

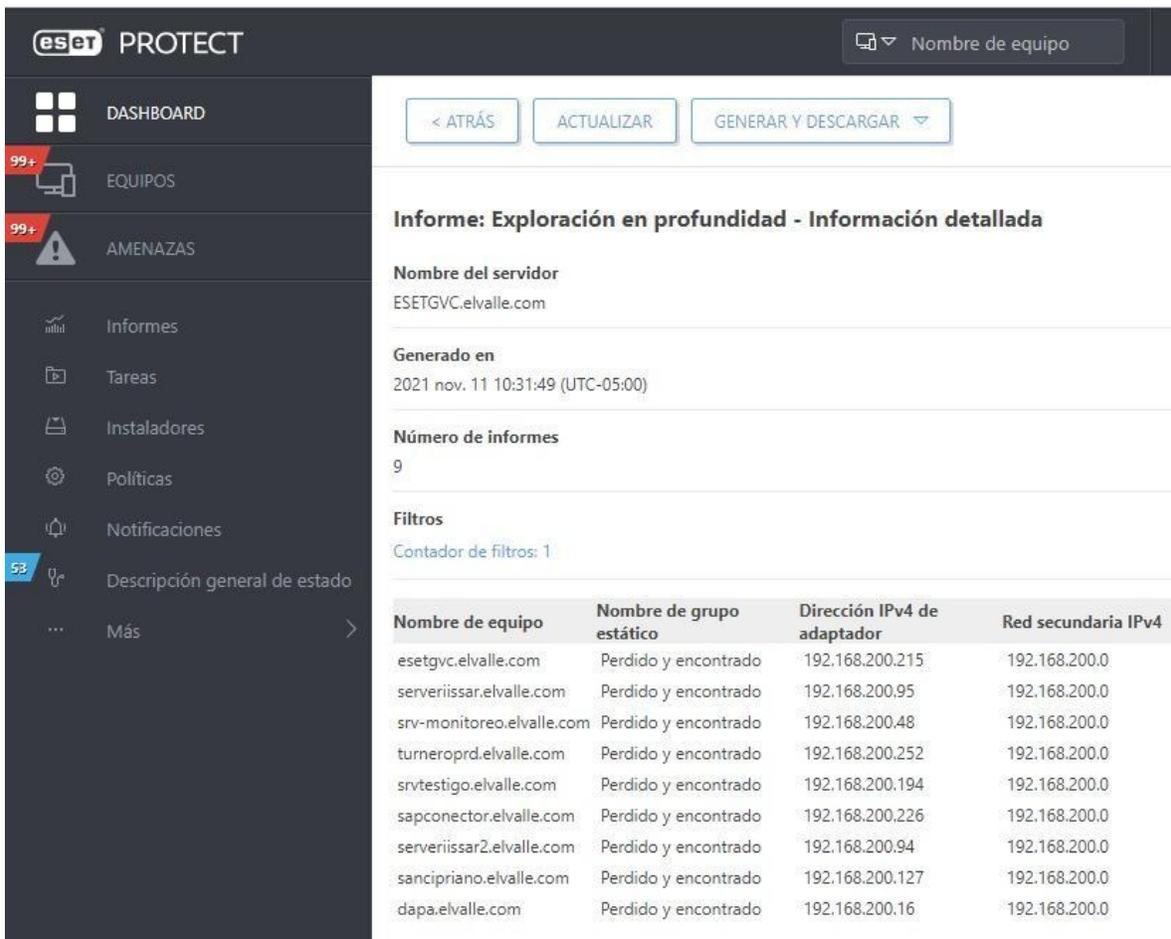
REPORTE DE ANÁLISIS SOBRE CONDICIONES MÍNIMAS DE SEGURIDAD DIGITAL - ANEXO NO.3. RESOLUCIÓN 1519 DE 2020

De acuerdo al análisis realizado a los ítems relacionados en el anexo 3 de la resolución 1519 de 2020 en materia de la infraestructura tecnológica, nos permitimos dar respuesta a los siguientes puntos:

1. Se implementan sistemas antivirus en el servidor web, para garantizar medidas contra infecciones de malware a los archivos del mismo.

RESPUESTA:

Para los servidores con sistema operativo Windows se tiene el antivirus ESET PROTEC licenciado hasta el año 2022.



eset PROTECT Nombre de equipo

DASHBOARD

99+ EQUIPOS

99+ AMENAZAS

Informes

Tareas

Instaladores

Políticas

Notificaciones

53 Descripción general de estado

Más

< ATRÁS ACTUALIZAR GENERAR Y DESCARGAR

Informe: Exploración en profundidad - Información detallada

Nombre del servidor
ESETGVC.elvalle.com

Generado en
2021 nov. 11 10:31:49 (UTC-05:00)

Número de informes
9

Filtros
Contador de filtros: 1

Nombre de equipo	Nombre de grupo estático	Dirección IPv4 de adaptador	Red secundaria IPv4
esetgvc.elvalle.com	Perdido y encontrado	192.168.200.215	192.168.200.0
serveriissar.elvalle.com	Perdido y encontrado	192.168.200.95	192.168.200.0
srv-monitoreo.elvalle.com	Perdido y encontrado	192.168.200.48	192.168.200.0
tuneroprdr.elvalle.com	Perdido y encontrado	192.168.200.252	192.168.200.0
srvestigo.elvalle.com	Perdido y encontrado	192.168.200.194	192.168.200.0
sapconector.elvalle.com	Perdido y encontrado	192.168.200.226	192.168.200.0
serveriissar2.elvalle.com	Perdido y encontrado	192.168.200.94	192.168.200.0
sancipriano.elvalle.com	Perdido y encontrado	192.168.200.127	192.168.200.0
dapa.elvalle.com	Perdido y encontrado	192.168.200.16	192.168.200.0

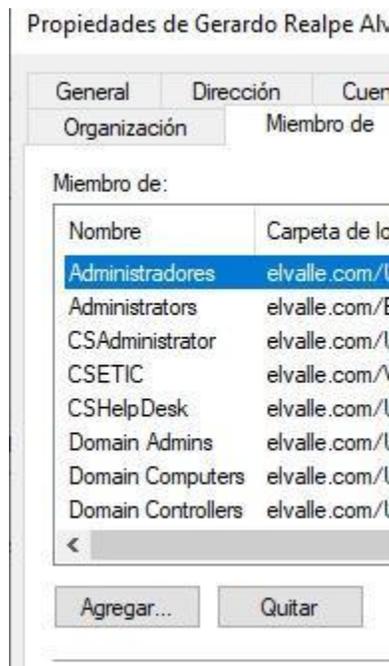
2. Se controla el escalamiento de privilegios en los Sistemas Operativos, servidor web y Bases de datos que hacen parte de la infraestructura del portal web.

RESPUESTA:

Se manejan privilegios de usuarios en servidores Linux brindando accesos de SUPER USER según la necesidad.

```
GNU nano 2.5.3          Fichero: /etc/sudoers
ALL  ALL=(ALL) ALL  # WARNING! Only use this together with 'Defaults targetpw!'
##
## Runas alias specification
##
##
## User privilege specification
##
root          ALL=(ALL)    ALL
grealpe      ALL=(ALL)    NOPASSWD:ALL
hvalenci     ALL=(ALL)    NOPASSWD:ALL
jspetro      ALL=(ALL)    ALL
## Uncomment to allow members of group wheel to execute any command
# %wheel ALL=(ALL) ALL
## Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL
## Read drop-in files from /etc/sudoers.d
## (the '#' here does not indicate a comment)
```

Se manejan permisos de usuarios según estructura de directorio activo en servidores Windows Sever



3. Se exigen medidas de seguridad al proveedor del hosting (políticas de seguridad robustas y un nivel de madurez en seguridad optimizado).

RESPUESTA:

La empresa Open Group es la encargada de realizar el análisis de “SEGURIDAD GOBERNACION DEL VALLE” para el hosting de la entidad:



INTRODUCCION

En el presente informe se sacaron las estadísticas del 1 de octubre al 31 de octubre de 2021.

Para la supervisión continua de las plataformas de seguridad desde nuestro NOC, actualmente se tienen configurados 152 sensores, en la herramienta de monitoreo PRTG, los cuales abarcan todos los servicios contratados con Open Group S.A.

4. Se ejecutan monitoreos de seguridad sobre las páginas web que contemple, entre otras, las siguientes acciones: escaneo de archivos infectados, escaneo de vulnerabilidades, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios.

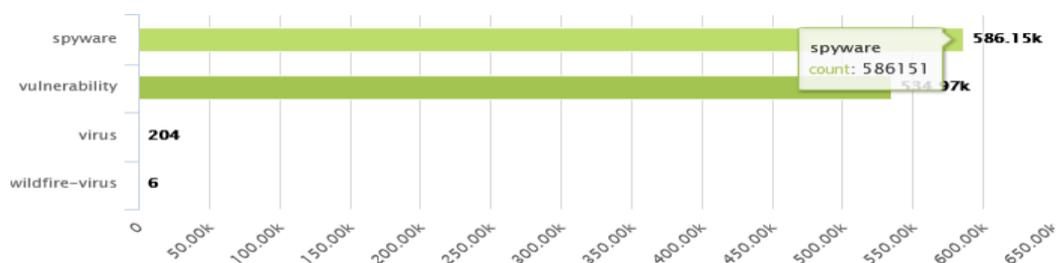
RESPUESTA:

La empresa Open Group realiza monitoreos diarios de seguridad sobre las páginas web



Los principales ataques presentados se registran en las plataformas de páginas web aplicaciones web y sistema operativos.

Actividad de Amenazas – Críticas



5. Se crean copias de respaldo.

Se realizan copias semanales de los servidores On Premise existentes en la Secretaría de TIC, de igual forma los servidores de nube tienen soporte de Backup bajo el contrato existente.

 DEPARTAMENTO DEL VALLE DEL CAUCA GOBERNACIÓN <small>Departamento de Gestión, Planeación y Desarrollo Institucional</small> <small>Secretaría de Tecnologías de Información y Comunicaciones</small>						
Secretaría de las Tecnologías de Información y las Comunicaciones REGISTRO DE BITACORA BACKUPS						
Semana No. 44 Full Backup OnPremise						
DETALLE DE REGISTROS						
Ubicación	SERVIDOR	HORA INICIO	FECHA INICIO	HORA FINAL	FECHA FINAL	VALIDACION
NASSAP1	SARPRD	9:45:00 AM	11/1/2021	11:45:00 AM	11/2/2021	CORRECTO
	VUR	10:45:00 AM	11/1/2021	12:45:00 PM	11/2/2021	CORRECTO
AVAMAR BK	AGRICULTURA_	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	GRANADA	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	KALI_	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	KRISHNA_	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	MOODLE_2020	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	OBSERVATORIO_APP	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	OBSERVATORIO_BD	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	ORACLE11_	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	PANCE2	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	SERVERBDSAR_2	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	SRV-PACIFICIC-APP	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	SRV-PACIFICIC-ELK	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	VISION-4.7 WAF-	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	ALTHEON-HA	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	WAF-ALTHEON-PPAL	4:00 PM	10/31/2021	4:00 PM	10/31/2021	CORRECTO
	ESETGVC	10:00 AM	10/31/2021	10:00 AM	10/31/2021	CORRECTO
	SANCIPRIANO_	10:00 AM	10/31/2021	10:00 AM	10/31/2021	CORRECTO
	SAR-RECAUDOGDV	10:00 AM	10/31/2021	10:00 AM	10/31/2021	CORRECTO
	SERVERISSARGDV	10:00 AM	10/31/2021	10:00 AM	10/31/2021	CORRECTO
	SRV-ARCGIS-APP	10:00 AM	10/31/2021	10:00 AM	10/31/2021	CORRECTO
SRV-ARCGIS-BD	10:00 AM	10/31/2021	10:00 AM	10/31/2021	CORRECTO	
SRV-IMPRESORAS	10:00 AM	10/31/2021	10:00 AM	10/31/2021	CORRECTO	
SRV-WSUS	10:00 AM	10/31/2021	10:00 AM	10/31/2021	CORRECTO	
TURNEROPRD	10:00 AM	10/31/2021	10:00 AM	10/31/2021	CORRECTO	

Rodolfo Tejada Naverros Gerardo Realpe
 Supervisor Técnico Encargado

6. Se implementan monitoreos de seguridad sobre la plataforma tecnológica que hace parte del sitio web (escaneo de vulnerabilidades, escaneo de archivos infectados, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios) y realizar las acciones de mitigación correspondientes.

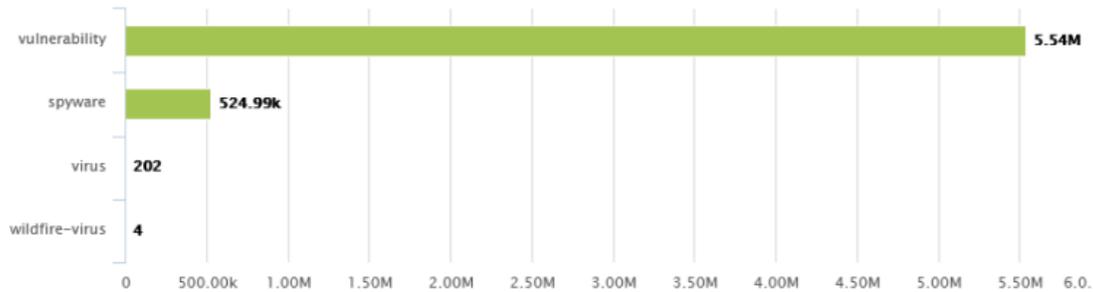
RESPUESTA:

La empresa Open Group realiza monitoreos diarios de seguridad sobre la plataforma



PALO ALTO – NGFW

La plataforma de NGFW presento los siguientes eventos de seguridad, los cuales fueron registrados y bloqueados.



Microsoft Windows user enumeration	30842	inform	vulnerability	info-leak	4.8M
genericochentaremc.duckdns.org	4035...	medium	spyware	dns-wildfre	514.7k
SIPViduous Scanner Detection	54482	medium	vulnerability	info-leak	40.18k
Non-RFC Compliant DNS Traffic on Port 53/5353	56505	inform	vulnerability	protocol-anomaly	226.3k
Windows Local Security Architect lsardelete access	30857	low	vulnerability	info-leak	149.6k
Service Enum Through SMB ServiceEnum2 <	30867	inform	vulnerability	info-leak	142.2k
Non-RFC Compliant SSL Traffic on Port 443	56112	inform	vulnerability	protocol-anomaly	91.0k
Non-RFC Compliant DNS Traffic on Port 53/5353	56502	inform	vulnerability	protocol-anomaly	88.2k
Apache Tomcat WebSocket Denial-of-Service Vulnerability	59026	high	vulnerability	dos	84.5k
CoinMiner Command and Control Traffic Detection	86358	critical	spyware	cryptominer	55.7k
Non-RFC Compliant DNS Traffic on Port 53/5353	56499	inform	vulnerability	protocol-anomaly	44.9k
IP Address Disclosure Detection	56610	inform	vulnerability	info-leak	18.3k
RPC Portmapper DUMP Request Detected	32796	medium	vulnerability	info-leak	15.7k
OpenSSL SSLv2 Man-in-the-Middle Vulnerability	59268	inform	vulnerability	code-execution	14.6k
SIP INVITE Method Request Flood Attempt	40016	high	vulnerability	brute-force	11.8k
Microsoft Windows Registry Read Attempt	34940	low	vulnerability	info-leak	8.7k
DNS RRSIG Query Type Packet	34405	low	vulnerability	dos	7.6k
genericomnatuor.com	4218...	medium	spyware	dns	6.9k
Non-RFC Compliant NTP Traffic on Port 123	56472	inform	vulnerability	protocol-anomaly	6.5k
Non-RFC Compliant DNS Traffic on Port 53/5353	56537	inform	vulnerability	protocol-anomaly	5.9k
Metasploit VxWorks WDB Agent Scanner Detection	56693	medium	vulnerability	info-leak	4.9k
SIP Malformed Request: Unknown URI Schemes in Header Fields	39006	inform	vulnerability	dos	4.1k
DCS-2530L Unauthenticated Information Disclosure Vulnerability	90255	high	vulnerability	info-leak	4.0k
Non-RFC Compliant TFTP Traffic on Port 69	56461	inform	vulnerability	protocol-anomaly	3.6k
SSL Weak Cipher Suite Selection Vulnerability	59220	inform	vulnerability	info-leak	3.5k
Suspicious Telerik Web UI Request	59014	low	vulnerability	code-execution	3.3k
OpenSSL Handshake Cipher Two More Times Changed Anomaly	31120	low	vulnerability	dos	3.2k
Microsoft Windows Server Service NetShareEnum access	30862	inform	vulnerability	info-leak	2.8k
ZGrab Application Layer Scanner Detection	57955	medium	vulnerability	info-leak	2.7k
Microsoft Windows Server Service NetServerGetInfo Opnum 21 Access Attempt	30861	inform	vulnerability	info-leak	2.6k
Non-RFC Compliant NTP Traffic on Port 123	56472	inform	vulnerability	protocol-anomaly	6.5k

Santiago de cali, 07 de Julio del 2021

Señores.

Gobernación del valle

Asunto: Respuestas de seguridad ticket 0120783

Cordial saludo,

De acuerdo al anexo 3 de la resolución 1519 de 2020, relacionado con la seguridad digital web, requerimos por favor sean revisados los siguientes ítems, tanto para el portal web, como para la sede electrónica, especificando las acciones o actividades actualmente realizadas y estipulando si se cumple o no, con las condiciones de seguridad. Agradecemos una respuesta detallada para cada uno de los puntos.

1. Se Implementan o implementaron controles de seguridad durante todo el ciclo de vida del desarrollo de software.

R/ Se implementan controles de seguridad de acuerdo al manual de buenas prácticas de seguridad de la información para la Plataforma web Nexura Cloud.

Anexo No. 1

2. Se aplican mecanismos de hardening para eliminar configuraciones y credenciales por defecto, además de deshabilitar métodos HTTP peligrosos como put, delete, trace y restringir en lo posible la administración remota.

R/ Sí hay mecanismos de hardening para eliminar configuraciones por default, y restringir en lo posible la administración remota.

- **Cortafuegos / Proxies**
- **Software de Proxy**
- **Cortafuegos**
- **Seguridad del Kernel**
- **El Kernel de Linux**
- **Parches de seguridad del Kernel y del Compilador**
- **Registro de logs y monitorización**
- **Herramientas de monitorización de Hosts**
- **Ficheros de log y otros métodos de monitorización**
- **Limitación y monitorización de usuarios**

- Bloqueo de intentos de brute force

EL proveedor encripta todos los sistemas de ficheros y todo el almacenamiento está encriptado.

3. Se protege la integridad del código, mediante: (i) la validación exhaustiva de: inputs, variables post y get (no enviar parámetros sensibles a través del método get), Cookies (habilitar atributos de seguridad como Secure y HttpOnly), y, cabeceras HTTP; (ii) la sanitización de los parámetros de entrada: es decir, que cuando se reciba la información de dichas variables se eliminen etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un script, además de la restricción de formatos y tamaños de subidas de archivos; (iii) la sanitización y escape de variables en el código; (iv) verificación estándar de las Políticas de Origen de las cabeceras; y (v) la verificación y comprobación del token de CSRF (cuando aplique).

R/ El código cumple con validaciones cliente y servidor tanto para peticiones de métodos post como para métodos get además de contar con token CSRF en las peticiones, también se cumple con la sanitización de parámetros.

4. Se exigen mecanismos de autenticación dentro de los sitios web a través de la creación de contraseñas fuertes y solicitar renovaciones periódicas de las mismas garantizando la accesibilidad de personas con discapacidad.

R/ No se tienen mecanismos de autenticación para los portales, los usuarios son creados pero no pide validación por correo electrónico o por mensaje de texto y tampoco se manejan las renovaciones periódicas de las contraseñas, pero el sistema si tiene validaciones para crear contraseñas fuertes.



The image shows a user interface for creating a password. It consists of three main elements: a 'Password' input field with a masked password '*****', a 'Fuerza' (Strength) indicator showing a progress bar at 21%, and a 'Confirmación *' (Confirmation) input field with a masked password '*****'.

5. Se mantiene actualizado el software, frameworks y plugins de los sitios web.

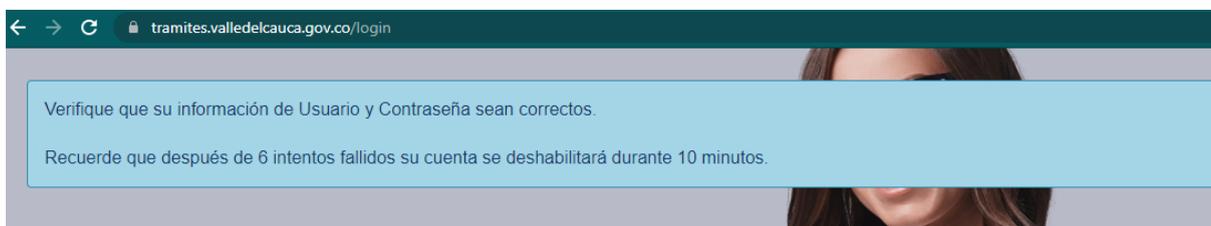
R/ El software constantemente recibe actualizaciones propias como de plugins y framework, siempre y cuando las actualizaciones externas no generen incidentes por lo cual son validadas previamente por un equipo técnico.

6. Se restringe el uso de login contra ataques de fuerza bruta, implementando, entre otros: mecanismos de captcha accesibles o auto detectable, y/o limitar la tasa de intentos de login.

R/ Para restringir los ataques de fuerza bruta se tiene implementados lo siguiente:

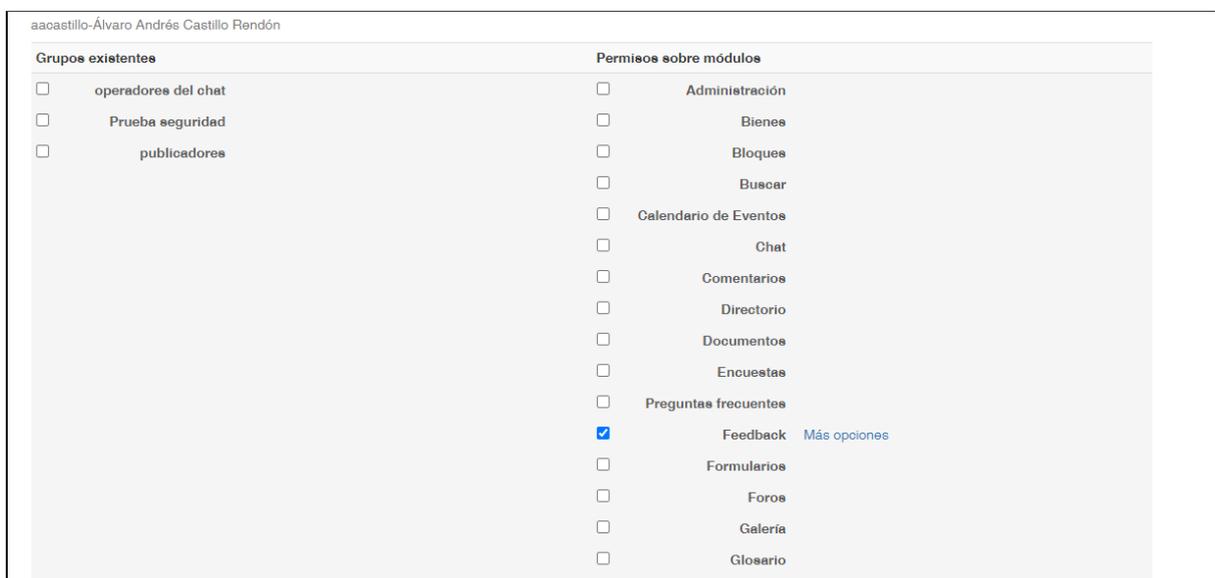
- **Configuración de captcha al iniciar sesión , formulario entre otros.**

- **Restricción por intentos fallidos al iniciar sesión.**



7. Se oculta y restringe páginas de acceso administrativo.

R/ Los módulos de administración del portal web son restringidos por un usuario y contraseña con sus permisos asignados a los módulos.



8. Se restringe la escritura de archivos desde la web a través de la asignación de permisos de solo lectura.

R/ El módulo de documentos tiene una opción de modo seguro que permite solo la lectura para documentos pdf, los archivos que no tienen esta opción pueden ser descargados desde la plataforma como usuario final, mientras esta categoría o archivo no esté como inactivo, porque si está inactivo solo podrán verlo los administradores del módulo.

GOBERNACIÓN DEL VALLE
SEDE ELECTRÓNICA

Valle
Invencible

GOBERNACIÓN DEL VALLE

Inicio > Documentos > Departamento Administrativo de Desarrollo Institucional
> Formatos para Trámites, OPAS (otros procedimientos administrativos) y servicios
> Formatos solicitudes de servicios Pasivo Pensional

Formatos solicitudes de servicios Pasivo Pensional

Ayuda [Compartir](#) [Buscar](#)

Ordenar por --- Seleccione ---

	Nombre FO-M8-P3-06 V04 SOLICITUD EXPEDICION CERTIFICADOS.docx 0.07 MB 15/05/2020
	Descripción Formato para solicitud de expedición de certificados (activos y jubilados) en formato Word.

FO-M8-P3-06 V04...pdf

Ayuda [Historio](#)

Actualizar archivo

Archivo actual	FO-M8-P3-05 V01 SOLICITUD CERTIFICADO TIEMPO DE SERVICIO.pdf
Tamaño	155 KB
Tipo de documento	Trámites, Servicios y Opas
Fecha de expedición	15/08/2018
Descripción*	Formato para solicitud de certificado tiempo de servicio (activos / retirados / jubilados) en formato PDF.
Estado	Activo
Documento seguro <input checked="" type="checkbox"/>	(Solo aplica para documentos PDF)
Modificar archivo	Seleccionar archivo Ningún archivo seleccionado

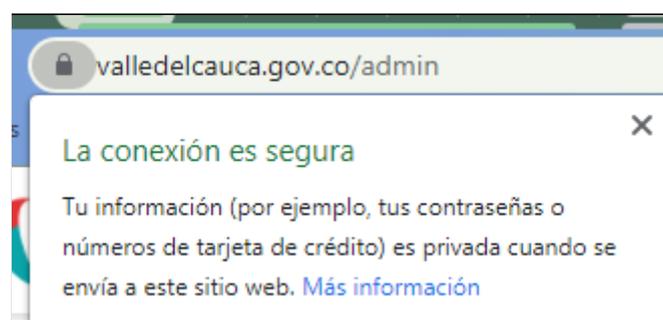
Cuando está marcada la opción documento seguro se visualiza así:

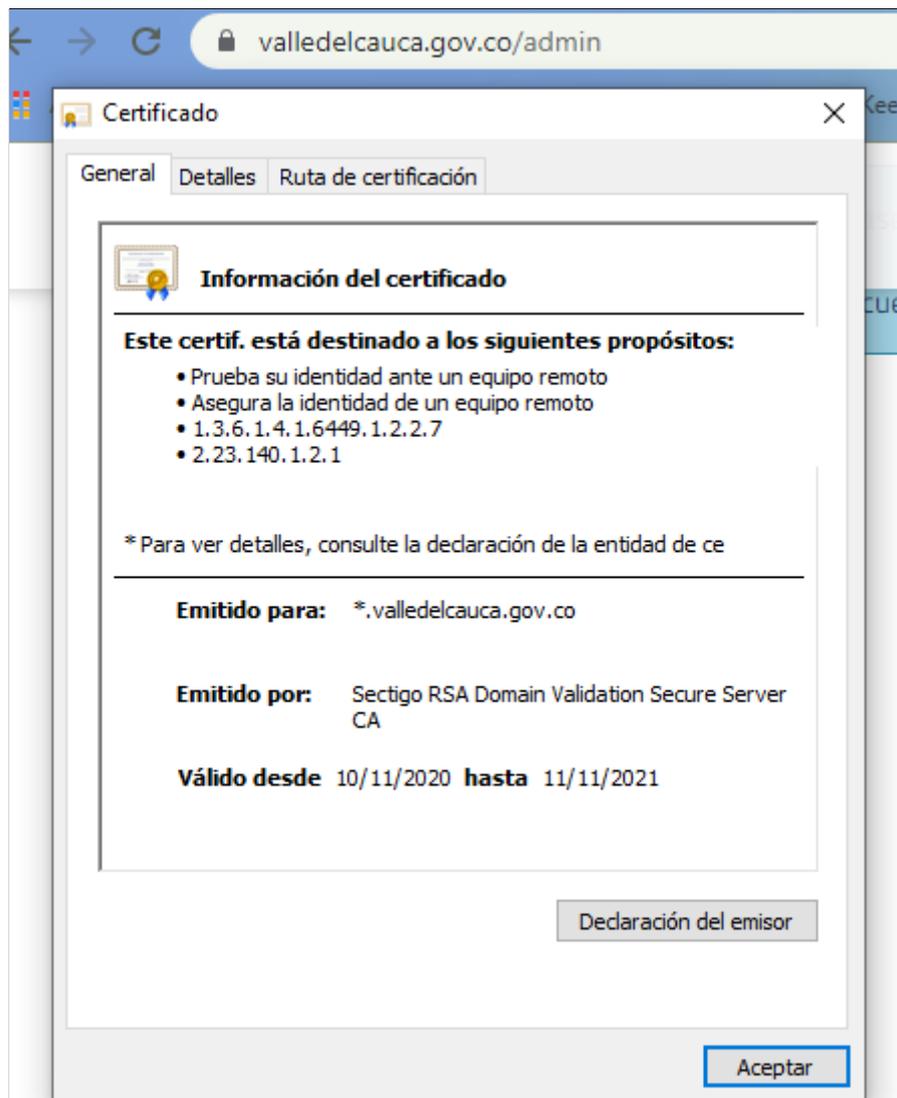
 Departamento del Valle del Cauca Gobernación	SOLICITUD CERTIFICADO TIEMPO DE SERVICIO (ACTIVOS / RETIRADOS / JUBILADOS)	Código: FO-M8-P3-05
		Versión: 01
		Fecha de aprobación: 15/08/2018
		Página 1 de 2

NOMBRE(S):
CÉDULA DE CIUDADANÍA:
DEPENDENCIA EN LA QUE LABORÓ (1):
CARGO:
FECHA: DESDE: día ___ mes ___ año ___ HASTA: día ___ mes ___ año ___
DEPENDENCIA EN LA QUE LABORÓ (2):
CARGO:
FECHA: DESDE: día ___ mes ___ año ___ HASTA: día ___ mes ___ año ___
Observaciones: (opcional):
¿PRESENTÓ ALGUNO DE LOS SIGUIENTES AUSENTISMOS?:

9. Se garantiza conexiones seguras a través del uso de certificados, SSL (HTTPS para la confianza de usuarios) y cifrado en la estructura de las peticiones para portales transaccionales, para evitar la manipulación de parámetros en las peticiones. (adicional al cifrado SSL), También deben habilitar las cabeceras de seguridad, entre otras las siguientes: Content-Security-Policy (CSP), X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Strict-Transport-Security (HSTS), Public-Key-Pins (HPKP) Referrer-Policy, Feature-Policy.

R/ Si existe el uso de certificados SSL también hay cabeceras de seguridad implementadas además de otros sistemas de seguridad.





10. Se Implementa mensajes genéricos de error, que no revelen información acerca de la tecnología usada, excepciones o parámetros que dispararon el error específico, los cuales deberán ser comprensibles por parte de las personas, incluyendo la accesibilidad para las personas con discapacidad.

R/ Si están desactivados los mensajes errores por defecto y los mensajes que se muestran no revelan información sensible.



11. Se protege el binario de la aplicación, a través de métodos de ofuscación que impidan realizar procedimientos de ingeniería inversa (reversing) para analizar la lógica de la aplicación.

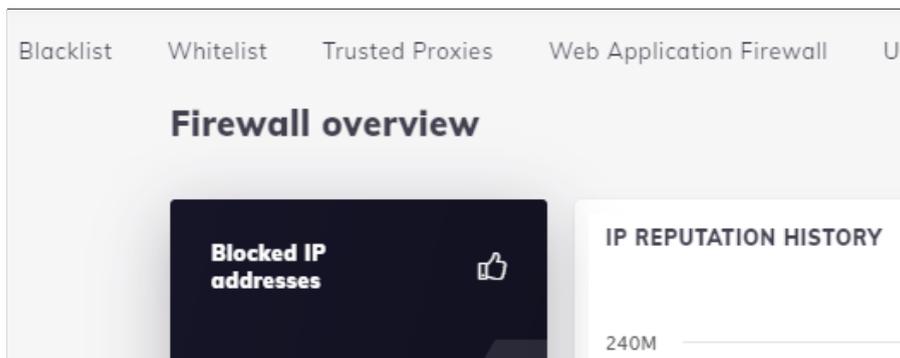
16. Se restringe la escritura de archivos en el servidor web a través de la asignación de permisos de roles y los privilegios asociados.

R/ Sí hay control y restricción sobre qué usuario o servicio puede realizar lectura o ejecución en el servidor web así como como en los demás servicios.

```
user nginx;  
worker_processes
```

17. Se implementan controles de protección de acceso y de ataques como Cross-site scripting y SQL injection

R/ Sí hay una herramienta WAF para prevenir o hacer frente a los ataques como Cross-site scripting y SQL injection también otras herramientas frente a este tipo de ataques.



System
BL_PORT_HONEYPOT_BADPORT
BL_WEB_HONEYPOT_DELIST_BADURL
BL_SMTP_REQUEST_ATTEND
BL_WEB_HONEYPOT_CAPTCHA_FAIL
WL_WEB_HONEYPOT_BIC_SUCCESS
BL_BN_LOG
WL_WEB_HONEYPOT_CAPTCHA_SUCCESS
BL_BN_DOS