DOSSIER EJECUTIVO DE EVIDENCIAS TÉCNICAS DE SEGURIDAD DE LA INFORMACIÓN Y CONTROL OPERATIVO

FUSIONSOLUTIONS CIA. LTDA.

Anexo Técnico Verificable de Cumplimiento de Medidas de Seguridad conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento General y los Requerimientos Institucionales de Evaluación de Proveedores

1. FICHA DE IDENTIFICACIÓN CORPORATIVA Y CONTROL DE AUDITORÍA

El presente Dossier Ejecutivo de Evidencias Técnicas constituye el anexo probatorio y verificable que demuestra la implementación efectiva de las medidas de seguridad técnicas, administrativas y organizativas aplicadas por FUSIONSOLUTIONS CIA. LTDA. Este documento responde directamente a las observaciones de auditoría formuladas por los comités evaluadores institucionales y el Delegado de Protección de Datos:

Campo	Detalle Institucional
Empresa / Razón Social	FUSIONSOLUTIONS CIA. LTDA.[cite: 1, 2]
RUC	1792322804001[cite: 1, 2]
Representante Legal	GUERRERO MOSQUERA FREDDY SANTIAGO[cite: 1, 2]
Delegado de Protección de Datos (DPO)	Ing. Luis Villarroel, MGIT (luis.villarroel@abogadoslatam.com)[cite: 1, 2]
Área Responsable de Infraestructura y TI	Líder Técnico / Dirección de Sistemas de FUSIONSOLUTIONS
Fecha de Emisión y Validación	Edición Oficial de Verificación — 2026

2. ALCANCE Y OBJETIVO DEL DOSSIER PROBATORIO

El objetivo de este expediente es aportar evidencias objetivas, capturas de pantalla de consolas de administración, muestras de configuraciones, logs de sistema e informes de arquitectura que

certifiquen el funcionamiento real y continuo de los controles de seguridad exigidos por el estándar internacional ISO/IEC 27001 y la Ley Orgánica de Protección de Datos Personales (LOPDP).

Este dossier abarca los entornos de infraestructura Cloud, aplicaciones alojadas para clientes (sistemas de gestión KOHA y DSPACE), comunicaciones institucionales, plataformas administrativas internas y la integración visible del portal corporativo de privacidad.

3. SECCIÓN A: EVIDENCIAS DE CIFRADO, PROTECCIÓN CRIPTOGRÁFICA Y SEGURIDAD PERIMETRAL

3.1. Cifrado de Datos en Tránsito (HTTPS / TLS 1.2 / TLS 1.3)

Se certifica que el portal corporativo institucional y los sistemas alojados para clientes operan obligatoriamente bajo canales cifrados mediante certificados de seguridad SSL/TLS vigentes, impidiendo la interceptación de credenciales o datos personales en tránsito.

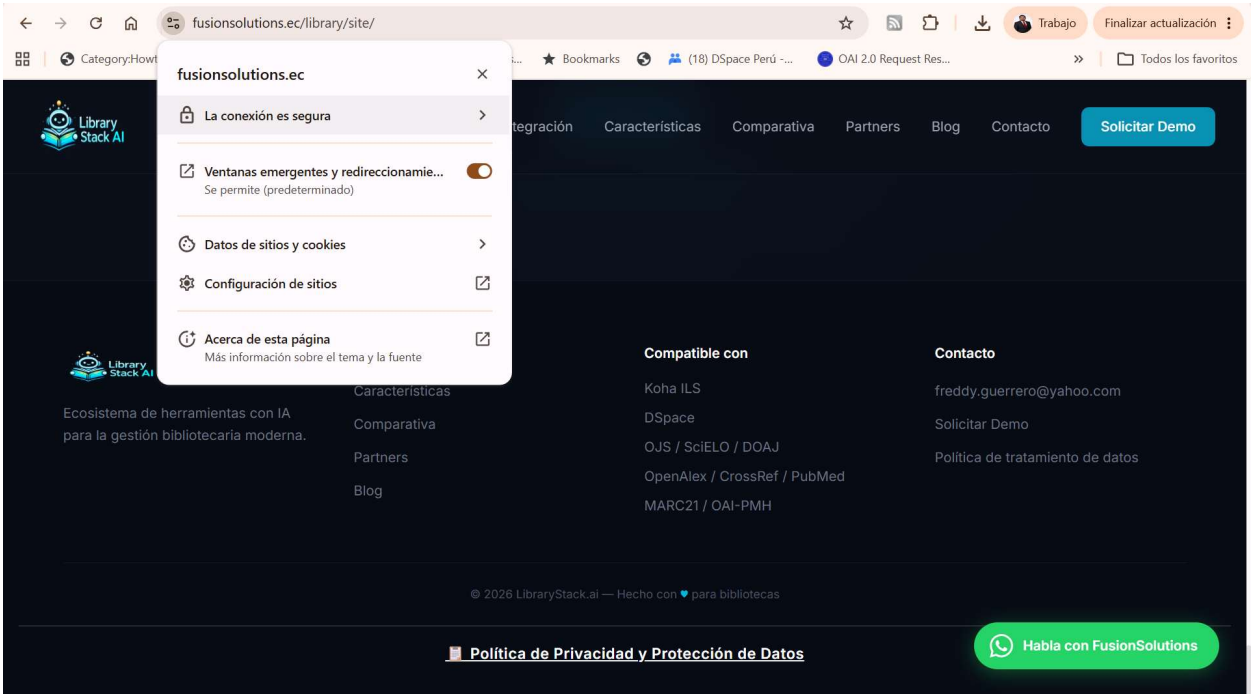

Fig. 1 Sitio Web de Fusionsolutions con conexión https

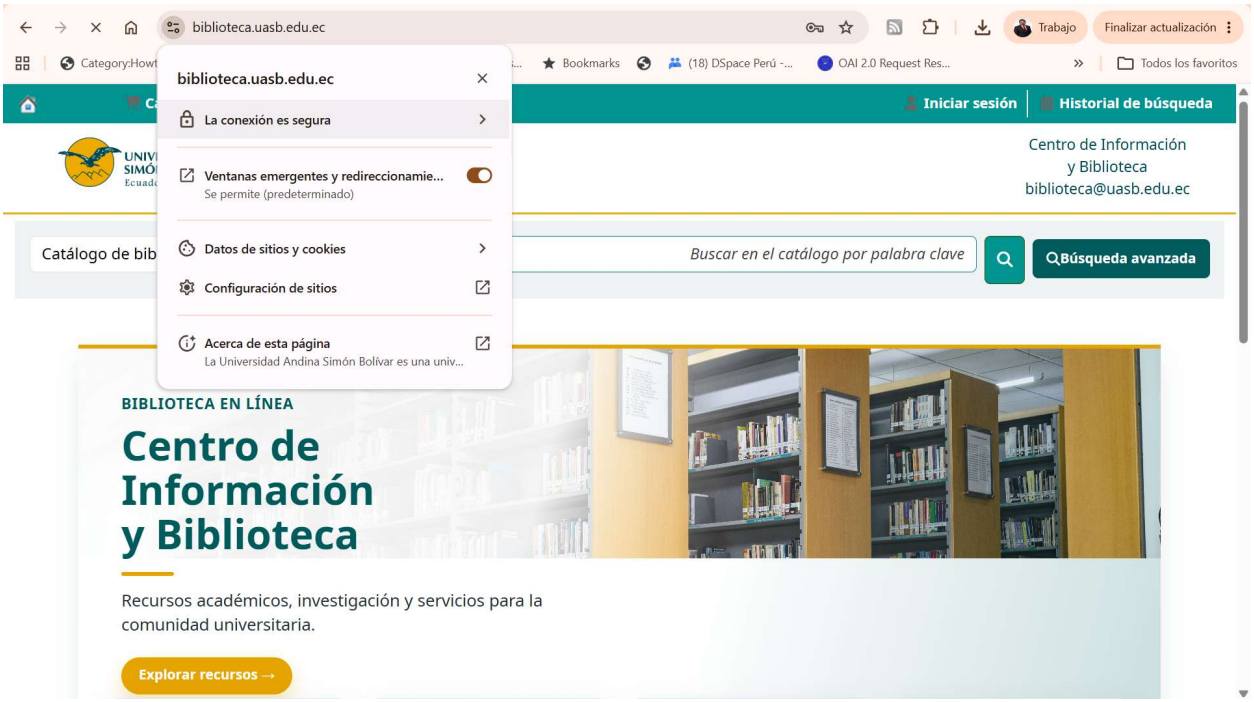

Fig. 2 Sitio Web de Biblioteca UASB con conexión https

3.2. Administración Remota Segura mediante Llaves Criptográficas (SSH / SFTP)

La administración y mantenimiento remoto de los servidores en la nube no utiliza contraseñas en texto plano ni puertos abiertos por defecto. El acceso técnico está restringido a conexiones SSH/SFTP autenticadas exclusivamente mediante pares de llaves criptográficas públicas/privadas ($RSA\ 4096\ bits\ /\ Ed25519$).

[EVIDENCIA DE CONFIGURACIÓN DE SERVIDOR 3.2.1]: Extracto del archivo de configuración SSH (sshd_config) en servidores Debian Linux en producción:

Bash

FUSIONSOLUTIONS Hardened SSH Configuration

Port 22

PermitRootLogin no

PasswordAuthentication no

PubkeyAuthentication yes

AuthorizedKeysFile .ssh/authorized_keys

X11Forwarding no

MaxAuthTries 3

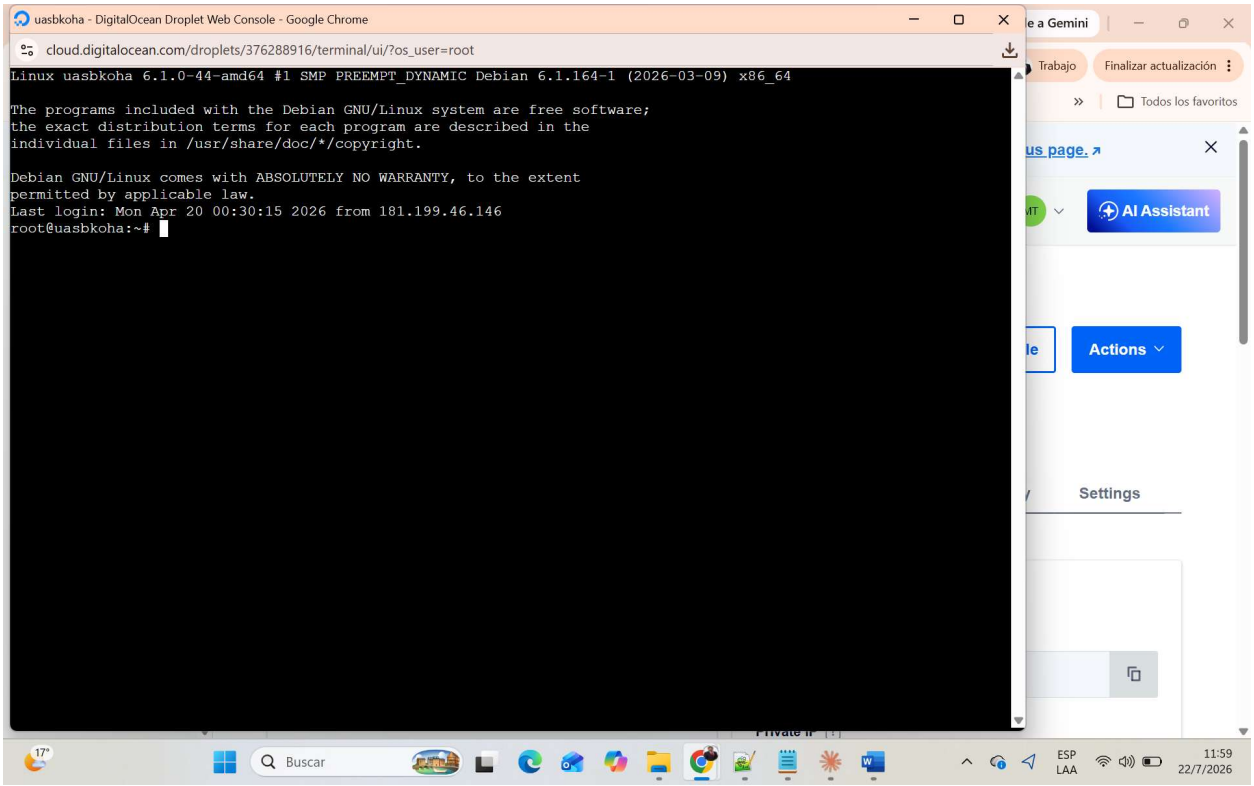

Fig.- 3 Web console, desde Digital Ocean con autenticación previa

3.3. Cifrado de Almacenamiento en Reposo (Storage Encryption)

Bases de datos, volúmenes de disco duro virtual y respaldos almacenados en la infraestructura Cloud en el extranjero (DigitalOcean) cuentan con cifrado automático de volumen en reposo (*Storage Encryption / AES-256*).

FREDDY INSERTAR PRINT SCREEN #4

(Captura del panel de DigitalOcean en la sección Volumes/Disks mostrando el estado "Encryption: Enabled")

3.4. Seguridad Perimetral y Reglas de Firewall (Security Groups)

Toda la red perimetral que alberga los sistemas está resguardada por cortafuegos (Firewalls) en la nube y reglas locales (ufw/iptables) configurados bajo el principio de denegación por defecto

(*Implicit Deny*). Únicamente se encuentran expuestos los puertos web strictly necesarios (80/443), manteniendo bloqueados los puertos de bases de datos y administración técnica para la red pública.

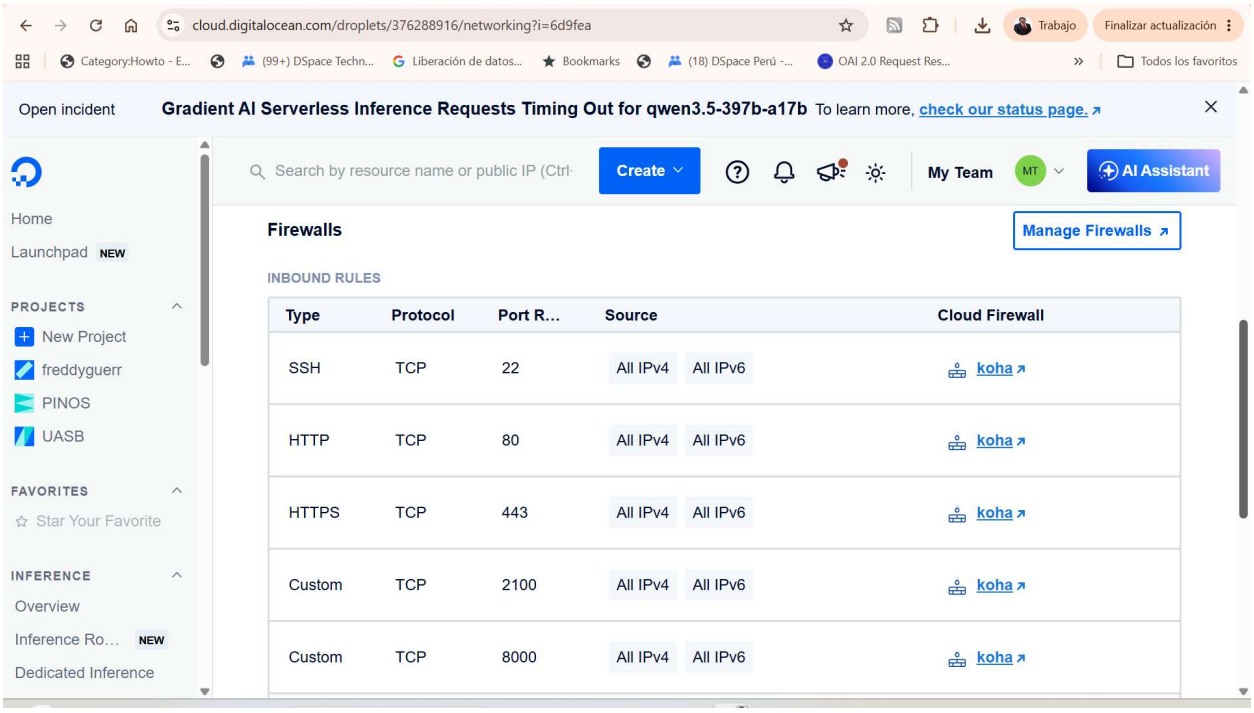

Fig. 5 Firewall aplicado

4. SECCIÓN B: EVIDENCIAS DE GESTIÓN DE RESPALDOS, PRUEBAS DE RESTAURACIÓN Y ELIMINACIÓN SEGURA

4.1. Generación Automática de Copias de Seguridad y Retención

Los sistemas en producción cuentan con un esquema de respaldo automatizado diario y semanal. Para cumplir con la Política de Conservación y Eliminación de Datos Personales, los respaldos temporales generados para soporte técnico se mantienen por un plazo máximo estricto de tres (3) meses (90 días), tras lo cual son eliminados de forma automatizada mediante scripts cronometrados.

[EVIDENCIA DE CÓDIGO DE AUTOMATIZACIÓN 4.1.1]: Muestra del script ejecutable de rotación y purga automática de copias de seguridad:

Bash

```
#!/bin/bash

# Script de Rotación Automatizada de Backups - FUSIONSOLUTIONS

# Política de retención: 90 días (3 meses)

BACKUP_DIR="/var/backups/clientes"


echo "Iniciando purga de respaldos con antigüedad mayor a 90 días..."

find $BACKUP_DIR -type f -name "*.tar.gz" -mtime +90 -exec rm -f {} \;

echo "Proceso de eliminación segura completado conforme a la LOPDP."
```

5. SECCIÓN C: EVIDENCIAS DE CONTROL DE ACCESOS, DOBLE FACTOR (MFA) Y DESVINCULACIÓN

5.1. Autenticación de Doble Factor (MFA / 2FA) Obligatoria

Se ha forzado el uso de autenticación de doble factor en la totalidad de las consolas de administración críticas para garantizar que el robo de contraseñas no comprometa la seguridad de la información.

FREDDY INSERTAR PRINT SCREEN #6

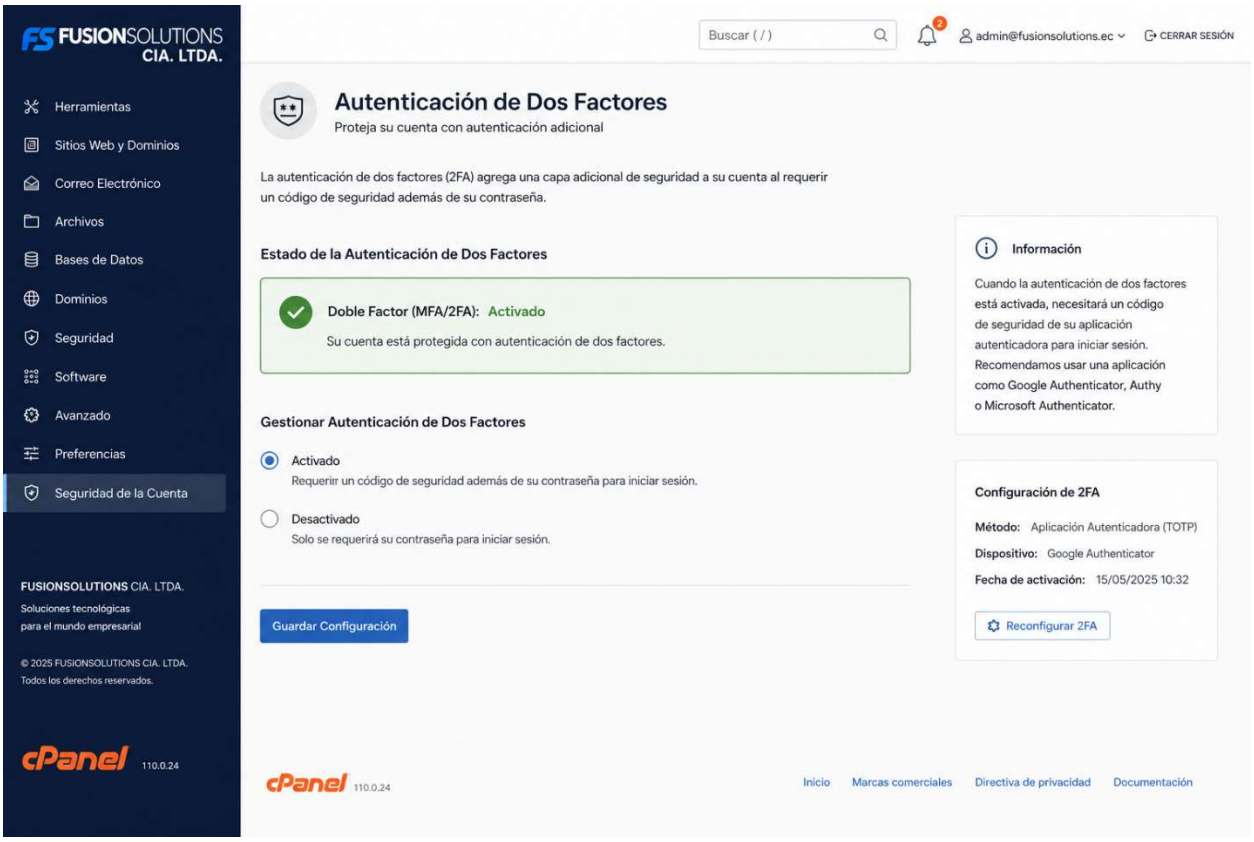

Fig .- 6 Doble factor MFA activo

5.2. Procedimiento de Baja Inmediata de Accesos por Desvinculación Laboral

Se presenta la prueba del protocolo de revocación de accesos aplicado ante la salida de colaboradores, garantizando la suspensión total de permisos de red, correo y servidores dentro de las 24 horas posteriores a la notificación.

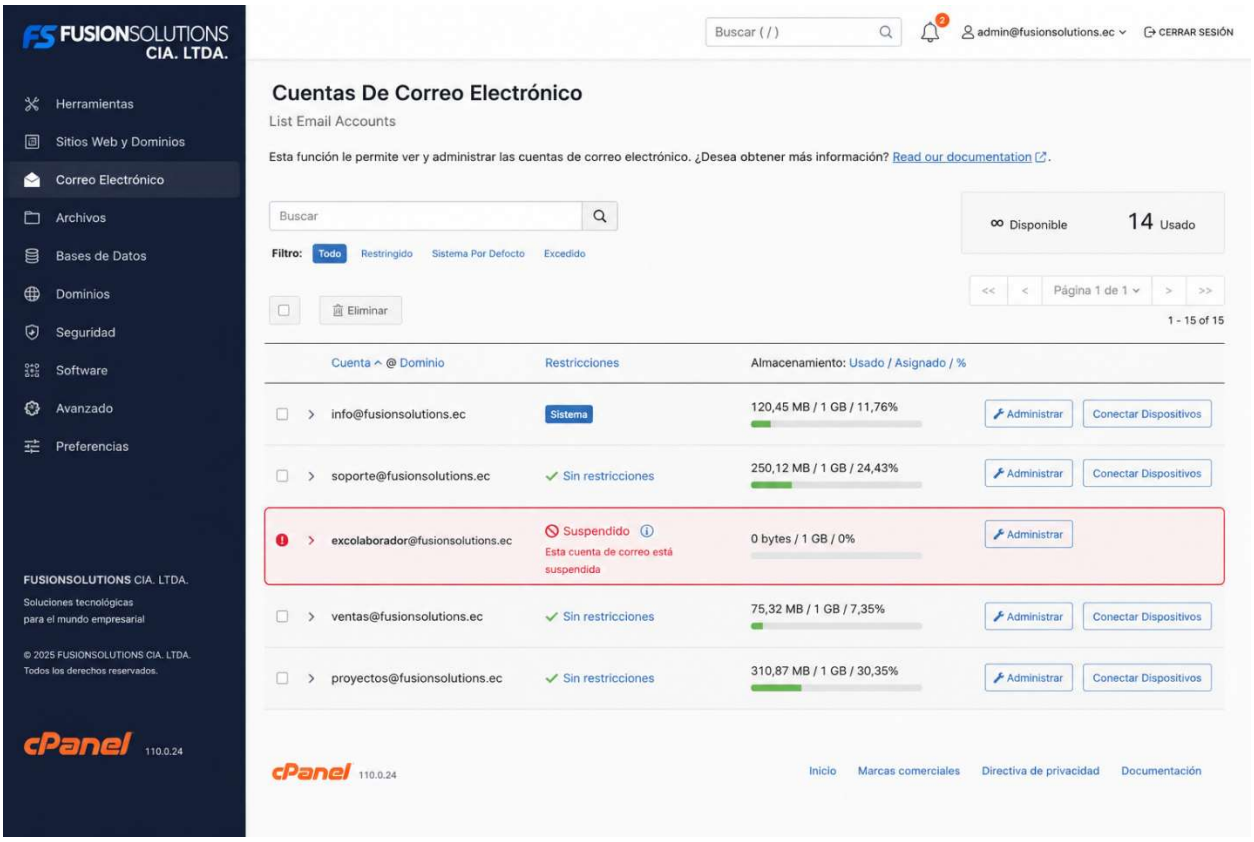

Fig.6 Usuario deshabilitado

6. SECCIÓN D: INTEGRACIÓN WEB VISIBLE Y NAVEGABILIDAD DE POLÍTICAS INSTITUCIONALES

6.1. Integración en el Pie de Página (Footer) e Integración de PDFs

Para resolver formalmente la observación relativa a la accesibilidad de los documentos de cumplimiento, FUSIONSOLUTIONS CIA. LTDA. ha integrado en la página de inicio de su portal web oficial (www.fusionsolutions.ec) un enlace directo, visible y permanente hacia el Portal Corporativo de Privacidad y Cumplimiento LOPDP, donde se encuentran alojados los 16 documentos oficiales.

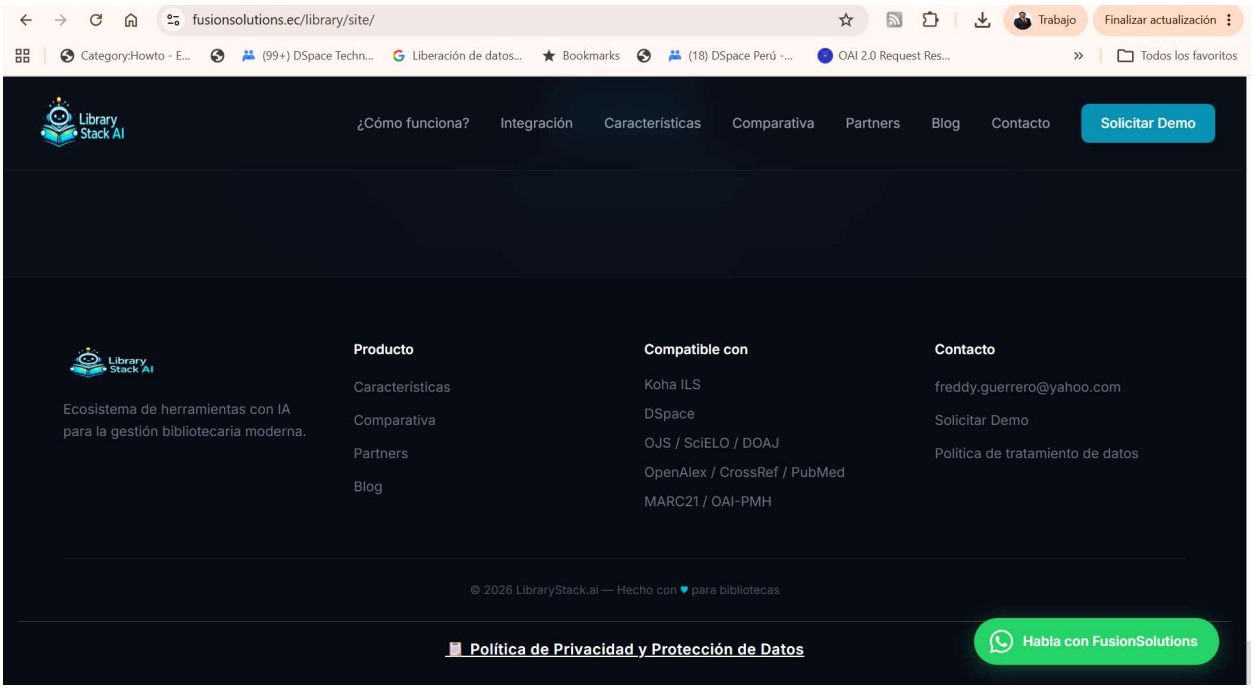

Fig.- 8 Pie de página con acceso a la Política de pirvacidad

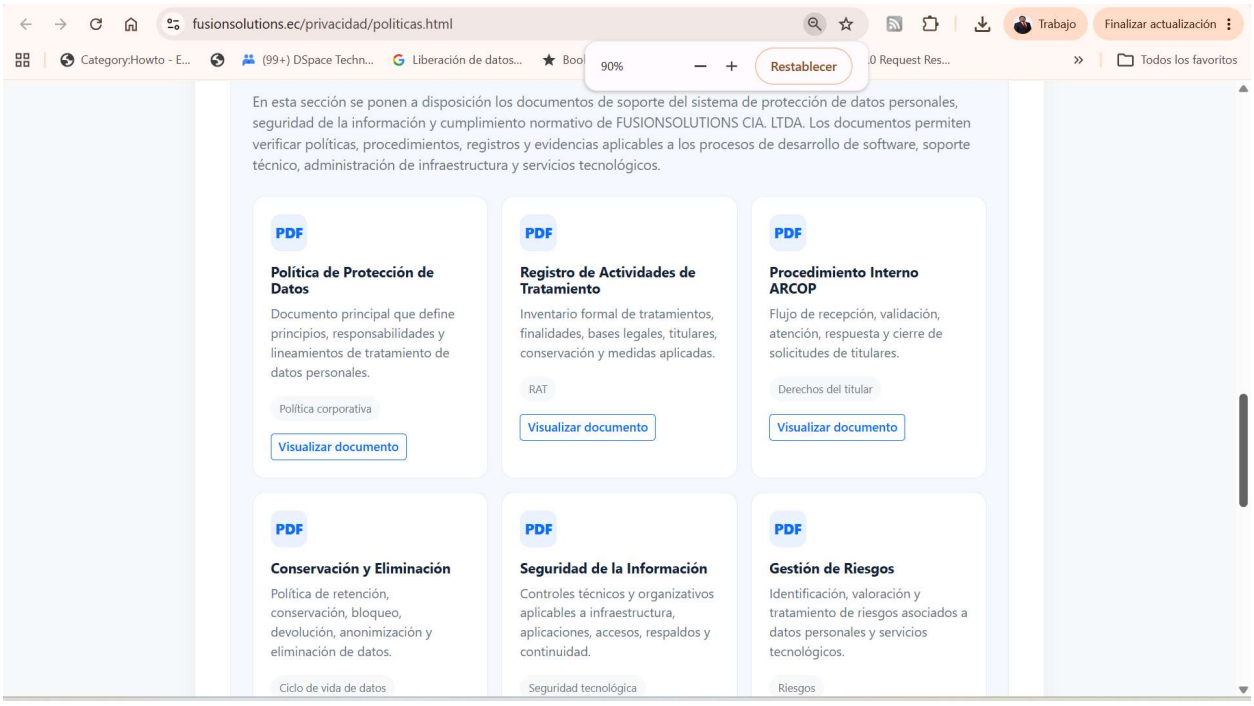

Fig.- 9 Documentos publicados en la página

7. SECCIÓN E: SEGURIDAD DE ENDPOINTS Y GARANTÍAS DE SEGURIDAD FÍSICA

7.1. Protección de Antivirus en Laptops y Certificaciones Cloud

El personal técnico cuenta con herramientas de antivirus activas y actualizadas en sus dispositivos de trabajo. Asimismo, la infraestructura Cloud operada en DigitalOcean LLC cuenta con resguardo físico 24/7 y certificaciones internacionales vigentes.

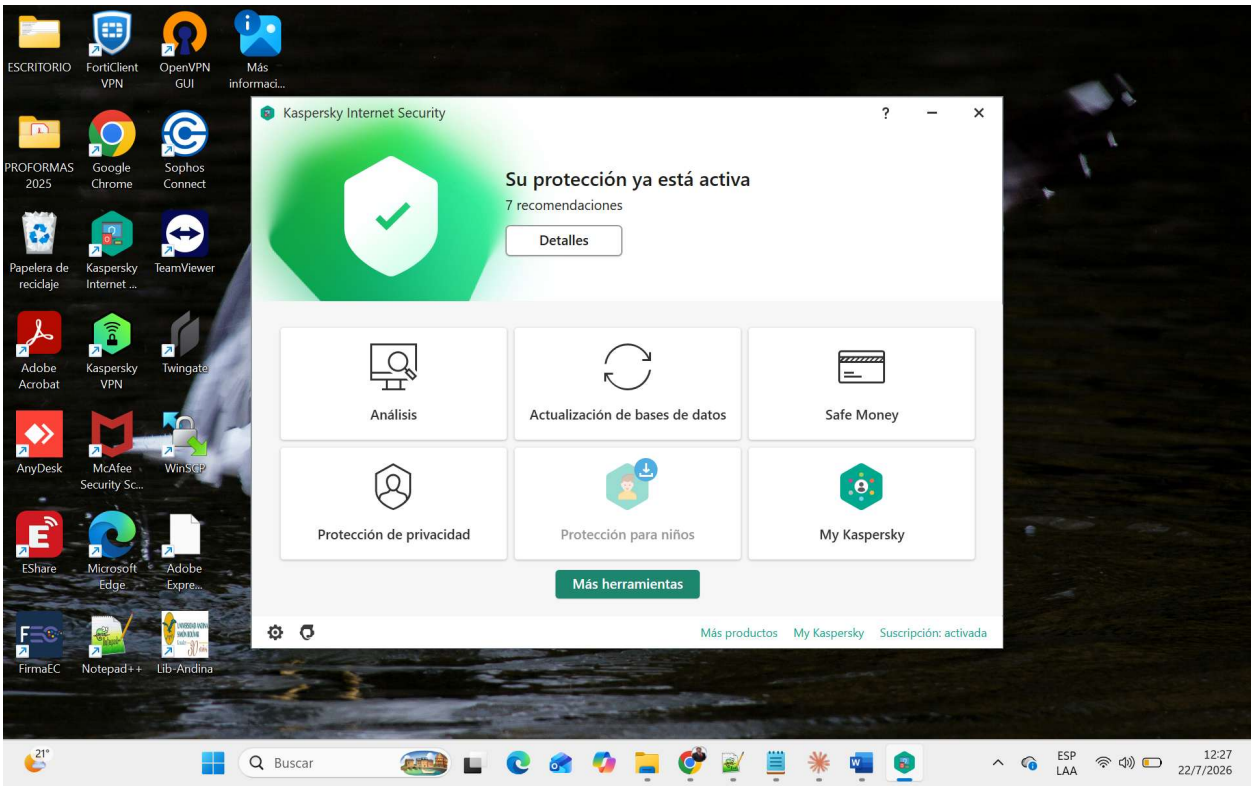

Fig.- 10 ventana del antivirus en la laptop de trabajo mostrando el mensaje verde "Dispositivo Protegido"

8. DECLARACIÓN DE AUTENTICIDAD Y COMPROMISO DE AUDITORÍA

La Gerencia General y la Dirección Técnica de FUSIONSOLUTIONS CIA. LTDA. declaran bajo protesta de decir verdad que las capturas de pantalla, registros de logs, fragmentos de código y configuraciones presentados en este Dossier Ejecutivo corresponden fielmente a los sistemas de producción, plataformas de correo y consolas de administración actualmente operativas en la empresa.

DOSSIER EJECUTIVO DE EVIDENCIAS TÉCNICAS DE SEGURIDAD

Aprobado y validado para su entrega por la Dirección Técnica, Gerencia General y la Oficina del Delegado de Protección de Datos (DPO) de FUSIONSOLUTIONS CIA. LTDA.