Política de seguridad de las operaciones

Propietario de la política: Victor Acosta Lopez

Fecha de entrada en vigencia: 09/04/2024

Objetivo

Para garantizar el funcionamiento correcto y seguro de los sistemas e instalaciones de procesamiento de la información.

Alcance

Todos los sistemas de información de D3M3NT SA DE CV que son críticos para el negocio o que procesan, almacenan o transmiten datos de la empresa. Esta Política se aplica a todos los

empleados de D3M3NT SA DE CV y otras entidades de terceros con acceso a redes y recursos del sistema de D3M3NT SA DE CV.

Seguridad de las operaciones

Procedimientos operativos documentados

Los procedimientos operativos, tanto técnicos como administrativos, se documentarán según sea necesario y se pondrán a disposición de todos los usuarios que los necesiten.

Gestión de cambios

Los cambios en la organización, los procesos empresariales, las instalaciones de procesamiento de la información, el *software* y la infraestructura de producción, y los sistemas que afectan la seguridad de la información en el entorno de producción y los sistemas financieros se probarán, revisarán y aprobarán antes de la implementación de la producción. Todos los cambios significativos en los sistemas y redes dentro del alcance deben documentarse.

1. Documentación y revisión de cambios:

- Todos los cambios significativos en los sistemas, redes e instalaciones de procesamiento deben documentarse.
- La documentación debe abarcar el propósito del cambio, la especificación, el impacto potencial considerando las dependencias y el plan de despliegue.
- Los cambios deben probarse y revisarse en entornos segregados tanto de la producción como del desarrollo (por ejemplo, entornos de ensayo).

2. Aprobación y autorización:

- Los cambios con un impacto sustancial en la seguridad de la información y en las funcionalidades operativas, deben obtener una autorización formal antes de desplegarse.
- Los cambios de emergencia pueden acelerarse, pero deben someterse a una revisión y autorización retrospectivas.

3. Procedimientos de gestión de cambios:

- Planificación y evaluación del impacto: evalúe los impactos potenciales de los cambios teniendo en cuenta las dependencias del sistema.
- Autorización: asegure las aprobaciones necesarias antes de iniciar los cambios. Comunicación: informe con anticipación a las partes interesadas internas y externas pertinentes sobre los cambios previstos, los calendarios y el impacto esperado.
- Pruebas y control de calidad: asegúrese de que los cambios se prueban a fondo (consulte la sección 8.29 para conocer los detalles de las pruebas y la aceptación) y cumplen los estándares de calidad antes de implementarlos.
- Implementación y despliegue: ejecute los cambios de acuerdo con el calendario de despliegue previsto.
- Gestión de emergencias: Remediación: si los cambios fallan o presentan problemas inesperados, se revertirán.
- Mantenimiento de la documentación:Asegúrese de que los sistemas de tickets o la plataforma de repositorio de código mantienen un registro de los cambios, compromisos y despliegues.

4. Continuidad y coherencia:

- Asegúrese de que los planes de continuidad de las TIC y los procedimientos de respuesta y recuperación se actualizan para que sigan siendo adecuados y coherentes con los cambios realizados.

- Asegúrese de que la documentación operativa y los procedimientos de usuario se modifican y siguen siendo adecuados.

5. Seguridad e integridad:

- Garantice que los cambios preservan y no comprometen la confidencialidad, integridad y disponibilidad de la información en las instalaciones y sistemas de procesamiento.

Gestión de la capacidad

El uso de recursos de procesamiento y almacenamiento del sistema se supervisará y ajustará para garantizar que la disponibilidad y el rendimiento del sistema cumplan con los requisitos de D3M3NT SA DE CV.

Las habilidades, la disponibilidad y la capacidad de los recursos humanos se revisarán y se tendrán en cuenta como un componente de la planificación de la capacidad y como parte del proceso anual de evaluación de riesgos.

El escalamiento de recursos para lograr una capacidad adicional de procesamiento o almacenamiento, sin cambios en el sistema, se puede realizar fuera del proceso estándar de administración de cambios e implementación de código.

Prevención de fugas de datos

En cumplimiento de esta Política de prevención de fugas de datos, y con el fin de minimizar el riesgo de fugas de información confidencial, la organización deberá:

- Identificar y clasificar la información de acuerdo con la Política de gestión de datos
- Proporcionar capacitación de concientización a los usuarios, incluyendo el uso y manejo apropiados de la información confidencial.

Considerar el uso de herramientas técnicas de monitorización y Prevención de pérdidas de datos (DLP, por sus siglas en inglés) de acuerdo con los riesgos para la organización y los sujetos de los datos.

Filtrado web

La organización garantizará un uso seguro, protegido y adecuado de Internet por parte del personal de la organización.

Acceso y bloqueo de sitios web:

- Implemente mecanismos, como DNS seguro y bloqueo de direcciones IP o dominios, para restringir el acceso a sitios web que supongan un riesgo sustancial debido a su contenido o a la distribución conocida de malware, virus o material de phishing.
- Emplee navegadores y tecnologías antimalware capaces de bloquear automáticamente los sitios web o configurados para ello.
- A menos que esté justificado por razones empresariales legítimas, considere la posibilidad de bloquear el acceso a sitios web con:

1. Capacidades de carga de información.
2. Contenido malicioso conocido o sospechoso.
3. Actuar como servidores de mando y control.
4. Identificados como maliciosos mediante inteligencia de amenazas.
5. Compartir contenido ilegal.

Reglas y pautas de uso:

- El usuario deberá cumplir todas las reglas de la empresa de acuerdo con el Código de conducta y la Política de uso aceptable que se encuentra en la Política de seguridad de la información.

Separación de entornos de desarrollo, ensayo y producción

Los entornos de desarrollo y ensayo se separarán estrictamente de los entornos SaaS de producción para reducir los riesgos de acceso no autorizado o de cambios en el entorno operativo. Los datos confidenciales de los clientes de producción no deben utilizarse en entornos de desarrollo o prueba sin la aprobación expresa del Oficial de cumplimiento.

Consulte la Política de Gestión de Datos para obtener una descripción de los datos confidenciales. Si se aprueba el uso de los datos de los clientes de producción durante el desarrollo o las pruebas, se eliminará toda información confidencial que contenga cuando sea factible.

Configuración, endurecimiento y revisión de sistemas y redes

Los sistemas y redes se aprovisionarán y mantendrán de acuerdo con los estándares de configuración y refuerzo descritos en el Apéndice A de esta política.

Los *firewalls* o los controles y configuraciones de acceso a la red adecuados se utilizarán para controlar el tráfico de la red hacia el entorno de producción y de conformidad con esta política.

Las reglas de configuración del acceso a la red de producción se revisarán, al menos, una vez al año. Los *tickets* se crearán para obtener aprobaciones para cualquier cambio que sea necesario.

Protección contra *malware*

Para proteger la infraestructura de la empresa contra la introducción de *software* malicioso, se implementarán controles de detección, prevención y recuperación para protegerse contra *malware*, junto con el conocimiento adecuado del usuario.

Las protecciones antimalware se utilizarán en todos los puntos de conexión emitidos por la empresa, a excepción de aquellos que ejecutan sistemas operativos que normalmente no son propensos a software malicioso. Además, se utilizará software de detección de amenazas y respuesta para el correo electrónico de la empresa. Las protecciones antimalware utilizadas serán capaces de detectar todas las formas comunes de amenazas maliciosas y realizar la actividad de mitigación adecuada (como eliminar, bloquear o poner en cuarentena).

D3M3NT SA DE CV debe escanear todos los archivos cuando se introducen en los sistemas, y escanear continuamente los archivos cuando se accede a ellos, se modifican o se descargan. Las actualizaciones de las definiciones y motores *antimalware* y deben configurarse para que se descarguen e instalen automáticamente siempre que haya nuevas actualizaciones disponibles. Los incidentes de *malware* conocidos o sospechosos deben reportarse como un incidente de seguridad.

Es una infracción de la política de la empresa desactivar o alterar la configuración de las protecciones *antimalware* sin autorización.

Copia de seguridad de la información

Se considerará la necesidad de realizar copias de seguridad de sistemas, bases de datos, información y datos, y se diseñarán, planificarán e implementarán los procesos de copia de seguridad adecuados. Los procedimientos de copia de seguridad deben incluir procedimientos para mantener y recuperar los datos de los clientes de conformidad con los SLA documentados. Las medidas de seguridad para proteger las copias de seguridad se diseñarán y aplicarán en función de la confidencialidad de los datos. Se tomarán copias de seguridad de la información, el *software* y

las imágenes del sistema regularmente para protegerse contra la pérdida de datos. Las copias de seguridad y las capacidades de restauración se probarán periódicamente, al menos, una vez por año.

D3M3NT SA DE CV no realiza copias de seguridad regulares de los dispositivos de los usuarios, como las computadoras portátiles. Se espera que los usuarios almacenen archivos e información críticos en depósitos de almacenamiento de archivos autorizados por la empresa.

Las copias de seguridad se configuran para ejecutarse diario en los sistemas dentro del alcance. Los programas de copia de seguridad se mantienen dentro del *software* de la aplicación de copia de seguridad.

Se debe realizar una prueba de restauración de copia de seguridad, al menos, una vez al año para validar los datos de copia de seguridad y el proceso de copia de seguridad.

Registro y monitoreo

La infraestructura de producción se configurará para producir registros detallados de acuerdo a la función que desempeña el sistema o dispositivo. Los registros de eventos que registren actividades del usuario, excepciones, fallas y eventos de seguridad de la información se producirán, guardarán y revisarán a través de procesos manuales o automatizados según sea necesario. Se configurarán alertas correspondientes para los eventos que representen una amenaza significativa para la confidencialidad, disponibilidad o integridad de los sistemas de producción o datos confidenciales.

El registro debe cumplir con los siguientes criterios para aplicaciones de producción e infraestructura de soporte:

- Inicio y cierre de sesión del usuario
- Registrar operaciones CRUD (crear, leer, actualizar, eliminar) en usuarios y objetos de aplicaciones y sistemas
- Cambios en la configuración de seguridad del registro (incluido deshabilitar o modificar el registro)
- Registrar el acceso del propietario o administrador de la aplicación a los datos del cliente (es decir, la transparencia de acceso)
- Los registros deben incluir ID de usuario, dirección IP, marca de tiempo válida, tipo de acción realizada y objeto de esta acción.
- Los registros deben almacenarse durante, al menos, 30 días y no deben contener datos confidenciales ni cargas útiles.

Protección de la información de registro

El centro de registros y la información de registro estarán protegidos contra alteraciones y accesos no autorizados.

Registros de administradores y operadores

Las actividades del administrador y operador del sistema se registrarán, revisarán o avisarán de acuerdo con la clasificación y la importancia para el sistema.

Registros de restauración de datos

En caso de que la empresa necesite restaurar los datos de producción que contengan información de identificación personal de las copias de seguridad, ya sea con el fin de prestar servicios o con fines de prueba, se registrará o se realizará un seguimiento en *tickets* auditables.

Sincronización de reloj

Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad se sincronizarán con servidores de tiempo de red mediante fuentes de tiempo confiables.

Monitoreo de la integridad de archivos y detección de intrusiones

Los sistemas de producción de D3M3NT SA DE CV estarán configurados para supervisar, registrar y autorreparar o alertar sobre cambios sospechosos en los archivos críticos del sistema cuando sea posible.

Las alertas se configurarán para detectar condiciones sospechosas y los ingenieros revisarán los registros de forma regular.

Las intrusiones no autorizadas y los intentos de acceso o cambios en los sistemas de D3M3NT SA DE CV se investigarán y repararán de acuerdo con el Plan de Respuesta ante Incidentes.

Control del *software* operativo

La instalación de *software* en los sistemas de producción deberá cumplir con los requisitos de gestión de cambios definidos en esta política.

Inteligencia de amenazas

La información relativa a las amenazas para la seguridad de la información debe recopilarse y analizarse para producir inteligencia sobre amenazas.

Recopilación: recurra a diversas fuentes, como blogs, artículos de noticias, actualizaciones de proveedores, bases de datos públicas y comunidades del sector.

Análisis: examine los datos para obtener perspectivas procesables y permitir iniciativas de respuesta proactivas.Informe sobre cualquier idea procesable o amenaza específica al equipo de seguridad.

Difusión: garantice la comunicación eficaz de la inteligencia sobre amenazas a los equipos pertinentes para que tomen medidas efectivas.El equipo de seguridad difundirá la información procesable a través de canales de comunicación como Slack, correo electrónico y alertas de emergencia.

Comentarios: cultive la mejora continua aprovechando los comentarios para mejorar las políticas.Integre los comentarios en las modificaciones de las políticas y realice revisiones periódicas de las mismas.

Gestión técnica de vulnerabilidades

La información sobre las vulnerabilidades técnicas de los sistemas de información que se utilizan se obtendrá de manera oportuna, se evaluará la exposición de la organización a dichas vulnerabilidades y se tomarán las medidas apropiadas para abordar el riesgo asociado. Se utilizará una variedad de métodos para obtener información sobre vulnerabilidades técnicas, incluido análisis de vulnerabilidades, pruebas de penetración, revisión de alertas de proveedores externos y el programa de recompensas por errores.

Los análisis de vulnerabilidad se realizarán en sistemas públicos en el entorno de producción, al menos, trimestralmente.

Las pruebas de penetración de las aplicaciones y de la red de producción se realizarán, al menos, una vez al año. Se realizarán análisis y pruebas adicionales después de cambios importantes en los sistemas y *software* de producción.

Los departamentos de TI e Ingeniería evaluarán la gravedad de las vulnerabilidades identificadas de cualquier fuente y, si se determina que es una vulnerabilidad crítica relevante para el riesgo o de alto riesgo, se creará un *ticket* de servicio. El nivel de gravedad evaluado por D3M3NT SA DE CV puede diferir del nivel generado automáticamente por el *software* de escaneo o determinado por investigadores externos en función del conocimiento interno y la comprensión de D3M3NT SA DE CV de la arquitectura técnica y el impacto/explotabilidad en el mundo real. Los *tickets* se asignan a los propietarios del sistema, la aplicación o la plataforma para una mayor investigación o corrección.

Las vulnerabilidades evaluadas por D3M3NT SA DE CV se parchearán o remediarán en los siguientes plazos:

Gravedad determinada	Tiempo de reparación
Crítico	30 días
Alto	30 días
Medio	60 días
Bajo	90 días
Informativo	Según sea necesario

Los *tickets* de servicio para cualquier vulnerabilidad que no se pueda solucionar dentro del cronograma estándar deben mostrar un plan de tratamiento de riesgos y un cronograma de reparación planificado.

Restricciones en la instalación de software

Las reglas que rigen la instalación de *software* por parte de los usuarios se establecerán e implementarán de acuerdo con la Política de Seguridad de la Información de D3M3NT SA DE CV.

Consideraciones de auditoría de los sistemas de información

Los requisitos de auditoría y las actividades que impliquen la verificación de los sistemas operativos se planificarán y acordarán cuidadosamente para minimizar las interrupciones de los procesos empresariales.

Evaluación y requisitos de seguridad de los sistemas

Los riesgos se considerarán antes de la adquisición o cambios significativos en los sistemas, las tecnologías o las instalaciones. Cuando se identifiquen formalmente los requisitos, se incluirán los requisitos de seguridad pertinentes. La adquisición de nuevos proveedores y servicios se realizará de conformidad con la Política de Gestión de Terceros.

La empresa realizará una evaluación anual de la seguridad de la red que incluye una revisión de los cambios importantes en el entorno, como los nuevos componentes del sistema y la topología de la red.

Enmascaramiento de datos

D3M3NT SA DE CV implementará el enmascaramiento de datos en función del riesgo o de un requisito específico para hacerlo.

Guía de técnicas:

- Adopte técnicas apropiadas, como el enmascaramiento de datos, la seudonimización o la anonimización para proteger eficazmente la PII y otros datos confidenciales.

- Garantice que los métodos de seudonimización y anonimización rompen eficazmente el vínculo entre la PII y los individuos o elementos de datos confidenciales.
- Confirme que se tienen en cuenta todos los elementos de la información para una adecuada anonimización de los datos.
- Emplee métodos adicionales de enmascaramiento de datos, como la codificación, la anulación/eliminación de caracteres, la variación de números y fechas, la sustitución y el reemplazo de valores por sus hashes.

Consideraciones sobre el enmascaramiento de datos:

- Diseñe consultas y máscaras de datos para revelar solo los datos mínimamente necesarios a los usuarios, salvaguardando la privacidad y la seguridad.
- Desarrolle mecanismos para el enmascaramiento de datos, teniendo en cuenta las circunstancias específicas en las que ciertos datos deben ocultarse a los usuarios.
- Brinde opciones para que los responsables de la PII controlen la visibilidad de sus datos enmascarados y se adhieran a cualquier requisito legal o reglamentario aplicable relacionado con el enmascaramiento de datos.

Uso del enmascaramiento de datos, la seudonimización o la anonimización:

- Determine el nivel de seguridad, los controles de acceso, los acuerdos de usuario y las restricciones de uso adecuados para los datos procesados.
- Impida la combinación de los datos procesados con otra información para identificar a las principales PII y garantice la trazabilidad de los datos procesados proporcionados y recibidos.

Excepciones

Las solicitudes de excepción a esta política deben enviarse al gerente de TI para su aprobación.

Infracciones y cumplimiento

Cualquier infracción conocida de esta política debe ser reportada al gerente de TI. Las infracciones de esta política pueden dar lugar a la retirada o suspensión inmediata de los privilegios del sistema y la red o medidas disciplinarias de acuerdo con los procedimientos de la empresa, incluido el despido.

Versión	Fecha	Descripción	Autor	Aprobado por
1.1	09/04/2024	Ajuste por traducción	Víctor Acosta	Marco Villanueva

APÉNDICE A - Estándares de configuración y endurecimiento

Los estándares de configuración y endurecimiento se mantendrán en el portal de documentación interna.

intra.dmente.mx/recursos

Incluya enlaces a fuentes externas o muestras creadas internamente:

https://aws.amazon.com/compliance/resources/

https://www.mongodb.com/products/platform/trust

https://www.make.com/en/security

Aborde la gestión e implementación de la configuración de referencia según el control 3.4, 7.1.

Servidores y máquinas virtuales

Este es el estándar para el fortalecimiento de la configuración del servidor a nivel de sistema y del servidor virtual (VM). Es posible que se requiera alguna personalización de esta configuración para configurar el sistema para su entorno de destino específico, como establecer los nombres, los grupos, la configuración de autenticación y otras opciones de personalización adecuados.

UBUNTU LTS / AWS INSTANCE

Además de los requisitos para asegurar los sistemas a la línea base descrita anteriormente, todos los sistemas físicos y virtuales deben cumplir con los siguientes requisitos técnicos:

- Todas las contraseñas predeterminadas del proveedor (incluyendo las contraseñas predeterminadas de los sistemas operativos, el software que proporciona servicios de seguridad, las cuentas de aplicaciones y sistemas, las cadenas de comunidad del Protocolo simple de gestión de redes deben cambiarse antes de instalar un sistema en la red.
- Las cuentas predeterminadas innecesarias (incluidas las cuentas utilizadas por sistemas operativos, *software* de seguridad, aplicaciones, sistemas, SNMP, entre otros) deben eliminarse o deshabilitarse antes de instalar un sistema en la red.
- Solo se puede implementar una función principal por servidor o máquina virtual para evitar que las funciones que requieren diferentes niveles de seguridad coexistan en el mismo sistema.
- Solo se pueden habilitar los servicios, protocolos, daemons, entre otros, necesarios, y solo según sea necesario para la función del sistema. Todas las funciones innecesarias (como *scripts*, controladores, características, subsistemas, sistemas de archivos y servidores web innecesarios) deben estar deshabilitadas.
- Todos los parches de seguridad identificados como críticos deben aplicarse a los sistemas dentro de los SLA establecidos en esta política.

Estándares de red

- La administración de las reglas y configuraciones de la red solo la pueden realizar los miembros autorizados del equipo de TI y todos los cambios deben cumplir con los procedimientos de administración definidos en la Política de Seguridad Operativa.
- Los controles de red compatibles para las redes de producción son AWS NACL. La administración de los sistemas de red de producción se realiza mediante el uso de SISTEMA DE ADMINISTRACIÓN, SSH, ENTRE OTROS
- En el ENTORNO DE PRODUCCIÓN, deben aplicarse las reglas y configuraciones definidas para controlar el tráfico desde redes que no sean de confianza (por ejemplo,servicios disponibles públicamente) a las redes de producción internas.
- Los sistemas de control de red deben configurarse para utilizar la traducción de direcciones de red predeterminada para evitar la divulgación de direcciones IP internas a Internet.
- Los dispositivos móviles que se conecten a las redes de producción deben cumplir los requisitos de la Política para dispositivos móviles que se encuentra en la Política de seguridad de la información.
- Todos los sistemas de control de red deben configurarse con reglas de *antispoofing* predeterminadas para bloquear o rechazar direcciones internas entrantes originadas en Internet.

- Las configuraciones externas deben limitar el tráfico entrante solo a los componentes del sistema que proporcionan servicios, protocolos y puertos autorizados de acceso público.
- Está prohibido el uso de servicios y protocolos no seguros sin justificación y documentación de características de seguridad adicionales implementadas para mitigar el riesgo.
- Las sesiones de acceso remoto deben configurarse para que se aplique el tiempo de espera después de un periodo especificado de 12 horas
- Las tecnologías de acceso remoto para proveedores y socios comerciales utilizadas para acceder a los sistemas de producción deben habilitarse solo cuando sea necesario para fines comerciales y desactivarse inmediatamente después de su uso.
- Todas las redes híbridas con acceso tanto a la nube como a las instalaciones se escanearán y probarán, al menos, una vez al año para garantizar que se mantengan los requisitos de seguridad.

I. Endurecimiento de la nube

1. Gestión de identidades y accesos (IAM, por sus siglas en inglés)

- Principio del mínimo privilegio: asegúrese de que cada entidad (usuario, servicio, sistema) posee el acceso mínimo necesario.
- Imponga la autenticación multifactor (MFA, por sus siglas en inglés) para el acceso de producción.

2. Gestión y almacenamiento de datos

- Cifrado de datos: garantice el cifrado de datos en reposo y en tránsito de acuerdo con la *Política de cifrado*
- Gestión del ciclo de vida de los datos: configure copias de seguridad para los repositorios de datos de los clientes.

3. Seguridad de la red

- Aislamiento: utilice VPC y subredes para aislar entornos y segmentar redes.
- Firewalls: implemente soluciones de firewall nativas de la nube o de terceros y servicios de protección DDoS.

4. Monitoreo y registro

- Registro: configure el registro enfocándose en el almacenamiento de escritura única y lectura múltiple para evitar la manipulación.
- Alertas: implemente alertas basadas en la nube (Amazon CloudWatch, Azure Alerts) para responder a incidentes en tiempo real.

II. Endurecimiento de contenedores

1. Seguridad de imágenes

- Imagen de fuente segura: cree imágenes solo a partir de imágenes base o repositorios autorizados porD3M3NT SA DE CV.
- Diseño minimalista: adopte imágenes base mínimas para reducir los vectores de ataque.

2. Seguridad en tiempo de ejecución

Análisis en tiempo de ejecución: implemente herramientas de seguridad en tiempo de ejecución para la detección en vivo de vulnerabilidades y amenazas.

3. Seguridad de la red

Controles basados en políticas: implemente políticas de red utilizando herramientas de terceros o nativas de la nube.

4. Seguridad de orquestación

- Servidor API: blinde el servidor API con firewalls adecuados, controles IAM y canales de comunicación seguros.
- RBAC: establezca y revise periódicamente los privilegios de acceso a la orquestación, garantizando la conformidad con el principio de mínimo privilegio.

5. Seguridad de CI/CD

Acceso al pipeline: minimice el acceso a los pipelines de CI/CD, empleando controles de acceso basados en funciones y registros de auditoría.

- Análisis de dependencias: analice las dependencias vulnerables durante los procesos de creación.

III. Servidores y máquinas virtuales

Configuración de la línea de base

- Asegúrese de que los sistemas están alineados con las líneas de base estándar del sector (puntos de referencia del CIS, pautas del NIST).

Adherencia técnica

- Valores predeterminados del proveedor: todas las configuraciones predeterminadas, especialmente las contraseñas, deben alterarse antes de la integración en la red.
- Especialización de funciones: mantenga una función principal singular por VM para mantener la segregación de funciones y reducir las oportunidades de movimiento lateral.
- Gestión de parches: establezca una estrategia de gestión de parches para cumplir los SLA definidos.

IV. Estándares de red

Gestión y documentación de la red

- Gestión de cambios: cualquier alteración de la configuración de la red debe adherirse a los procesos de gestión de cambios.

Gestión del tráfico en entornos de producción

- Aplicación de reglas: aplique estrictamente las reglas predefinidas, que deben revisarse y validarse al menos una vez al año.
- Control del acceso remoto: garantice un control y una auditoría estrictos del acceso remoto, restringiendo y registrando todas las conexiones.

NACL y control del tráfico

- Establezca reglas estrictas que regulen el tráfico de acuerdo con una justificación empresarial definida.