

INFORME DE SEGURIDAD

Conformidad con ISO/IEC 27001:2022

1. Introducción

El presente Informe de Seguridad describe los controles, capacidades técnicas y medidas de protección implementadas en el servicio en nube de ETB, el cual permite a los clientes alojar cargas de trabajo empresariales en una nube confiable

El servicio opera bajo el marco del **SGSI de ETB, certificado en la norma ISO/IEC 27001:2022**, garantizando la gestión de riesgos, la protección de la información, la continuidad del servicio y el cumplimiento de controles exigidos por la norma.

El producto de Hosting Virtual provee recursos de cómputo, almacenamiento y networking, con posibilidad de integración híbrida y esquemas de recuperación ante desastres (DRaaS). Se soporta en una arquitectura multitenant, orientada a flexibilidad, escalabilidad y eficiencia operativa. ETB administra la infraestructura subyacente y entrega servicios mediante Internet o canales de datos dedicados.

Los componentes tecnológicos principales incluyen:

2.1 Hardware

- **Hitachi Virtual Storage Platform G350 y G370** con múltiples tiers (SSD, SAS, NL-SAS) que soportan cargas críticas.
- **Switches Dell EMC PowerEdge MX SmartFabric y Cisco Nexus**, garantizando baja latencia, segmentación y redundancia.
- Infraestructura moderna de aliados tecnológicos: **Dell-EMC, Hitachi, VMware.**

2.2 Software y Virtualización

- **VMWare vSphere 6.7 ESXi** para despliegue de máquinas virtuales.
- **VMWare NSX 6.4.6** para microsegmentación, virtualización de redes y servicios Edge Gateway.
- **VMWare vCloud Director 10** para orquestación, multi-tenant y gestión integrada.

01/08/2025

07-07.7-F-020-v.10

"Una vez impreso este documento, se considerará **documento no controlado**"

- **VMWare vCloud Availability 4.0** para replicación y failover de máquinas virtuales.

2.3 Sites de operación

- **ETB Ciudad Universitaria – Bogotá**
- **ETB Santa Mónica – Cali**

Ambos sitios operan como infraestructura activa para servicios de DR, continuidad y resiliencia.

3. Controles de Seguridad Implementados (ISO/IEC 27001:2022)

A partir de la arquitectura descrita, los controles aplicados se alinean con los dominios de la norma, particularmente los controles del Anexo A (versión 2022).

3.1 Controles de Control de Acceso (A.5)

- Segmentación lógica mediante **NSX**, aislamiento por tenant y microsegmentación.
- Control de tráfico perimetral y reglas de firewall distribuidos.
- Gestión de roles y privilegios en plataformas VMware y consolas administrativas.
- Autenticación reforzada para administradores y monitoreo de accesos críticos.

3.2 Controles de Protección de la Información (A.8)

- **Terminación SSL** con aceleración AES-NI.
- Certificados administrados en LB y pasarela de servicios (Client-Side + Server-Side SSL).
- Soporte **IPv6** bajo estándares de encriptación.
- Backups protegidos con Dell EMC NetWorker.

07-07.7-F-020-v.10

01/08/2025

“Una vez impreso este documento, se considerará **documento no controlado**”

3.3 Controles Antimalware (

Se implementa:

- **Symantec Endpoint Protection (Broadcom)** para sistemas Windows y Linux.
- Actualización de firmas y análisis continuo de amenazas.

3.4 Controles de Respaldo y Recuperación

- Política de backup predeterminada:
 - **Incremental diario**
 - **Full semanal**
 - **Retención mensual**
- Respaldos almacenados en disco.
- Replicación y failover mediante **vCloud Availability 4.0**.
- Eliminación de snapshots una vez se ejecuta copia de seguridad para evitar inconsistencias.
- Opcionalmente, snapshots con retención máxima de 48 horas (solo si el cliente lo solicita).

3.5 Seguridad en Comunicaciones

- Switches Dell EMC y Cisco Nexus con políticas de redundancia.
- Virtualización de red mediante NSX (túneles seguros, aislamiento lógico).
- Balanceadores de carga compatibles con:
 - **TCP, UDP, HTTP, HTTPS**
 - Algoritmos: *Weighted Round Robin, IP Hash, URI, Least Connection*.
- Modos L4/L7 transparente para alta disponibilidad.

07-07.7-F-020-v.10

01/08/2025

"Una vez impreso este documento, se considerará **documento no controlado**"

3.6 Controles de Continuidad del Negocio

- Arquitectura multisitio (Bogotá – Cali).
- DRaaS habilitado para cargas críticas.
- Orquestación de failover automatizado con VMware.
- Plan de continuidad y recuperación dentro del SGSI certificado por ISO 27001.

3.7 Monitoreo y Detección

- **vRealize Operations Manager 7 Enterprise:**
 - Optimización de carga
 - Planeación de capacidad
 - Alertas tempranas
 - Troubleshooting con visibilidad 360°
- **vRealize Log Insight:**
 - Recolección de logs en tiempo real
 - Análisis por algoritmos de autoaprendizaje
 - Correlación de eventos
 - Identificación de amenazas y anomalías

4. Riesgos Mitigados por la Arquitectura

1. **Riesgo de indisponibilidad**
Mitigado con arquitectura multitenant, sites redundantes y balanceo L4/L7.
2. **Riesgo de pérdida de información**
Controlado mediante políticas de backup, retención mensual y replicación en DR.

07-07.7-F-020-v.10

01/08/2025

“Una vez impreso este documento, se considerará **documento no controlado**”

3. Riesgo de brechas de seguridad

Reducido gracias a microsegmentación NSX, firewalls distribuidos, SSL terminación y controles de acceso.

4. Riesgo de ataques malware o ransomware

Minimizado mediante antivirus centralizado y análisis continuo en endpoints virtuales.

5. Riesgo de fallas operativas

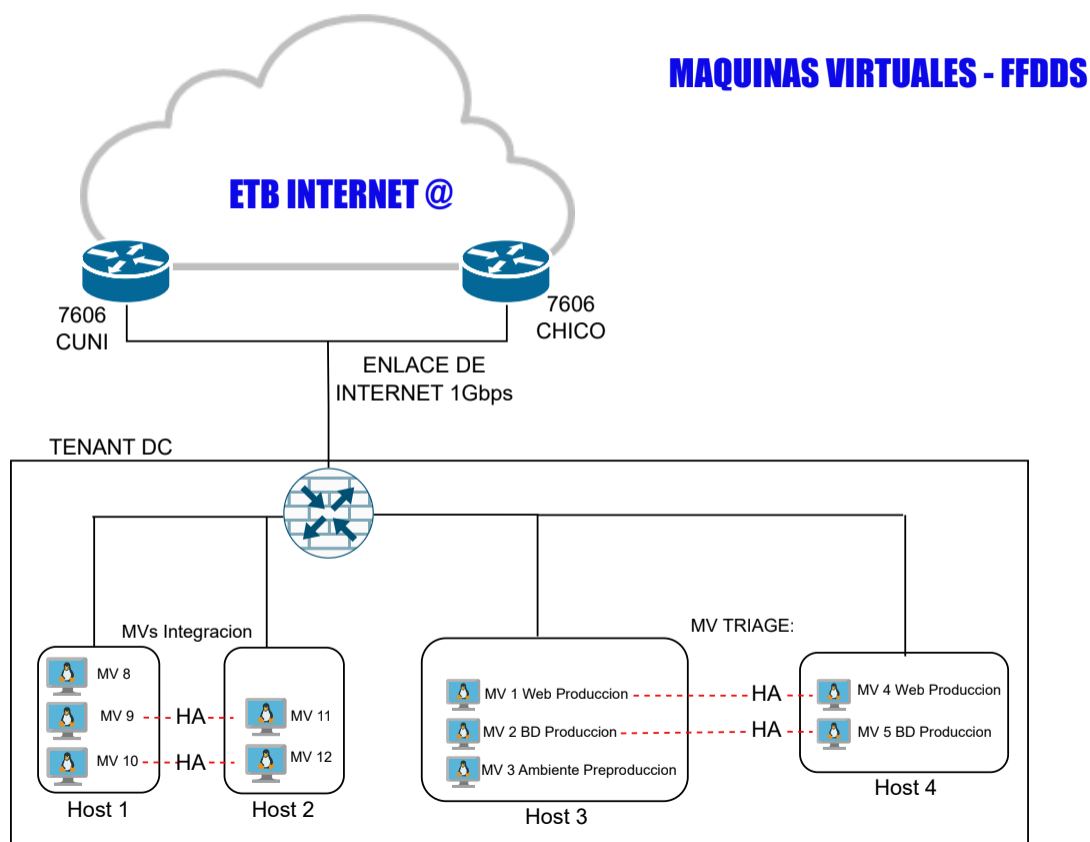
Mitigado con monitoreo 24/7, analítica avanzada y automatización mediante vRealize.

5. Cumplimiento ISO/IEC 27001:2022

ETB opera esta plataforma bajo su **SGSI certificado**, lo que garantiza:

- Gestión integral de riesgos.
- Controles del Anexo A implementados para infraestructura, comunicaciones, acceso, operaciones y continuidad.
- Ciclo PHVA (Planear – Hacer – Verificar – Actuar) aplicado a plataforma de Hosting Virtual.
- Auditorías internas y externas anuales.
- Políticas corporativas de seguridad, confidencialidad y uso aceptable.
- Controles específicos para proveedores, integridad de la información y protección de datos sensibles.

6. Diagrama máquinas virtuales



7. Conclusiones

La plataforma de Hosting Virtual de ETB proporciona un entorno altamente seguro, resiliente y alineado con los requisitos de la **ISO/IEC 27001:2022**. Su arquitectura moderna basada en VMWare, almacenamiento Hitachi y hardware Dell-EMC, combinada con microsegmentación, monitoreo avanzado, políticas de backup robustas y capacidades DRaaS, garantiza:

- **Confidencialidad, Integridad y Disponibilidad** de la información del cliente.
- **Continuidad del negocio** ante fallas o desastres.
- **Cumplimiento de estándares internacionales** de gestión de seguridad.
- **Flexibilidad y escalabilidad** del servicio bajo un modelo IaaS administrado por ETB.

El entorno es adecuado para alojar **cargas sensibles, críticas o de alta disponibilidad**, cumpliendo estrictamente con normas y mejores prácticas del sector.

8. Servidores

Hostname	Sistema operativo	Virtual CPU	RAM(GB)	Disco (GB)	Usuario	IP Servicio
sds-set-pro-01	Red Hat Enterprise Linux release 9.3	4	16	500	padminsys dev02 dev03 dev04	10.216.150.66
sds-setpsql-pro-02	Red Hat Enterprise Linux release 9.3	4	16	500	padminsys dev02 dev03 dev04	10.216.150.67
sds-set-pre-03	Red Hat Enterprise Linux release 9.3	4	16	500	padminsys dev02 dev03 dev04	10.216.150.68
sds-setpsql-proha-04	Red Hat Enterprise Linux release 9.3	4	16	500	padminsys dev02 dev03 dev04	10.216.150.69
sds-set-proha-05	Red Hat Enterprise Linux release 9.3	4	16	500	padminsys dev02 dev03 dev04	10.216.150.70
sds-app-pre-06	Red Hat Enterprise Linux release 9.3	4	16	500	padminsys dev02 dev03 dev04	10.216.150.71
sds-app-pro-07	Red Hat Enterprise Linux release 9.3	10	24	500	padminsys dev02 dev03 dev04	10.216.150.72
sds-pgsql-pro-08	Red Hat Enterprise Linux release 9.3	8	24	1000	padminsys dev02 dev03 dev04	10.216.150.73
sds-app-proha-09	Red Hat Enterprise Linux release 9.3	10	24	500	padminsys dev02 dev03 dev04	10.216.150.74
sds-pgsql-proha-10	Red Hat Enterprise Linux release 9.3	8	24	1000	padminsys dev02 dev03 dev04	10.216.150.75

Firma



Julio César Caicedo Caicedo
 Líder PMO ETB

07-07.7-F-020-v.10

01/08/2025

“Una vez impreso este documento, se considerará **documento no controlado**”