

INFORME JUSTIFICATIVO

Adquisición de una Solución Especializada de Almacenamiento, Confidencialidad, Integridad y Alta Disponibilidad de Datos para la Superintendencia del Mercado de Valores.

I. Contexto Actual

La Superintendencia del Mercado de Valores (SIMV), como entidad autónoma del Estado dominicano, responsable de regular y supervisar el mercado de valores de la República Dominicana, ha venido fortaleciendo su infraestructura tecnológica y sus capacidades de ciberseguridad, en cumplimiento con (i) el Reglamento de Ciberseguridad del Mercado de Valores; (ii) la Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado dominicano; y (iii) el Decreto núm. 313-22 que aprueba la Estrategia Nacional de Ciberseguridad 2030.

Durante este proceso, se ha identificado la necesidad crítica de contar con una infraestructura de almacenamiento de alta disponibilidad, rendimiento y resiliencia, que permita soportar tanto las operaciones actuales como el crecimiento proyectado, garantizando la integridad, confidencialidad y disponibilidad de la información institucional.

El servicio de archivos compartidos institucional se gestiona a través de Windows Server desplegado en una infraestructura en la nube, utilizando el rol de File Server y respaldos automáticos, mediante herramientas nativas de la nube. Esta solución ha permitido dar continuidad al servicio, sin embargo, se han identificado limitaciones importantes que comprometen la eficiencia operativa, la seguridad de la información y la capacidad de respuesta ante incidentes, tales como:

- **Restauraciones granulares ineficientes:** La herramienta de copia de respaldo actual, no permite restaurar archivos individuales de forma ágil ni directamente desde instantáneas, lo que retrasa la recuperación ante errores humanos o incidentes.
- **Dependencia de recursos virtuales y consumo de almacenamiento en la nube:** El uso de almacenamiento en la nube incrementa los costos mensuales a medida que crecen los volúmenes de datos.
- **Ausencia de funciones avanzadas de control de acceso y auditoría de actividad sobre archivos,** lo que limita la visibilidad de uso y el cumplimiento con políticas de seguridad y trazabilidad.
- **Mecanismos nativos de defensa contra ransomware:** Los respaldos no protegen de forma nativa contra ataques de ransomware o eliminación maliciosa de datos por parte de usuarios con acceso elevado.

Estas limitaciones implican un riesgo operativo, un costo de recuperación elevado y una exposición ante auditorías regulatorias, al no poder demostrar con trazabilidad completa el ciclo de vida de la información gestionada.

En el marco del análisis técnico y la exploración de mercado realizada por la Dirección de Tecnología, se evaluaron distintas plataformas NAS empresariales que operan sobre protocolo SMB/CIFS con integración nativa a Active Directory, permitiendo snapshots inmutables, auditoría en tiempo real, protección contra ransomware y operación sin requerir servidores Windows intermedios. Como resultado, se identificó que

únicamente la línea NetApp AFF con sistema operativo ONTAP cumple con todas estas condiciones de manera nativa, integrada, certificada y soportada oficialmente, sin recurrir a soluciones externas, virtualizaciones adicionales ni licenciamientos complementarios. Esta investigación también permitió confirmar la existencia de múltiples representantes autorizados del fabricante en República Dominicana, confirmando que estamos ante un proceso de exclusividad limitada a solo tres representantes locales con capacidad de proveer, instalar, configurar y brindar soporte, los cuales son, según carta del fabricante de fecha veintiocho (28) de mayo del año dos mil veinticinco (2025):



28 de mayo de 2025

Atencion:
Superintendencia del Mercado de Valores de la República Dominicana (SIMV)
Av. César Nicolás Penso No. 66
Santo Domingo
Dominican Republic

Estimados,

NetApp, Inc. es una empresa estadounidense líder en infraestructura de datos. La empresa tiene su sede en San José, California.

NetApp distribuye sus productos y soluciones exclusivamente a través de su red de partners y distribuidores debidamente certificados y autorizados no solo para la comercialización de los productos sino también para la implementación y soporte de estos.

Los representantes autorizados y calificados para comercializar, implementar, soportar y renovar en la República Dominicana, las soluciones y el portafolio completo de NetApp son:

- Integratec: Victor de los Santos victor.santos@integratec.com.do
- PBS: Ricardo Rodriguez ricardo.rodriguez@pbs.group
- IQtek: Jean Pimentel jpimentel@iqteksolutions.com

Quedamos a la orden para cualquier adicional.

Atentamente,

A handwritten signature in black ink, appearing to read 'Carlos Viera'.

Carlos Viera
District Manager LATAM Multi-Country Organization MCO
05/13/2025

LOS

II. Objetivo de la adquisición

El objetivo de contar con una solución de almacenamiento institucional en sitio, incrementar la capacidad de almacenamiento actual con escalabilidad futura, con arquitectura All-Flash para una baja en la latencia y tiempo de respuesta más reducidos. Además de:

- Operación nativa como File Server sobre SMB/CIFS, sin requerir servidores Windows adicionales, con integración directa con Active Directory para gestión de permisos.
- Restauración granular por el usuario, sin intervención de TIC, para los casos de eliminación accidental de documentos, retención inmutable y largo tiempo, de instantáneas. Sistema integrado de auditoría detallada e integración con sistema SIEM y protección contra ransomware basado en IA.

III. Justificación para la selección explícita del modelo NetApp AFF A20 All-Flash

El modelo NetApp AFF A20 All-Flash ha sido seleccionado tras un análisis de soluciones NAS empresariales que operan con SMB/CIFS y se integran con Active Directory. La selección responde a las características necesarias por la SIMV estando presente en esta línea de producto, que no están presentes de forma nativa o eficiente en otras soluciones del mercado, estas características son:

- Operación como File Server sin Windows:** A diferencia de otras soluciones de almacenamiento que requieren una máquina virtual Windows para ofrecer recursos compartidos en SMB, el AFF A20 ofrece esta funcionalidad de forma nativa y segura, eliminando la necesidad de licencias adicionales, configuraciones intermedias o parches del sistema operativo.
- Snapshots visibles como "Versiones Anteriores" en Windows:** Los usuarios pueden recuperar archivos directamente desde el explorador de archivos sin intervención de TI, algo que solo permite el sistema operativo ONTAP, propio de la solución.
- SnapLock:** Mecanismo de retención inmutable a nivel de volumen o archivo, conforme a requerimientos de cumplimiento normativo, sin necesidad de soluciones externas.
- FPolicy:** Motor nativo para auditar y controlar el acceso a archivos en tiempo real, con capacidad para integrarse al SOC y generar alarmas en caso de comportamiento inusual.
- Detección proactiva de ransomware:** ONTAP detecta patrones de cifrado y dispara snapshots automáticos como defensa temprana.
- Gestión centralizada con System Manager y automatización vía API/CLI:** Facilita la administración, el monitoreo y la integración con procesos institucionales.
- Sincronización no disruptiva con almacenamiento en nube,** dando la capacidad de mover automáticamente archivos desde almacenamiento en la nube sin afectar el acceso desde el usuario.

Estas características, sumadas al soporte local de partners certificados y a la madurez de la plataforma ONTAP, hacen del NetApp AFF A20 será la solución alineada con la visión institucional de modernización, continuidad operativa y seguridad de la información.

Base Legal

El párrafo único, numeral 3 del artículo 6 de la Ley núm. 340-06 sobre Compras y Contrataciones Públicas, establece: “Serán considerados casos de excepción y no una violación a la ley, a condición de que no se utilicen como medio para vulnerar sus principios y se haga uso de los procedimientos establecidos en los reglamentos, las siguientes actividades: 3) Las compras y contrataciones de bienes o servicios con exclusividad o que sólo puedan ser suplidos por una determinada persona natural o jurídica”.

El artículo 54 del Reglamento de Aplicación de la Ley núm. 340-06, emitido mediante Decreto núm. 416-23, establece: “Procedimiento de excepción por exclusividad. Se utilizará el procedimiento de excepción por exclusividad para obtener bienes o servicios que por su especialidad solo pueden ser suplidos por un número limitado de proveedores que pueden atender al requerimiento, que en ningún caso podrá ser mayor de cinco (5). Los oferentes que poseen la exclusividad deben demostrarlo mediante una acreditación o certificación, en caso de que la hubiere, que puede ser nacional o internacional, emitida por una persona, institución u organismo público o privado con autoridad para hacerlo.

LOS

IV. Conclusión

En virtud del análisis técnico realizado, la evaluación de mercado y la comparación funcional con otras tecnologías disponibles, se concluye que la solución NetApp AFF A20 All-Flash representa la alternativa más adecuada para resolver las limitaciones actuales del entorno de almacenamiento institucional. Esta solución no solo garantiza la alta disponibilidad, integridad y rendimiento para el acceso a archivos mediante SMB/CIFS con integración nativa a Active Directory, sino que también proporciona características avanzadas de ciberseguridad como snapshots inmutables, auditoría de accesos, detección de comportamiento anómalo y recuperación ante incidentes.

Cabe destacar que, a diferencia de otras opciones del mercado, el NetApp AFF A20 no requiere servidores Windows intermedios para funcionar como File Server, lo que reduce complejidad, costos de licenciamiento y vectores de vulnerabilidad. Asimismo, al estar respaldado por múltiples distribuidores autorizados en el país, se garantiza la competencia de mercado y la disponibilidad de soporte técnico especializado.

Por lo tanto, se recomienda proceder con la adquisición de esta solución como parte de la estrategia de fortalecimiento de la infraestructura tecnológica institucional, cumpliendo con las normativas de ciberseguridad vigentes y alineado a los objetivos estratégicos de continuidad operativa, resiliencia digital y gobernanza de la información.



Leonil Corporan Sosa
CISO SIMV