MicroStar, SRL

Proveedor de Servicios de Facturación Electrónica — Documentación de soporte DGII

ANEXO 1.1 — Política de Seguridad de la Información

Código de documento:	MMS-POL-SEG-001
Versión:	1.1
Fecha de emisión:	15 de julio de 2026
Elaborado por:	Leandro Alberto Castillo Flores – Gerente General
Aprobado por:	Leandro Alberto Castillo Flores – Gerente General
Clasificación:	Uso interno / Presentación regulatoria (DGII)

1. Objetivo

Establecer los lineamientos, controles y responsabilidades que MicroStar, SRL (en adelante "MicroStar" o "la empresa") aplica para proteger la confidencialidad, integridad y disponibilidad de la información propia, de sus clientes y de los comprobantes fiscales electrónicos procesados a través de sus plataformas, en cumplimiento de la normativa de la Dirección General de Impuestos Internos (DGII) para proveedores de servicios de facturación electrónica.

2. Alcance

Esta política aplica a toda la infraestructura tecnológica operada por MicroStar, incluyendo los sistemas Hubi (hubi.do), ECFManager (ecfmanager.net.do), FacilPlus (facilplus.do), Gplus (gplus.do), el portal corporativo (microstar.com.do), el portal de pagos/comisiones MSPagos, y el MicroStar Management System — MMS (mms.do), plataforma interna de soporte técnico, documentación y monitoreo de infraestructura, así como el personal, procesos y servidores que dan soporte a dichos sistemas.

3. Infraestructura y arquitectura de servidores

MicroStar opera su infraestructura sobre servidores virtuales privados (VPS) en la nube, distribuidos en dos proveedores independientes como medida de segmentación y redundancia, físicamente ubicados en Estados Unidos:

Identificador	Proveedor	Sistema(s) alojados	Ambiente
srv-prod-A	Proveedor Cloud A	Hubi (hubi.do)	Producción
srv-prod-B	Proveedor Cloud A	Gplus (gplus.do) y FacilPlus	Producción
srv-prod-C	Proveedor Cloud A	Portal corporativo (microstar.com.do), MSPagos y MMS (mms.do)	Producción
srv-qa-01	Proveedor Cloud A	ECFManager (ecfmanager.net.do)	Pruebas / QA
srv-contingencia-01	Proveedor Cloud B	Infraestructura de respaldo / contingencia	Producción

El uso de dos proveedores independientes responde a una estrategia deliberada de mitigación de riesgo: ante una falla, incidente o interrupción del servicio de un proveedor, MicroStar cuenta con

capacidad de operar y redirigir tráfico desde infraestructura independiente.

4. Controles técnicos de seguridad implementados

4.1 Perímetro y filtrado de tráfico

- Firewall a nivel de sistema operativo (UFW – Uncomplicated Firewall) activo en todos los servidores, restringiendo puertos y servicios expuestos al mínimo necesario.
- Nginx como proxy inverso frente a las aplicaciones, centralizando el enrutamiento HTTP/HTTPS y ocultando los servicios internos de acceso directo.

4.2 Cifrado en tránsito

- Todos los dominios de producción (hubi.do, ecfmanager.net.do, facilplus.do, gplus.do, microstar.com.do, mms.do) operan bajo HTTPS con certificados TLS emitidos por Let's Encrypt, con renovación automática.

4.3 Control de accesos

- Acceso administrativo a los servidores exclusivamente mediante SSH con autenticación de clave.
- Las credenciales de acceso administrativo de los servidores de producción y pruebas son de conocimiento exclusivo del Gerente General.
- En el servidor de contingencia (Proveedor Cloud B), no se otorga acceso root; en su lugar se creó un usuario con privilegios elevados de alcance limitado para el personal de soporte autorizado.
- El acceso al panel de administración de cada sistema (Hubi, ECFManager, FacilPlus, Gplus) está restringido por autenticación individual.

4.4 Segmentación

Cada sistema corre en su propio VPS o grupo reducido de VPS, de forma que un incidente de seguridad o de disponibilidad en una aplicación no compromete directamente a las demás.

5. Monitoreo de infraestructura (MMS)

MicroStar opera un sistema centralizado de monitoreo de servidores como parte del MMS, diseñado bajo el principio de mínimo privilegio: el monitoreo nunca requiere ni almacena credenciales root de los servidores monitoreados.

5.1 Arquitectura de agente de bajo privilegio

- Cada servidor monitoreado ejecuta un agente local (proceso propio, sin privilegios de root) que expone únicamente métricas de uso de CPU, memoria y disco, y el estado de un conjunto de servicios previamente autorizado.
- La comunicación entre el MMS y cada agente se autentica mediante un token secreto único por servidor, transmitido únicamente por HTTPS o restringido por firewall a la IP del servidor central del MMS.
- El agente solo puede iniciar o reiniciar los servicios explícitamente incluidos en una lista blanca configurada por el Gerente General — cualquier otro nombre de servicio es rechazado.
- El permiso para ejecutar dichas acciones se otorga mediante reglas de sudo restringidas a comandos exactos (sudoers), nunca acceso root general ni contraseñas compartidas.

5.2 Alertas

El MMS notifica de forma automática cuando el uso de CPU, memoria o disco de un servidor supera umbrales críticos, o cuando un servidor deja de responder, permitiendo una respuesta proactiva antes de que se degrade el servicio a los clientes.

6. Bitácora de eventos (logs) y trazabilidad

Cada uno de los sistemas de facturación electrónica de MicroStar genera un registro (log) individual por transacción y por empresa contribuyente procesada, lo que permite trazabilidad completa de cada comprobante fiscal electrónico gestionado. Estos registros se conservan de forma íntegra dentro de los respaldos (backups) periódicos de cada aplicación, garantizando su disponibilidad histórica para fines de auditoría interna o requerimientos de la DGII.

Adicionalmente, el MMS mantiene una bitácora de auditoría propia que registra inicios de sesión, cambios de estado, y acciones administrativas realizadas dentro del portal de soporte.

7. Gestión de contraseñas y credenciales

Las credenciales administrativas no se comparten ni se almacenan en texto plano. El acceso administrativo a la infraestructura de producción y pruebas está limitado a una única persona responsable (Gerente General), reduciendo la superficie de exposición. Para el servidor con soporte externo se aplica el principio de mínimo privilegio mediante un usuario elevado sin acceso root. El mismo principio aplica a los agentes de monitoreo descritos en la sección 5.

8. Responsables de la seguridad de la información

Rol	Nombre	Responsabilidad
Responsable principal de seguridad	Leandro Alberto Castillo Flores	Administración de accesos, infraestructura, respaldo y respuesta ante incidentes
Soporte secundario	Personal de soporte autorizado	Continuidad operativa en ausencia del responsable principal

9. Vigencia y actualización

La presente política entra en vigor a partir de su fecha de emisión y será revisada como mínimo una vez al año, o antes si se produce un cambio relevante en la infraestructura, los proveedores de hosting, o la normativa aplicable de la DGII. Es responsabilidad del Gerente General mantener este documento actualizado y notificar a la DGII cualquier cambio sustancial conforme a la normativa vigente.