



POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Empresa: Speed Net Courier S.A.S.

Código: PSI-002-2026

Versión: 2.0

Fecha de aprobación: 21/08/2026

Fecha de vigencia: 22/08/2028

Responsable: Área de Sistemas / Dirección Administrativa y Operativa

Periodicidad de revisión: Mínimo cada dos (2) años o cuando se presenten cambios relevantes

1. OBJETIVO

Establecer los lineamientos, responsabilidades y controles para proteger la información de Speed Net Courier S.A.S. frente a accesos, usos, modificaciones, divulgaciones, pérdidas, destrucción o indisponibilidad no autorizada

La política busca preservar:

1.1 Confidencialidad: garantizar que la información sea conocida únicamente por personas autorizadas

1.2 Integridad: garantizar que la información permanezca completa, exacta y protegida contra modificaciones no autorizadas

1.3 Disponibilidad: garantizar que la información y los sistemas estén disponibles para los usuarios autorizados cuando sean requeridos

1.4 Trazabilidad: permitir, cuando técnicamente sea posible, identificar las actividades realizadas sobre los sistemas y la información

2. ALCANCE

Esta política aplica a:

2.1 Todos los funcionarios de Speed Net Courier S.A.S.

2.2 Contratistas.

2.3 Proveedores.

2.4 Terceros autorizados.

2.5 Practicantes.

2.6 Personal temporal.

2.7 Administradores de sistemas.

Cualquier persona que tenga acceso a información o recursos tecnológicos de la compañía

Aplica a:

2.8 Computadores y servidores



- 2.9 Redes corporativas
- 2.10 Sistemas de información
- 2.11 Aplicativo Sis Postal
- 2.12 Bases de datos
- 2.13 Correo electrónico
- 2.14 Servicios en la nube
- 2.15 Dispositivos móviles corporativos y Dispositivos de almacenamiento.
- 2.16 Información física y digital.
- 2.17 Copias de seguridad.
- 2.18 Información de clientes, empleados, proveedores y terceros.

3. PRINCIPIOS DE SEGURIDAD

Speed Net Courier S.A.S. establece los siguientes principios:

3.1 Mínimo privilegio

Cada usuario tendrá únicamente los permisos necesarios para realizar sus funciones

3.2 Necesidad de conocer

El acceso a información estará limitado a las personas que requieran dicha información para cumplir sus responsabilidades

3.3 Responsabilidad individual

Cada usuario será responsable de las actividades realizadas utilizando sus credenciales

3.4 Defensa en profundidad

La seguridad deberá implementarse mediante diferentes controles administrativos, técnicos y humanos, evitando depender de una única medida de protección

3.5 Gestión basada en riesgos

Los controles de seguridad deberán priorizarse teniendo en cuenta la probabilidad e impacto de los riesgos identificados

3.6 Mejora continua

Los controles deberán revisarse y actualizarse considerando cambios tecnológicos, nuevos riesgos, incidentes y necesidades del negocio



4. RESPONSABILIDADES

4.1 Dirección Administrativa y Operativa

La Dirección Administrativa y Operativa deberá:

- Aprobar la presente política
- Asignar responsabilidades
- Facilitar los recursos necesarios para implementar controles de seguridad
- Revisar los riesgos relevantes
- Apoyar la gestión de incidentes
- Promover una cultura de seguridad de la información

4.2 Área de Sistemas

El Área de Sistemas será responsable de:

- Administrar los sistemas y recursos tecnológicos
- Crear, modificar y deshabilitar usuarios
- Administrar privilegios
- Mantener actualizados los sistemas
- Administrar respaldos
- Supervisar controles de seguridad
- Gestionar incidentes tecnológicos
- Mantener registros y evidencias de los controles implementados
- Realizar revisiones periódicas de cuentas y accesos
- Informar riesgos relevantes a la Dirección

4.3 Funcionarios y terceros

Los funcionarios y terceros deberán:

- Cumplir esta política
- Proteger sus credenciales
- Utilizar únicamente los recursos autorizados
- Reportar incidentes o situaciones sospechosas
- Proteger la información bajo su responsabilidad
- Participar en las capacitaciones de seguridad establecidas

5. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN



Speed Net Courier S.A.S. deberá identificar y evaluar periódicamente los riesgos asociados con la información y los activos tecnológicos.

Como mínimo deberán considerarse:

- Accesos no autorizados
- Malware y ransomware
- Phishing
- Pérdida o robo de equipos
- Pérdida de información
- Fallas de hardware
- Fallas eléctricas – Fallas de Software
- Incendios, inundaciones u otros eventos físicos
- Errores humanos
- Divulgación de información
- Vulnerabilidades de sistemas
- Riesgos relacionados con proveedores y terceros

Los riesgos identificados deberán registrarse y, cuando corresponda, contar con:

- Responsable
- Nivel de riesgo
- Control asociado
- Acción de tratamiento
- Fecha objetivo
- Estado

6. GESTIÓN DE ACTIVOS

Speed Net Courier S.A.S. deberá mantener un inventario actualizado de los principales activos tecnológicos

El inventario deberá incluir, cuando corresponda:

- Equipos de cómputo
- Servidores
- Equipos de red
- Dispositivos móviles corporativos
- Sistemas y aplicaciones
- Bases de datos
- Servicios tecnológicos
- Dispositivos de almacenamiento
- Licencias relevantes

Cada activo deberá tener un responsable o área responsable.



Cuando un activo sea retirado, vendido, reemplazado o dado de baja, deberá aplicarse un procedimiento que evite la exposición de información almacenada.

7. CONTROL DE ACCESO

7.1 Creación de usuarios

Cada funcionario deberá contar con una cuenta individual

Las cuentas serán creadas por el Área de Sistemas previa autorización correspondiente

No se permitirá compartir cuentas personales

7.2 Revisión de usuarios

El Área de Sistemas deberá mantener un inventario de:

- Usuarios estándar
- Usuarios administradores
- Cuentas de servicio
- Cuentas especiales
- Cuentas temporales

Las cuentas deberán revisarse como mínimo trimestralmente para verificar que continúen autorizadas

7.3 Cuentas administrativas

Las cuentas administrativas deberán utilizarse únicamente para actividades que requieran privilegios elevados

Cuando sea técnicamente posible, los administradores deberán disponer de:

- Una cuenta estándar para actividades cotidianas
- Una cuenta administrativa separada para tareas administrativas

No deberá utilizarse una cuenta administrativa para navegación, correo electrónico u otras actividades rutinarias cuando pueda evitarse

7.4 Cuentas de servicio

Las cuentas utilizadas por aplicaciones, bases de datos, respaldos u otros servicios deberán:

- Estar identificadas



Tener un responsable
Tener únicamente los permisos necesarios
No utilizarse para actividades interactivas de usuarios
Ser revisadas periódicamente

8. POLÍTICA DE CONTRASEÑAS Y AUTENTICACIÓN

8.1 Requisitos

Las contraseñas deberán:

Tener una longitud mínima de ocho (8) caracteres cuando el sistema no permita una política superior
Ser preferiblemente de mayor longitud, especialmente para cuentas críticas
Ser únicas para cada servicio
No contener información personal fácilmente identificable
No corresponder a contraseñas conocidas, comunes o comprometidas
No ser compartidas
No almacenarse en documentos, correos, notas visibles o archivos no autorizados

8.2 Autenticación multifactor

Speed Net deberá implementar progresivamente autenticación multifactor (MFA) en:

1. Cuentas administrativas
2. Correo corporativo
3. Acceso remoto
4. Sistemas críticos
5. Servicios que almacenen información sensible
6. Plataformas en la nube que soporten MFA

El MFA deberá priorizarse especialmente para cuentas con privilegios elevados

8.3 Bloqueo

Los sistemas deberán implementar mecanismos de protección frente a intentos repetidos de autenticación fallida

Cuando una cuenta sea bloqueada, el restablecimiento deberá realizarse mediante un procedimiento que permita verificar la identidad del solicitante

8.4 Restablecimiento

El Área de Sistemas no deberá solicitar al usuario que revele su contraseña actual



El restablecimiento deberá realizarse mediante mecanismos seguros y verificando previamente la identidad del solicitante

9. BLOQUEO DE EQUIPOS

Todos los equipos deberán configurarse para bloquear automáticamente la sesión después de un máximo de cinco (5) minutos de inactividad, cuando la configuración técnica lo permita

Los usuarios deberán bloquear manualmente sus equipos cuando se retiren de su puesto de trabajo

10. SEGURIDAD DE EQUIPOS

Los equipos corporativos deberán contar, cuando corresponda, con:

- Sistema operativo soportado
- Actualizaciones de seguridad
- Antivirus o antimalware
- Firewall
- Windows Defender activo en equipos Windows
- Bloqueo automático
- Usuarios sin privilegios administrativos innecesarios
- Herramientas de protección disponibles para la infraestructura

Los usuarios no podrán desactivar los mecanismos de protección instalados por la compañía

11. ACTUALIZACIONES Y VULNERABILIDADES

El Área de Sistemas deberá mantener los sistemas operativos, aplicaciones y herramientas de seguridad actualizados

Las vulnerabilidades críticas deberán priorizarse según el riesgo que representen para la compañía

Cuando una actualización no pueda realizarse oportunamente por razones técnicas, deberá evaluarse la implementación de controles compensatorios

12. SEGURIDAD DE RED



La red corporativa deberá contar con controles destinados a impedir accesos no autorizados

Se deberán mantener, como mínimo cuando la infraestructura lo permita:

12.1 Red corporativa

Para equipos y dispositivos autorizados de Speed Net

12.2 Red de invitados

Para visitantes y dispositivos externos

La red de invitados deberá estar aislada de los recursos internos de la compañía

Los dispositivos personales no deberán conectarse a la red corporativa salvo autorización expresa

13. FIREWALL Y NAVEGACIÓN

Speed Net deberá mantener mecanismos de firewall adecuados para proteger la red y los equipos.

El acceso a Internet podrá estar restringido de acuerdo con:

- Riesgo de seguridad
- Necesidades operativas
- Consumo de recursos
- Políticas internas
- Requisitos legales

Las restricciones deberán revisarse periódicamente para evitar bloqueos innecesarios de servicios requeridos para la operación

14. CORREO ELECTRÓNICO Y PHISHING

Los funcionarios deberán considerar sospechosos los mensajes que:

- Soliciten contraseñas
- Soliciten transferencias o pagos inusuales
- Contengan enlaces sospechosos
- Soliciten información confidencial



Presenten archivos adjuntos inesperados
Simulen provenir de entidades o personas conocidas

Los usuarios deberán reportar mensajes sospechosos al Área de Sistemas

No se deberán introducir credenciales corporativas en sitios web desconocidos

15. DISPOSITIVOS DE ALMACENAMIENTO

El uso de:

Memorias USB

Discos externos

CD/DVD/Blu-ray

Otros dispositivos de almacenamiento externo deberán estar controlado, Cuando sea necesario utilizarlos, deberán ser revisados mediante herramientas de seguridad disponibles y utilizarse únicamente para fines laborales autorizados

La información confidencial no deberá copiarse a dispositivos personales sin autorización

16. PROTECCIÓN DE DATOS PERSONALES

Speed Net Courier S.A.S. deberá implementar medidas técnicas, humanas y administrativas para proteger los datos personales tratados por la compañía

El tratamiento de datos personales deberá realizarse de acuerdo con la normativa colombiana aplicable, incluyendo la Ley 1581 de 2012 y sus normas reglamentarias

Los datos personales deberán protegerse contra:

Pérdida

Adulteración

Acceso no autorizado

Uso no autorizado

Consulta no autorizada

Divulgación indebida

La obligación de confidencialidad respecto de datos personales deberá mantenerse incluso después de finalizar la relación laboral o contractual cuando



corresponda. La SIC reconoce expresamente los principios de seguridad y confidencialidad en el tratamiento de datos personales

Speed Net deberá mantener una política de tratamiento de datos personales independiente y complementario a esta política de seguridad de la información

17. CLASIFICACIÓN DE LA INFORMACIÓN

La información podrá clasificarse de acuerdo con su nivel de sensibilidad:

17.1 Pública

Información autorizada para divulgación pública

17.2 Interna

Información destinada al uso interno de Speed Net

17.3 Confidencial

Información cuyo acceso debe limitarse a personas autorizadas

17.4 Restringida

Información altamente sensible cuyo acceso requiere controles especiales

Los documentos que contengan información confidencial o restringida deberán manejarse mediante mecanismos apropiados de protección

18. MANEJO DE INFORMACIÓN

Los funcionarios deberán:

Los datos personales deberán protegerse contra:

Pérdida

Adulteración

Acceso no autorizado

Uso no autorizado

Consulta no autorizada

Divulgación indebida

Evitar dejar documentos confidenciales expuestos

No enviar información confidencial a cuentas personales

No utilizar servicios personales de almacenamiento para información corporativa

No compartir información con terceros sin autorización

Verificar destinatarios antes de enviar información sensible



Eliminar información de forma segura cuando ya no sea necesaria y exista autorización para su eliminación

19. COPIAS DE SEGURIDAD

Las copias de seguridad deberán permitir recuperar la información crítica ante incidentes que afecten su disponibilidad o integridad

El proceso de recuperación deberá contemplar planificación, ejecución, pruebas y recuperación de información de los activos a un estado confiable previo al incidente

19.1 Base de datos Sis Postal

Se realizarán respaldos mediante tareas programadas:

Todos los días – cada 6 horas

Archivo:

Bk_Correo.BAK

Automático Microsoft

19.2 Documentos de usuarios

Se deberán realizar respaldos de la información laboral almacenada en los equipos de los usuarios, de acuerdo con las capacidades técnicas de la infraestructura

19.3 Carpeta pública

La información almacenada en la carpeta pública del servidor deberá incluirse dentro del esquema de respaldo

19.4 Protección de los backups

Cuando técnicamente sea posible, deberá existir:

Una copia principal

Una copia independiente del sistema original

Una copia ubicada en una ubicación diferente

Una copia aislada o protegida contra modificación/eliminación no autorizada para información crítica



20. PRUEBAS DE RESTAURACIÓN

El Área de Sistemas deberá realizar pruebas periódicas de restauración

Como mínimo:

Verificación de ejecución de backups: mensual

Prueba de restauración de información crítica: mínimo anual

Prueba extraordinaria después de un incidente grave

21. GESTIÓN DE INCIDENTES

Todo incidente o sospecha de incidente deberá reportarse inmediatamente

Se consideran incidentes:

Malware

Ransomware

Phishing

Acceso no autorizado

Pérdida de información

Divulgación accidental

Compromiso de contraseñas

Fallas de backups

Ataques contra sistemas

Pérdida de disponibilidad de servicios críticos

El Área de Sistemas deberá:

Identificar el incidente

Contenerlo

Evaluar su impacto

Recuperar los servicios afectados

Documentar las acciones realizadas

Identificar causas cuando sea posible

Implementar acciones correctivas

22. GESTIÓN DE TERCEROS Y PROVEEDORES

Los proveedores que tengan acceso a información de Speed Net deberán cumplir los requisitos de seguridad definidos por la compañía.

Cuando corresponda, los contratos deberán establecer:



Obligaciones de confidencialidad
Protección de datos personales
Control de acceso
Uso autorizado de información.
Notificación de incidentes
Devolución o eliminación de información al finalizar el servicio
Responsabilidades frente a seguridad

23. ACCESO REMOTO

El acceso remoto a recursos corporativos deberá realizarse únicamente mediante mecanismos autorizados

Cuando sea técnicamente posible deberá utilizarse:

MFA
Canales cifrados
Equipos administrados o autorizados
Controles de sesión
Registro de accesos

No se permitirá el acceso remoto mediante herramientas no autorizadas por el Área de Sistemas

24. TRABAJO REMOTO

Los funcionarios que trabajen fuera de las instalaciones deberán:

Proteger físicamente los equipos
Evitar conectarse a redes públicas inseguras cuando existan alternativas
Utilizar los mecanismos de acceso autorizados
Evitar que terceros visualicen información corporativa
No almacenar información corporativa en equipos personales sin autorización

25. CONCIENTIZACIÓN Y CAPACITACIÓN

Speed Net deberá realizar actividades de concientización sobre seguridad de la información.

Como mínimo deberán abordarse:

Contraseñas
MFA
Phishing



- Protección de datos personales
- Manejo de información confidencial
- Uso seguro del correo
- Reporte de incidentes
- Uso de dispositivos externos

26. INGRESO DE FUNCIONARIOS

Antes o durante el ingreso de un funcionario deberá:

- Autorizarse el acceso requerido
- Crear las cuentas necesarias
- Asignar los permisos según el cargo
- Entregar los activos tecnológicos correspondientes
- Realizar inducción en seguridad
- Suscribir las obligaciones de confidencialidad correspondientes

27. CAMBIO DE CARGO

Cuando un funcionario cambie de cargo:

- Se deberán revisar sus permisos
- Se eliminarán accesos innecesarios
- Se crearán los nuevos accesos requeridos
- Se actualizarán los activos bajo su responsabilidad

Los accesos anteriores no deberán mantenerse únicamente por comodidad.

28. RETIRO DE FUNCIONARIOS

Ante la terminación de la relación laboral o contractual:

- Se deberán deshabilitar las cuentas
- Revocar accesos
- Recuperar equipos
- Recuperar activos tecnológicos
- Transferir información laboral
- Revisar accesos compartidos
- Cambiar credenciales compartidas cuando corresponda
- Realizar los respaldos requeridos
- Registrar el cierre del acceso



El proceso deberá realizarse de manera coordinada entre Recursos Humanos, el responsable del área y Sistemas

29. MONITOREO Y REGISTROS

Inicios de sesión
Cambios de permisos
Actividades administrativas
Eventos de seguridad
Fallas de backups
Incidentes.
Accesos a sistemas críticos.

Los registros deberán protegerse contra modificaciones no autorizadas y conservarse durante el período definido por la compañía.

30. INDICADORES DE SEGURIDAD

La compañía podrá establecer indicadores para medir el desempeño de sus controles.

Como mínimo se recomienda medir:

Porcentaje de usuarios con MFA
Porcentaje de equipos actualizados
Porcentaje de equipos con antivirus activo
Porcentaje de backups ejecutados correctamente
Porcentaje de pruebas de restauración exitosas
Número de incidentes de seguridad
Tiempo promedio de atención de incidentes
Número de cuentas inactivas detectadas
Porcentaje de funcionarios capacitados
Porcentaje de revisiones de accesos realizadas

31. INCUMPLIMIENTO

El incumplimiento de esta política podrá generar acciones administrativas de acuerdo con:

Reglamento interno
Contratos laborales



Contratos con terceros
Procedimientos internos
Legislación aplicable

Cuando el incumplimiento represente un riesgo de seguridad, podrá procederse a la suspensión temporal de accesos mientras se realiza la investigación correspondiente.

32. EXCEPCIONES

Cualquier excepción a esta política deberá:

Estar debidamente justificada
Identificar el riesgo
Definir controles compensatorios cuando corresponda
Tener un responsable
Tener una fecha de vencimiento
Ser aprobada por la autoridad correspondiente

No deberán existir excepciones indefinidas

33. REVISIÓN Y ACTUALIZACIÓN

Esta política será revisada como mínimo cada dos (2) años.

También deberá revisarse cuando:

Se presenten cambios tecnológicos relevantes.
Se incorporen sistemas críticos.
Se presenten incidentes importantes.
Cambien los riesgos de seguridad.
Se modifique la legislación aplicable.
Se modifiquen los procesos del negocio.
Se identifiquen nuevos requisitos de clientes o contratos.
Se inicie un proceso de certificación o auditoría.

La versión aprobada deberá comunicarse a los funcionarios y terceros a quienes les sea aplicable.



34. APROBACIÓN

La presente política deberá ser aprobada por la Dirección de Speed Net Courier S.A.S.

Elaboró: ALEJANDRA LEGUIZAMO

A handwritten signature in black ink, with the name 'Alejandra Leguizamo' written below it and 'AM. CONSULTORIA' in small capital letters at the bottom.

Cargo: Contratista Externo

Revisó: LILIANA BERMUDEZ

A handwritten signature in black ink, with the name 'Liliana Bermudez' written below it.

Cargo: Sistemas

Aprobó: KARIN VEGA ROZO

A handwritten signature in black ink, with the name 'Karin Vega Roza' written below it.

Cargo: Gerente

Fecha: 24/08/02026

Versión: 2.0