



**SERVICIOS DIGITALES
POPULAR**

E-commerce

Recomendaciones

para reducir la probabilidad
de bloqueos de conectividad



ÍNDICE

Propósito	3
Recomendaciones Generales	3
Utilizar infraestructura con buena reputación	3
Considerar la ubicación de la infraestructura	3
Mantener patrones de tráfico consistentes	3
Mantener una configuración técnica actualizada	4
Consideraciones Finales	4



Propósito

Compartir recomendaciones orientadas a reducir la probabilidad de restricciones de acceso a aplicaciones y servicios productivos protegidos por controles de seguridad perimetral.

Importante: Estas recomendaciones no constituyen una garantía de acceso a los servicios. Las decisiones de permitir o restringir conexiones son dinámicas y responden a múltiples factores, incluyendo la reputación de las direcciones IP de origen, la ubicación geográfica, requisitos regulatorios, inteligencia de amenazas y el comportamiento observado durante las conexiones. En consecuencia, una dirección IP que actualmente sea considerada confiable podría ser reclasificada en el futuro.

Recomendaciones Generales

Utilizar infraestructura con buena reputación

Se recomienda que las conexiones se originen desde proveedores de Internet, centros de datos o plataformas de nube reconocidas, cuyas direcciones IP mantengan un historial favorable y no presenten reportes relacionados con actividades maliciosas.

Cuando se empleen servicios VPN o plataformas de salida compartida, es aconsejable monitorear periódicamente la reputación de las direcciones IP utilizadas, ya que este factor puede influir directamente en las decisiones de los controles de seguridad.

Considerar la ubicación de la infraestructura

Los accesos pueden estar sujetos a validaciones geográficas, regulatorias o de riesgo. Por esta razón, es recomendable evaluar la ubicación de la infraestructura desde la cual se establecerán las conexiones hacia los servicios productivos.

Mantener patrones de tráfico consistentes

Ciertos comportamientos pueden ser interpretados como actividades de riesgo por los mecanismos de protección. Para minimizar esta posibilidad, se recomienda:

- Evitar incrementos inesperados o excesivos en el volumen de solicitudes.
- Evitar actividades de exploración o enumeración de recursos en ambientes productivos.
- No realizar pruebas de seguridad, escaneos o validaciones agresivas sobre servicios productivos sin la debida coordinación previa.
- Implementar mecanismos adecuados de control de concurrencia, limitación de tasas y gestión de reintentos.

Mantener una configuración técnica actualizada

Se recomienda utilizar protocolos y configuraciones de seguridad vigentes, certificados digitales válidos, resolución DNS correctamente configurada y mecanismos de monitoreo que permitan identificar y atender oportunamente problemas de conectividad o desempeño.

Consideraciones Finales

Los controles de seguridad perimetral evalúan continuamente múltiples indicadores de riesgo con el objetivo de proteger la plataforma, la información y los usuarios. Entre los factores considerados se encuentran la reputación de las direcciones IP, el historial de actividad observada, la inteligencia de amenazas disponible, la ubicación geográfica y los requisitos regulatorios aplicables.

Por lo tanto, aun siguiendo las recomendaciones descritas en este documento, no es posible garantizar que una conexión no sea restringida en algún momento. La reputación del proveedor de hosting, la calidad del servicio VPN utilizado, el comportamiento asociado a las direcciones IP involucradas y otros factores evaluados por los mecanismos de protección pueden influir en la decisión final de acceso.