	1 punto	1 punto	1 punto	1 punto	2 puntos	7 puntos

Ilustración 2: Métricas de evaluación

Respecto a las métricas de evaluación es importante también verificar en que parámetros se han generados falencias ya sea de configuración o seguridad dentro de los portales con el fin de que se pueda verificar la relevancia y la falta de compromiso hacia las buenas practicas que se deberían aplicar dentro de cada uno de los sitios web.

Elaborado por: Stalin Tipán | Departamento Preventa Vialynk
Colaboradores: David Ruiz y Ricardo Romo | Departamento Preventa Vialynk
Revisado y Aprobado por: Guillermo García Granda

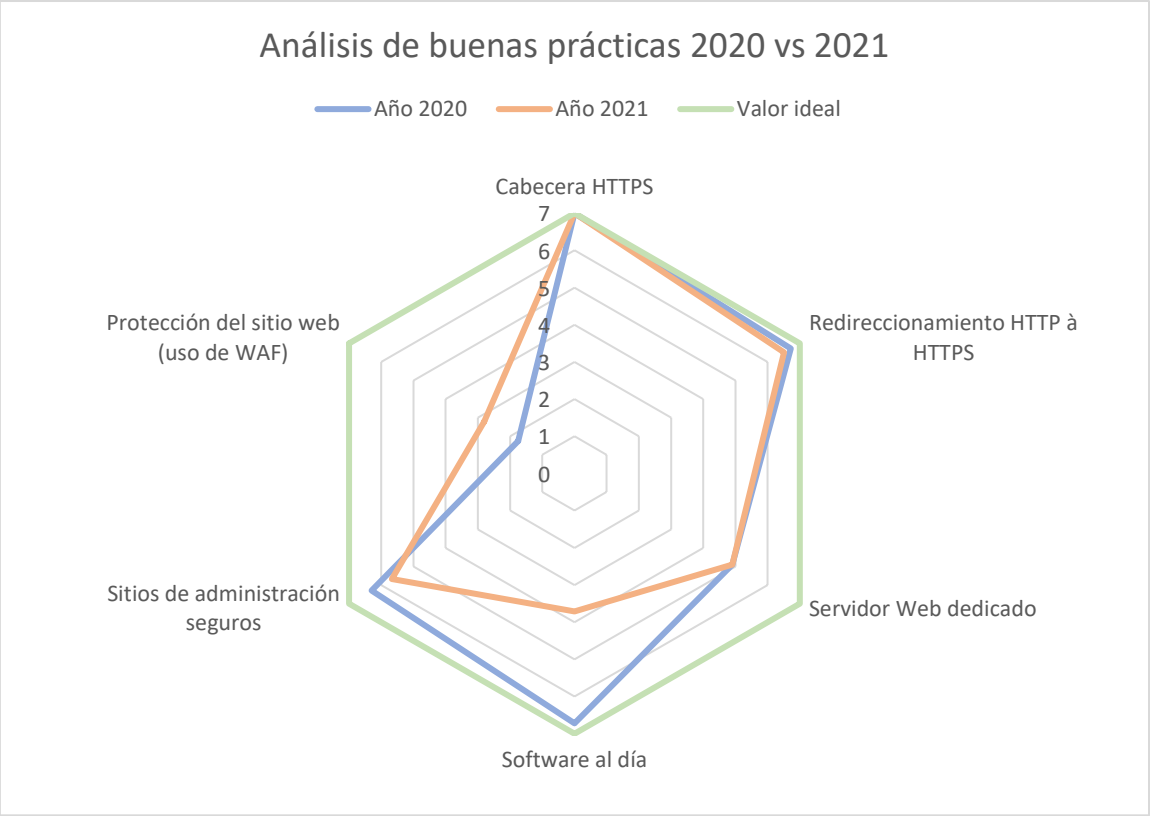


Ilustración 3: Visión del análisis de seguridad en buenas prácticas

También es importante mencionar que existen sitios que se encuentran peor que otros, por ende, es relevante verificar hacía que sectores están dirigidos los mismos, en este caso esto se puede apreciar de mejor manera mediante la siguiente gráfica:

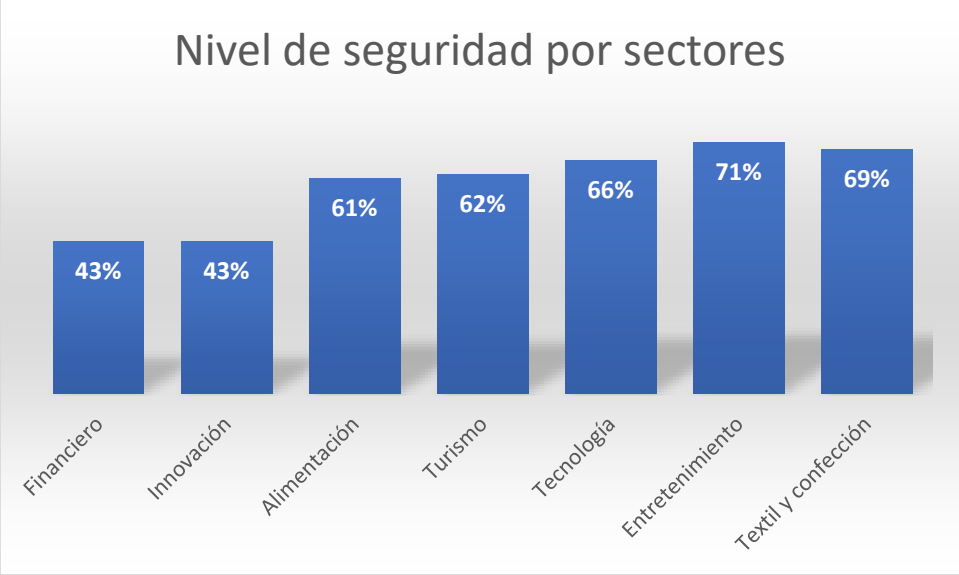


Ilustración 4: Verificación nivel de seguridad por sector empresarial

Elaborado por: Stalin Tipán | Departamento Preventa Vialynk
Colaboradores: David Ruiz y Ricardo Romo | Departamento Preventa Vialynk
Revisado y Aprobado por: Guillermo García Granda

Existe una gran cantidad entre los sitios web analizados que tienen falta de configuración, sean por infraestructura o netamente de seguridad, esto puede implicar que el riesgo y las vulnerabilidades a las que se exponen son mucho más grandes, ya que a medida que la tecnología avanza los ciberataques también lo hacen y de una manera exponencial que hoy es muy preocupante según el EITB de Estados Unidos.

Ahora bien, una de las buenas prácticas que se ha logrado determinar en cada sitio web analizado, es que cuenta con una cabecera segura y un redireccionamiento adecuado en casi todos los sitios. Por el contrario, se puede evidenciar que los factores más bajos según la evaluación es el no contar con un servidor web dedicado y no utilizar una protección en el sitio web como es la implementación de un WAF.

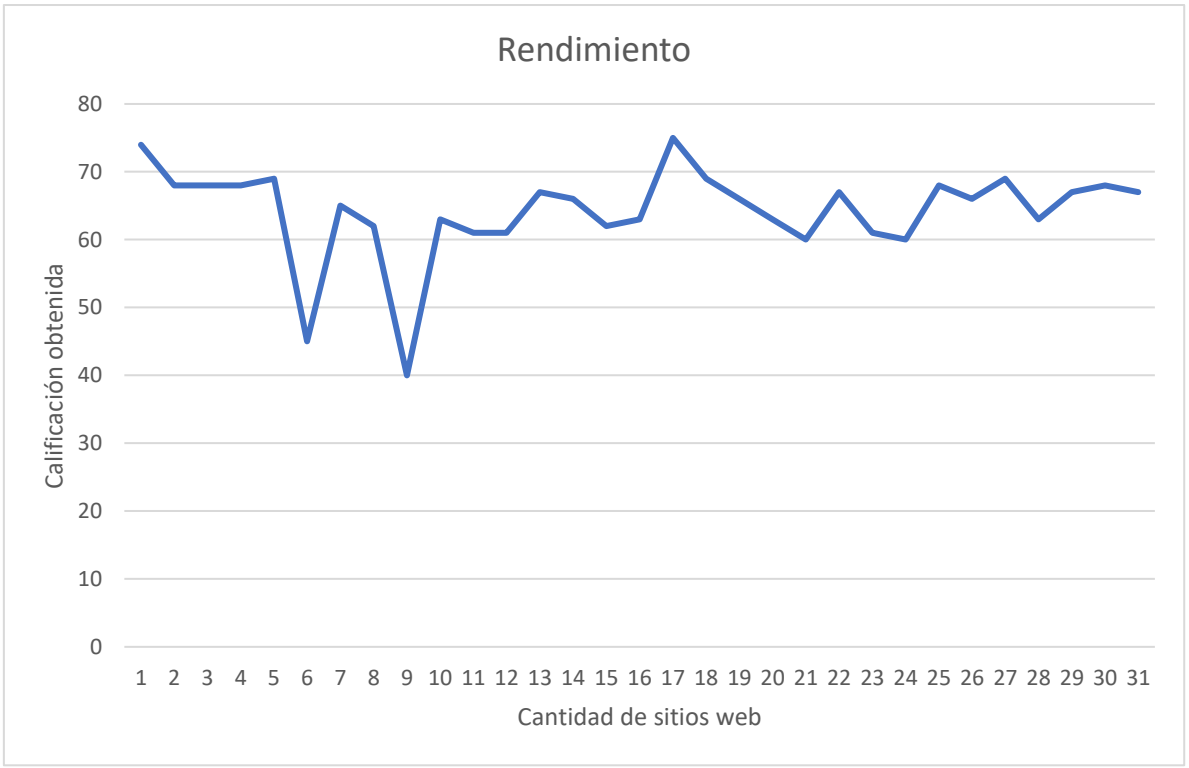
En este mismo contexto, dentro de cada uno de los portales web existen parámetros a nivel de funcionamiento, que también son importantes de verificar, en este sentido se encuentra el grado de desempeño y el tiempo de carga que pueden llegar a tener los mismos, esto se ha logrado verificar mediante el uso de herramientas como “Pingdom” que brindan la posibilidad de generar una prueba de velocidad del sitio web con el fin de probar el tiempo de carga y en el debido caso visualizar cuellos de botella.

Es así como se logró obtener **un promedio de velocidad de carga entre 0 a 3,5 segundos** que con relación a lo que se espera de un sitio web, absolutamente todos los que se han analizado se preocupan mucho por este tipo de parámetros.

Ilustración 5: Velocidad de carga de los sitios involucrados

Mientras que para el desempeño que tiene cada uno de los sitios web con respecto a la interacción del sitio es algo que a nivel general no se encuentra del todo bien. Cabe recalcar que este punto se ha logrado obtener al igual que el anterior con el uso de herramientas totalmente gratuitas que brindan la posibilidad de verificar este tipo de funcionalidades, para esta verificación la herramienta brinda un promedio sobre 100 respecto al desempeño de cada sitio, en donde se ha podido determinar lo siguiente:

Elaborado por: Stalin Tipán | Departamento Preventa Vialynk
Colaboradores: David Ruiz y Ricardo Romo | Departamento Preventa Vialynk
Revisado y Aprobado por: Guillermo García Granda



Como se puede apreciar, a nivel de rendimiento o desempeño de entre los 31 portales web analizados se encuentran en un promedio de 68 sobre 100 respecto al buen rendimiento que pueden brindar hacia el usuario final, es decir que existe un 22% en el día que un sitio web se pueda ver indispuesto y cause molestias respecto a lentitud.

A veces cuesta explicar lo necesarios que son los servicios de seguridad tanto en aplicaciones como infraestructura de red en una empresa. Y más aun, en la seguridad web ya que esta debería ser considerada como una prioridad que tanto usuarios como empresas no se percatan que; si existe una o varias vulnerabilidades automáticamente un número elevado de personas estará pensando como violar las mismas para hacer algún daño indistintamente de que beneficios pueden obtener, es por ello que gracias a este análisis se evidencia la falta de compromiso de las empresas con sus E-Commerce, logrando así que exista una brecha muy grande respecto a la información que tienen de sus clientes o el riesgo de que se infecten por malware o algún otro ataque que implique también la disponibilidad, confiabilidad e integridad del giro de negocio.

Finalmente hemos considerado importante aportar con unas cuantas evidencias sobre las malas practicas encontrada indistintamente de los portales analizados, dentro de estas la mas importante es que se tiene de manera publica el gestor de administración de los sitios web, el cual unicamente deberían acceder usuarios permitidos, identificados ya sea por la IP de conexión hacia internet o cualquier otra medida de seguridad.

Elaborado por: Stalin Tipán | Departamento Preventa Vialynk
Colaboradores: David Ruiz y Ricardo Romo | Departamento Preventa Vialynk
Revisado y Aprobado por: Guillermo García Granda

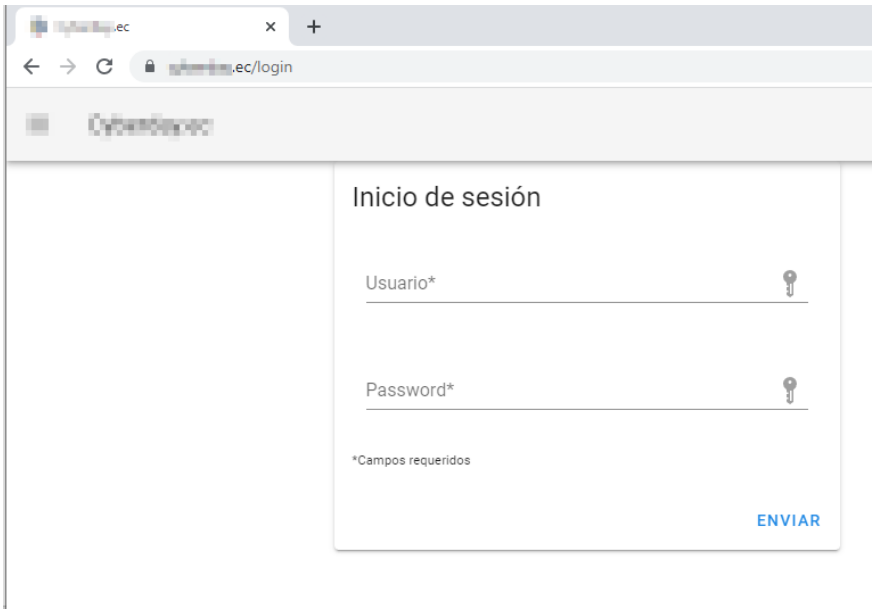


Ilustración 6: Gestor de administración expuesto.

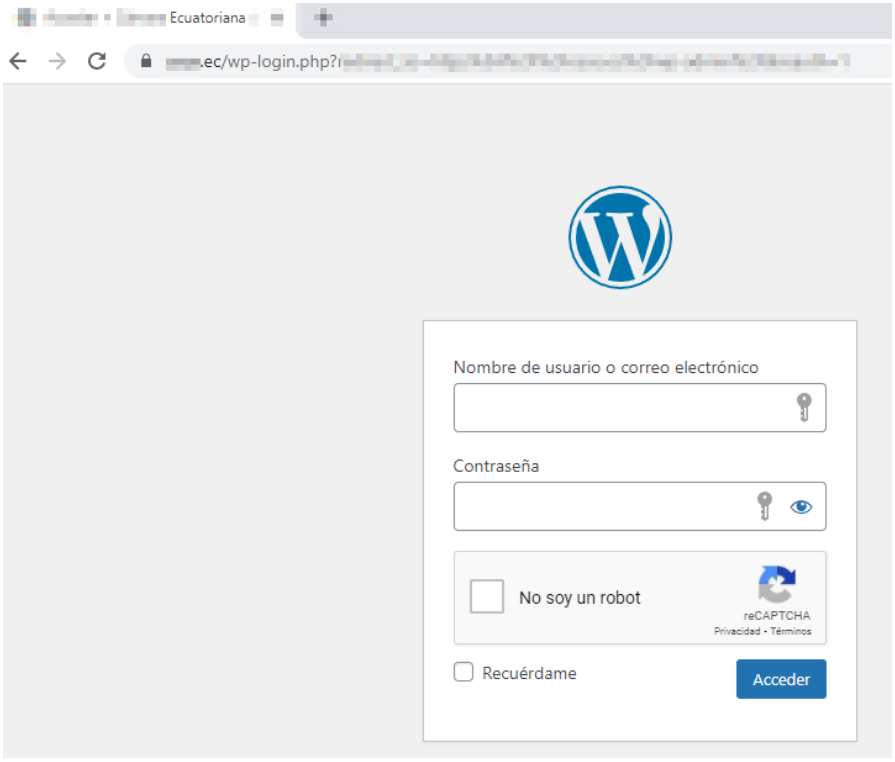


Ilustración 7: Gestor de administración de WordPress expuesto.

Elaborado por: Stalin Tipán | Departamento Preventa Vialynk
Colaboradores: David Ruiz y Ricardo Romo | Departamento Preventa Vialynk
Revisado y Aprobado por: Guillermo García Granda

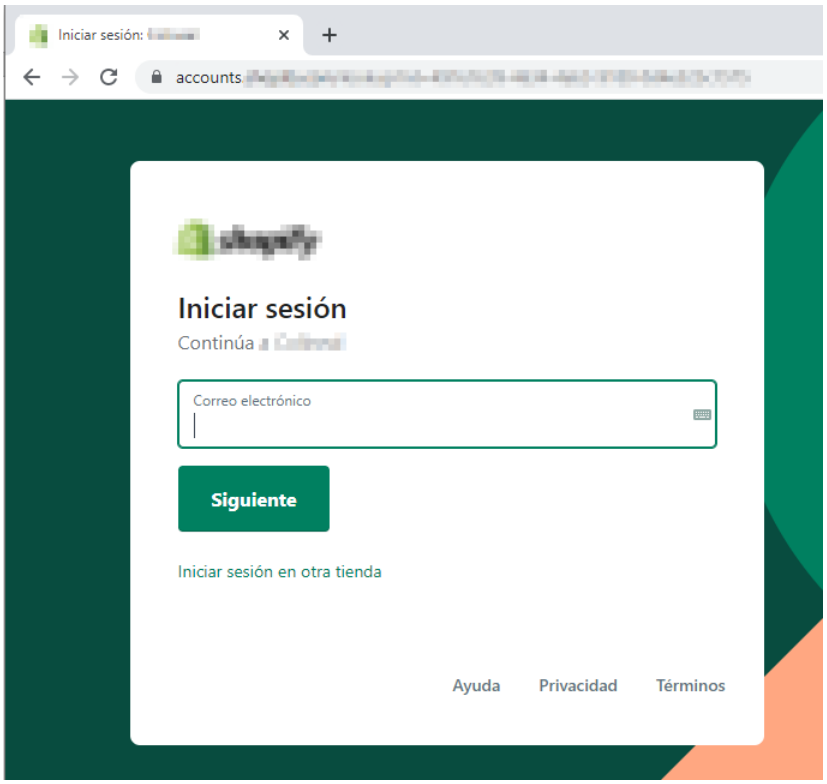


Ilustración 8: Gestor de administración expuesto

Como se puede evidenciar existen varios gestores de administración de manera pública de los sitios analizados, por ello es importante mencionar que si un ciberdelincuente genera un ataque de fuerza bruta o ingeniería social dirigida a las personas a cargo de este tipo de gestores, sería muy habitual tener intromisiones en los portales web y el servicio, producto e inclusive la información de los usuarios que utilizan este canal digital se puede ver comprometido, por ello es importante generar y verificar de manera periódica la adecuación de buenas practicas de seguridad en general y seguridad orientada a las aplicaciones web.

Bibliografía

CyberDay. (23 de 11 de 2021). *CyberDay.ec*. Obtenido de https://cyberday.ec/

OWSAP. (23 de 11 de 2021). *OWASP Top Ten*. Obtenido de https://owasp.org/

Pingdom. (24 de 11 de 2021). *Pingdom Website Speed Test*. Obtenido de https://tools.pingdom.com/

Sucuri. (23 de 11 de 2021). *Free website security check & malware scanner*. Obtenido de https://sitecheck.sucuri.net/

Valle, S. M. (12 de 07 de 2021). *Ecommerceday*. Obtenido de Ecuador vive un gran crecimiento en eCommerce: https://ecommerceday.org/2021/07/06/ecuador-vive-un-gran-crecimiento-en-ecommerce/

Elaborado por: Stalin Tipán | Departamento Preventa Vialynk
Colaboradores: David Ruiz y Ricardo Romo | Departamento Preventa Vialynk
Revisado y Aprobado por: Guillermo García Granda