# POLÍTICA DE SEGURIDAD DEL NEGOCIO

## Q MAS IT S. DE R.L. DE C.V.

**Código:** POL-MN-004
**Versión:** 4.0
**Fecha de emisión:** Enero 2026
**Elaboró:** Dirección General
**Revisión:** Anual
**Aprobó:** Dirección General

# 1. Objetivo

## 1.1 Objetivo General

La presente **Política de Seguridad del Negocio** tiene como finalidad establecer el marco de referencia, los principios y los lineamientos generales para proteger los activos físicos, tecnológicos, financieros e intangibles de **Q MAS IT S. de R.L. de C.V.**, garantizando la continuidad de sus operaciones, la protección de la información, la seguridad de sus colaboradores, clientes y proveedores, así como el cumplimiento de los requisitos legales, contractuales y normativos aplicables.

Como empresa dedicada a la **comercialización de soluciones tecnológicas, equipos de cómputo, software, infraestructura de TI, servicios de instalación, mantenimiento, soporte técnico y reparación de equipos en garantía**, Q MAS IT S. reconoce que la seguridad del negocio es un elemento estratégico para preservar la confianza de sus clientes, asegurar la disponibilidad de sus servicios y minimizar el impacto de eventos que puedan comprometer el desarrollo normal de sus actividades.

Esta política busca integrar la seguridad en todos los procesos de la organización, promoviendo una cultura organizacional basada en la prevención, la gestión de riesgos, la mejora continua y la responsabilidad compartida de todos los colaboradores.

---

## 1.2 Objetivos Específicos

Para cumplir con el objetivo general, la organización establece los siguientes objetivos específicos:

**a) Proteger los activos del negocio**

Implementar controles que garanticen la protección de todos los activos de la empresa, incluyendo:

- Equipos de cómputo.
- Servidores.
- Dispositivos móviles.
- Herramientas especializadas.
- Refacciones.
- Equipos de laboratorio.
- Vehículos.
- Información física y digital.
- Infraestructura tecnológica.
- Propiedad intelectual.
- Recursos financieros.

Estos activos deberán mantenerse protegidos contra robo, pérdida, daño, uso indebido, fraude o cualquier otra amenaza que afecte su disponibilidad o integridad.

---

**b) Garantizar la continuidad de las operaciones**

Establecer mecanismos que permitan a la organización continuar prestando sus servicios aun cuando se presenten eventos extraordinarios, tales como:

- Desastres naturales.
- Incendios.
- Inundaciones.
- Sismos.
- Fallas eléctricas.
- Interrupciones de Internet.
- Ataques cibernéticos.
- Robo de equipos.
- Indisponibilidad de proveedores.
- Emergencias sanitarias.

La empresa contará con planes de continuidad y recuperación que reduzcan los tiempos de interrupción y permitan restablecer las operaciones de manera eficiente.

---

**c) Proteger la información**

Garantizar que toda la información administrada por Q MAS IT S. sea protegida bajo los principios de:

- Confidencialidad.
- Integridad.
- Disponibilidad.

- Trazabilidad.
- Autenticidad.

Esto incluye información relacionada con:

- Clientes.
- Proyectos.
- Contratos.
- Cotizaciones.
- Bases de datos.
- Credenciales de acceso.
- Información financiera.
- Información técnica.
- Documentación de garantías.
- Información de proveedores.

---

**d) Reducir riesgos del negocio**

Identificar, evaluar y controlar los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos de la organización mediante un proceso continuo de gestión de riesgos.

---

**e) Cumplir los requisitos legales**

Garantizar el cumplimiento de todas las leyes, reglamentos, contratos, acuerdos de confidencialidad y demás obligaciones aplicables al giro de la empresa.

---

**f) Fortalecer la confianza de los clientes**

Mantener altos estándares de seguridad que permitan asegurar a los clientes que sus equipos, información y proyectos son administrados bajo controles adecuados.

---

**g) Promover una cultura de seguridad**

Fomentar entre todos los colaboradores una cultura basada en:

- Prevención.
- Responsabilidad.
- Honestidad.

- Confidencialidad.
- Reporte oportuno de incidentes.
- Cumplimiento de procedimientos.

La seguridad del negocio es responsabilidad de todo el personal, independientemente de su puesto.

---

**h) Mejorar continuamente**

Revisar periódicamente la eficacia de los controles de seguridad mediante auditorías, indicadores de desempeño, análisis de incidentes y revisiones por la dirección, implementando acciones correctivas y preventivas que fortalezcan el sistema de gestión.

---

### 1.3 Beneficios esperados

La correcta aplicación de esta política permitirá:

- Reducir pérdidas económicas derivadas de incidentes de seguridad.
- Incrementar la confianza de clientes y socios comerciales.
- Minimizar riesgos operativos.
- Fortalecer la reputación corporativa.
- Garantizar la continuidad del negocio.
- Mejorar la capacidad de respuesta ante emergencias.
- Cumplir con requisitos legales y contractuales.
- Incrementar la eficiencia operativa.
- Proteger la información estratégica de la organización.
- Favorecer el crecimiento sostenible de la empresa.

---

# 2. Alcance

## 2.1 Alcance General

La presente Política de Seguridad del Negocio es de **cumplimiento obligatorio** para todas las personas que, de manera directa o indirecta, desarrollen actividades relacionadas con **Q MAS IT S. de R.L. de C.V.**, independientemente de la ubicación física donde se ejecuten dichas actividades.

Esta política aplica a todas las operaciones de la empresa, incluyendo oficinas administrativas, almacenes, centros de servicio, talleres, sitios de instalación, instalaciones de clientes, vehículos

corporativos, plataformas digitales, infraestructura tecnológica y cualquier otro lugar donde se desarrollen actividades en representación de la organización.

---

## 2.2 Personal incluido

Esta política aplica a:

### Dirección General

Responsable de establecer los lineamientos estratégicos, asignar recursos y asegurar la implementación del Sistema de Seguridad del Negocio.

---

### Gerencias y Coordinaciones

Responsables de implementar esta política dentro de sus áreas, supervisar su cumplimiento y promover una cultura de seguridad.

---

### Personal Administrativo

Incluye al personal de:

- Compras.
- Ventas.
- Finanzas.
- Recursos Humanos.
- Facturación.
- Atención a clientes.
- Administración.
- Logística.

Este personal deberá proteger la información bajo su responsabilidad y cumplir los controles establecidos.

---

### Personal Técnico

Comprende a:

- Ingenieros de campo.
- Técnicos de soporte.
- Técnicos de reparación.
- Personal de garantías.
- Instaladores.
- Especialistas en redes.
- Especialistas en CCTV.
- Especialistas en control de acceso.

Durante la ejecución de sus actividades deberán proteger tanto los activos de la empresa como los de los clientes.

---

## Personal de Almacén

Responsable del resguardo de:

- Equipos.
- Refacciones.
- Herramientas.
- Inventarios.
- Materiales.
- Activos tecnológicos.

Deberá cumplir con procedimientos de recepción, almacenamiento, inventario y entrega para asegurar la trazabilidad de los bienes.

---

## Contratistas y Subcontratistas

Toda empresa o persona que preste servicios para Q MAS IT S. deberá cumplir esta política mientras se encuentre realizando actividades relacionadas con la organización.

---

## Proveedores

Los proveedores que tengan acceso a instalaciones, sistemas, información o activos deberán cumplir los controles de seguridad establecidos mediante contratos, acuerdos de confidencialidad o requisitos específicos.

---

## Visitantes

Toda persona ajena a la organización deberá cumplir las medidas de control de acceso, registro, acompañamiento y protección de la información durante su permanencia en las instalaciones.

---

## 2.3 Procesos incluidos

La política aplica a todos los procesos de la empresa, incluyendo:

- Comercialización de tecnología.
- Atención a clientes.
- Elaboración de propuestas.
- Gestión de proyectos.
- Compras.
- Recepción de mercancías.
- Almacenamiento.
- Inventarios.
- Logística.
- Transporte de equipos.
- Instalación de infraestructura tecnológica.
- Configuración de sistemas.
- Servicios en sitio.
- Soporte técnico.
- Reparación de equipos.
- Gestión de garantías.
- Atención postventa.
- Administración financiera.
- Recursos Humanos.
- Tecnologías de la Información.
- Gestión documental.
- Control de proveedores.
- Gestión de riesgos.
- Continuidad del negocio.

---

## 2.4 Activos protegidos

La política protege, entre otros, los siguientes activos:

### Activos físicos

- Equipos de cómputo.
- Impresoras.
- Servidores.

- Switches.
- Routers.
- Herramientas.
- Vehículos.
- Refacciones.
- Mobiliario.
- Infraestructura.

### Activos tecnológicos

- Sistemas ERP.
- Plataformas SaaS.
- Sistemas CRM.
- Correo electrónico corporativo.
- Servidores.
- Bases de datos.
- Licencias de software.
- Equipos de comunicación.

### Activos de información

- Información de clientes.
- Contratos.
- Cotizaciones.
- Información financiera.
- Datos personales.
- Documentación técnica.
- Planos.
- Diagramas.
- Manuales.
- Inventarios.
- Reportes de servicio.

### Activos intangibles

- Marca Q MAS IT S.
- Reputación corporativa.
- Propiedad intelectual.
- Know-how.
- Relaciones comerciales.
- Información estratégica.
- Cartera de clientes.

---

## 2.5 Exclusiones

Quedan fuera del alcance únicamente aquellas actividades o recursos sobre los cuales Q MAS IT S. no tenga control directo o responsabilidad contractual. No obstante, cuando dichas actividades puedan representar un riesgo para la organización, se establecerán mecanismos de supervisión, requisitos de seguridad o cláusulas contractuales para mitigar los riesgos identificados.

---

## 2.6 Vigencia del Alcance

El alcance de esta política será revisado al menos una vez al año o cuando ocurran cambios significativos en:

- La estructura organizacional.
- Los servicios ofrecidos.
- La infraestructura tecnológica.
- Los procesos del negocio.
- Los requisitos legales.
- Las necesidades de los clientes.
- Los riesgos identificados.

Toda modificación deberá ser aprobada por la Dirección General y comunicada oportunamente a las partes interesadas para asegurar su correcta implementación.

# 3. Compromiso de la Dirección

## 3.1 Declaración de Compromiso

La Alta Dirección de **Q MAS IT S. de R.L. de C.V.** reconoce que la seguridad del negocio es un componente estratégico para el éxito y la sostenibilidad de la organización. Debido a la naturaleza de nuestros servicios —que incluyen la comercialización de tecnología, implementación de infraestructura tecnológica, soporte técnico, mantenimiento preventivo y correctivo, reparación de equipos bajo garantía, administración de activos tecnológicos y desarrollo de proyectos de integración—, la empresa mantiene el firme compromiso de proteger a sus colaboradores, clientes, proveedores, activos físicos, infraestructura tecnológica, información y procesos críticos.

La Dirección General asume el liderazgo para promover una cultura organizacional orientada a la prevención, la gestión integral de riesgos y la mejora continua, garantizando que las decisiones estratégicas del negocio consideren permanentemente los aspectos de seguridad física, seguridad de la información, ciberseguridad, continuidad operativa y cumplimiento legal.

Asimismo, la Dirección reconoce que la seguridad del negocio no es responsabilidad exclusiva de un área específica, sino un compromiso compartido por todos los niveles de la organización, fomentando la participación activa de colaboradores, contratistas y socios comerciales.

## 3.2 Liderazgo y Responsabilidad

La Dirección General ejercerá un liderazgo visible y permanente mediante:

- Definir la estrategia corporativa en materia de Seguridad del Negocio.
- Aprobar y difundir la presente política.
- Integrar la seguridad como parte de la planeación estratégica de la empresa.
- Garantizar que los objetivos de seguridad estén alineados con los objetivos comerciales.
- Evaluar periódicamente el desempeño del Sistema de Seguridad del Negocio.
- Promover la cultura de prevención en toda la organización.
- Participar en revisiones periódicas del sistema de gestión.
- Asegurar que las responsabilidades relacionadas con la seguridad sean claramente comunicadas.
- Impulsar programas de mejora continua.
- Respaldar la implementación de acciones correctivas y preventivas.

La Dirección comunicará de manera constante la importancia de la seguridad mediante reuniones, comunicados internos, capacitaciones y revisiones de desempeño.

## 3.3 Asignación de Recursos

Para garantizar la eficacia del Sistema de Seguridad del Negocio, la Dirección proporcionará los recursos necesarios, incluyendo:

### Recursos Humanos

- Personal competente para la gestión de riesgos.
- Personal especializado en tecnologías de la información.
- Técnicos certificados.
- Responsables de seguridad.
- Personal administrativo capacitado.

### Recursos Tecnológicos

- Equipos de videovigilancia.
- Sistemas de control de acceso.
- Firewalls.
- Antivirus corporativos.
- Plataformas de monitoreo.
- Sistemas de respaldo.
- Equipos de protección eléctrica.

- Software de gestión de inventarios.
- Plataformas para administración documental.

### Recursos Financieros

La empresa asignará presupuesto para:

- Capacitación.
- Renovación tecnológica.
- Licenciamiento de software.
- Auditorías.
- Mantenimiento preventivo.
- Equipamiento de seguridad.
- Consultoría especializada.
- Mejoras de infraestructura.

### Recursos Materiales

- Herramientas.
- Equipos de medición.
- Equipos de protección personal.
- Dispositivos de almacenamiento seguro.
- Señalización.
- Extintores.
- Botiquines.
- Sistemas de respaldo energético.

---

## 3.4 Gestión Integral del Riesgo

La Dirección establecerá un proceso permanente para identificar y controlar riesgos relacionados con:

### Riesgos Operativos

- Errores humanos.
- Interrupciones de servicio.
- Fallas de equipos.
- Incumplimiento de procesos.
- Deficiencias en la logística.

### Riesgos Tecnológicos

- Ataques cibernéticos.

- Malware.
- Ransomware.
- Robo de información.
- Fallas de servidores.
- Pérdida de bases de datos.
- Vulnerabilidades en redes.

### Riesgos Físicos

- Robo.
- Vandalismo.
- Incendios.
- Inundaciones.
- Sismos.
- Daños estructurales.
- Sabotaje.

### Riesgos Comerciales

- Incumplimiento contractual.
- Dependencia de proveedores.
- Afectación a la reputación.
- Fraude.
- Pérdida de clientes.

Todos los riesgos deberán evaluarse considerando:

- Probabilidad de ocurrencia.
- Impacto potencial.
- Nivel de criticidad.
- Controles existentes.
- Acciones de mitigación.

---

## 3.5 Cumplimiento Legal

La Dirección garantizará el cumplimiento de:

- Legislación laboral.
- Normativa de protección civil.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Normas Oficiales Mexicanas aplicables.
- Requisitos fiscales.
- Obligaciones contractuales.
- Licencias de software.

- Requisitos de fabricantes.
- Políticas de clientes.

Asimismo, se mantendrá un proceso para identificar cambios regulatorios y actualizar los procedimientos internos cuando sea necesario.

---

## 3.6 Desarrollo de Competencias

La Dirección promoverá el desarrollo continuo del personal mediante programas de capacitación en:

- Seguridad física.
- Ciberseguridad.
- Protección de datos.
- Continuidad del negocio.
- Gestión de riesgos.
- Respuesta a incidentes.
- Prevención del fraude.
- Manejo seguro de activos tecnológicos.
- Ética y cumplimiento.

Se fomentará además la obtención de certificaciones técnicas relevantes para fortalecer la competencia del personal.

---

## 3.7 Comunicación y Cultura Organizacional

La Dirección impulsará una cultura basada en:

- Transparencia.
- Integridad.
- Responsabilidad.
- Confidencialidad.
- Trabajo en equipo.
- Reporte oportuno de incidentes.
- Aprendizaje continuo.
- Mejora permanente.

Se establecerán canales de comunicación para que cualquier colaborador pueda reportar riesgos, incidentes o actos inseguros sin temor a represalias.

---

## 3.8 Revisión por la Dirección

Al menos una vez al año, la Dirección realizará una revisión formal del Sistema de Seguridad del Negocio para evaluar:

- Cumplimiento de objetivos.
- Resultados de auditorías.
- Indicadores de desempeño.
- Incidentes registrados.
- Riesgos emergentes.
- Cambios tecnológicos.
- Cambios organizacionales.
- Acciones correctivas implementadas.
- Necesidades de recursos.
- Oportunidades de mejora.

Las decisiones derivadas de esta revisión se documentarán y darán seguimiento hasta su implementación.

---

# 4. Principios de Seguridad del Negocio

## 4.1 Generalidades

Los Principios de Seguridad del Negocio constituyen la base sobre la cual Q MAS IT S. desarrolla, implementa y mejora su Sistema de Gestión de Seguridad. Estos principios orientan todas las decisiones y actividades relacionadas con la protección de personas, activos, información y operaciones, buscando reducir riesgos y fortalecer la resiliencia organizacional.

Todo colaborador deberá conocer, comprender y aplicar estos principios en el desempeño de sus funciones.

---

## 4.2 Principio de Protección de las Personas

Las personas son el activo más importante de la organización. La empresa se compromete a proporcionar un entorno de trabajo seguro, promoviendo condiciones que prevengan lesiones, enfermedades, actos de violencia y cualquier situación que comprometa la integridad física o psicológica de los colaboradores.

Para ello se implementarán acciones como:

- Programas de capacitación en seguridad.
- Uso adecuado de Equipo de Protección Personal cuando aplique.
- Protocolos de actuación ante emergencias.
- Evaluaciones de riesgos laborales.
- Simulacros.
- Controles de acceso a instalaciones.
- Medidas para prevenir actos de violencia laboral.

---

## 4.3 Principio de Protección de los Activos

Todos los activos de la organización deberán ser protegidos durante todo su ciclo de vida, desde su adquisición hasta su disposición final.

Esto incluye:

### Activos físicos

- Equipos de cómputo.
- Servidores.
- Herramientas.
- Equipos de laboratorio.
- Vehículos.
- Refacciones.
- Infraestructura.

### Activos tecnológicos

- Redes.
- Software.
- Licencias.
- Sistemas de gestión.
- Plataformas en la nube.

### Activos intangibles

- Marca.
- Reputación.
- Información estratégica.
- Know-how.
- Relaciones comerciales.

Se implementarán controles como:

- Inventarios.

- Etiquetado de activos.
- Custodia.
- Mantenimiento preventivo.
- Control de préstamos.
- Auditorías físicas.
- Monitoreo mediante CCTV.
- Seguros cuando corresponda.

---

## 4.4 Principio de Protección de la Información

La información es uno de los activos más valiosos de la organización y deberá protegerse durante todo su ciclo de vida.

La empresa garantizará:

### Confidencialidad

Solo las personas autorizadas podrán acceder a la información.

### Integridad

La información deberá mantenerse completa y libre de modificaciones no autorizadas.

### Disponibilidad

La información deberá estar accesible cuando sea requerida para la operación del negocio.

### Trazabilidad

Toda modificación relevante deberá poder identificarse y rastrearse.

Para lograrlo se implementarán:

- Controles de acceso.
- Gestión de usuarios.
- Políticas de contraseñas.
- Cifrado de información.
- Respaldos periódicos.
- Clasificación documental.
- Destrucción segura de información obsoleta.

---

## 4.5 Principio de Gestión del Riesgo

Todas las decisiones deberán considerar los riesgos potenciales para el negocio.

La empresa mantendrá un proceso permanente para:

- Identificar amenazas.
- Detectar vulnerabilidades.
- Evaluar impactos.
- Priorizar riesgos.
- Implementar controles.
- Monitorear la eficacia de dichos controles.

La gestión del riesgo será preventiva y estará integrada en todos los procesos del negocio.

---

## 4.6 Principio de Continuidad del Negocio

La organización implementará mecanismos que permitan mantener la operación ante eventos adversos.

Entre ellos:

- Plan de Continuidad del Negocio (BCP).
- Plan de Recuperación ante Desastres (DRP).
- Respaldos automáticos.
- Infraestructura redundante cuando sea viable.
- Proveedores alternativos.
- Procedimientos de recuperación.
- Simulacros periódicos.

El objetivo es minimizar el impacto financiero y operativo de cualquier interrupción.

---

## 4.7 Principio de Cumplimiento

Todos los colaboradores deberán cumplir:

- Legislación aplicable.
- Contratos.
- Políticas internas.
- Procedimientos.
- Normas técnicas.

- Acuerdos de confidencialidad.
- Requisitos de clientes.

El incumplimiento podrá derivar en medidas disciplinarias o acciones legales.

---

## 4.8 Principio de Mejora Continua

El Sistema de Seguridad del Negocio será revisado y fortalecido de manera permanente mediante:

- Auditorías internas.
- Auditorías de clientes.
- Indicadores de desempeño.
- Evaluación de riesgos.
- Investigación de incidentes.
- Acciones correctivas.
- Acciones preventivas.
- Revisión por la Dirección.

La organización promoverá la innovación y la adopción de nuevas tecnologías que incrementen los niveles de seguridad.

---

## 4.9 Principio de Responsabilidad Compartida

La seguridad del negocio es responsabilidad de todos los integrantes de Q MAS IT S. Cada colaborador, sin importar su puesto o nivel jerárquico, deberá actuar de manera ética y responsable, protegiendo los recursos bajo su custodia y reportando cualquier condición insegura, vulnerabilidad o incidente que pueda afectar a la organización.

La colaboración entre áreas, la comunicación efectiva y el compromiso individual son elementos esenciales para mantener un entorno seguro y garantizar la continuidad de las operaciones.

# 5. Gestión Integral de Riesgos del Negocio

## 5.1 Objetivo

La Gestión Integral de Riesgos tiene como propósito establecer una metodología sistemática para identificar, analizar, evaluar, tratar, monitorear y controlar los riesgos que puedan afectar el

cumplimiento de los objetivos estratégicos, operativos, financieros, tecnológicos y comerciales de **Q MAS IT S. de R.L. de C.V.**

Como empresa dedicada a la comercialización de tecnología, integración de soluciones de TI, instalación de infraestructura tecnológica, mantenimiento preventivo y correctivo, reparación de equipos bajo garantía y soporte técnico especializado, Q MAS IT S. reconoce que la adecuada administración de los riesgos constituye un elemento esencial para garantizar la continuidad del negocio, la satisfacción del cliente y la protección de sus activos.

La gestión de riesgos permitirá anticiparse a eventos adversos, reducir pérdidas económicas, fortalecer la toma de decisiones y mejorar la capacidad de respuesta de la organización.

---

# 5.2 Alcance de la Gestión de Riesgos

La gestión de riesgos aplica a todos los procesos de la organización, incluyendo:

- Dirección General.
- Administración.
- Recursos Humanos.
- Compras.
- Ventas.
- Logística.
- Almacén.
- Servicios Técnicos.
- Ingeniería.
- Garantías.
- Soporte Remoto.
- Soporte en Sitio.
- Infraestructura Tecnológica.
- Seguridad Informática.
- Finanzas.
- Atención al Cliente.
- Gestión Documental.
- Transporte de Equipos.
- Instalaciones en sitio.
- Desarrollo e implementación de proyectos.

También aplica a:

- Colaboradores.
- Contratistas.
- Proveedores.
- Visitantes.
- Clientes cuando interactúan dentro de las instalaciones de la empresa.

# 5.3 Principios de la Gestión del Riesgo

La gestión de riesgos se basa en los siguientes principios:

- Enfoque preventivo.
- Participación de todas las áreas.
- Mejora continua.
- Evaluación objetiva.
- Toma de decisiones basada en evidencia.
- Cumplimiento legal.
- Protección de los activos del negocio.
- Continuidad operacional.
- Proporcionalidad de los controles.
- Responsabilidad compartida.

# 5.4 Metodología para la Gestión de Riesgos

Q MAS IT S. utilizará una metodología estructurada que comprende las siguientes etapas:

## Etapa 1. Identificación de Riesgos

Cada área deberá identificar periódicamente las amenazas que puedan afectar sus actividades.

La identificación incluirá riesgos relacionados con:

### Riesgos Estratégicos

- Pérdida de clientes.
- Competencia.
- Cambios tecnológicos.
- Cambios regulatorios.
- Dependencia de fabricantes.
- Dependencia de proveedores críticos.

### Riesgos Operativos

- Errores en instalaciones.
- Daño a equipos del cliente.
- Retrasos en entregas.
- Mala administración del almacén.

- Pérdida de inventario.
- Incumplimiento de garantías.
- Errores administrativos.

## Riesgos Tecnológicos

- Ataques cibernéticos.
- Ransomware.
- Malware.
- Robo de información.
- Caída de servidores.
- Interrupción de Internet.
- Falla de software.
- Pérdida de respaldos.

## Riesgos Financieros

- Fraude.
- Incumplimiento de pagos.
- Variación del tipo de cambio.
- Incremento de costos.
- Robo de recursos.
- Facturación incorrecta.

## Riesgos de Seguridad Física

- Robo.
- Vandalismo.
- Sabotaje.
- Incendios.
- Inundaciones.
- Sismos.
- Daños eléctricos.
- Accidentes.

## Riesgos Contractuales

- Incumplimiento de contratos.
- Penalizaciones.
- Incumplimiento de niveles de servicio (SLA).
- Demandas.
- Conflictos comerciales.

# Etapa 2. Análisis del Riesgo

Cada riesgo será analizado considerando:

### Probabilidad

Frecuencia con la que puede presentarse.

Clasificación:

- Muy Baja
- Baja
- Media
- Alta
- Muy Alta

### Impacto

Consecuencia para la organización.

El impacto podrá evaluarse sobre:

- Finanzas.
- Operación.
- Clientes.
- Imagen corporativa.
- Seguridad.
- Cumplimiento legal.
- Continuidad del negocio.

---

# Etapa 3. Evaluación

Con base en la probabilidad e impacto se determinará el nivel del riesgo:

- Bajo
- Moderado
- Alto
- Crítico

Los riesgos altos y críticos deberán contar con planes inmediatos de tratamiento.

---

# Etapa 4. Tratamiento

Dependiendo del nivel identificado podrán aplicarse las siguientes estrategias:

### Evitar

Eliminar completamente la actividad que genera el riesgo.

### Reducir

Implementar controles que disminuyan la probabilidad o el impacto.

Ejemplos:

- CCTV.
- Respaldos.
- Antivirus.
- Capacitación.
- Procedimientos.
- Supervisión.

### Transferir

Compartir el riesgo mediante:

- Seguros.
- Garantías.
- Contratos.
- Acuerdos con proveedores.

### Aceptar

Cuando el riesgo sea bajo y el costo del control sea mayor que el beneficio.

---

# Etapa 5. Monitoreo

Todos los riesgos serán revisados periódicamente para verificar:

- Cambios en la probabilidad.
- Cambios en el impacto.
- Nuevas amenazas.
- Eficacia de los controles.
- Necesidad de nuevas acciones.

# 5.5 Matriz de Riesgos

La empresa mantendrá una Matriz de Riesgos actualizada que incluya, como mínimo:

- Descripción del riesgo.
- Proceso afectado.
- Activo relacionado.
- Responsable.
- Probabilidad.
- Impacto.
- Nivel del riesgo.
- Controles existentes.
- Acciones de mitigación.
- Fecha de revisión.
- Estado del riesgo.

Esta matriz será revisada al menos una vez al año o cuando ocurran cambios significativos en los procesos.

# 5.6 Controles Preventivos

La organización implementará controles preventivos como:

### Controles Administrativos

- Procedimientos documentados.
- Políticas.
- Capacitación.
- Supervisión.
- Auditorías.
- Segregación de funciones.

### Controles Tecnológicos

- Antivirus.
- Firewalls.
- VPN.
- Autenticación multifactor.
- Monitoreo de redes.
- Respaldos automáticos.

- Cifrado de información.

**Controles Físicos**

- CCTV.
- Alarmas.
- Control de accesos.
- Cerraduras electrónicas.
- Inventarios.
- Etiquetado de activos.

---

# 5.7 Gestión de Riesgos de Proveedores

Antes de contratar proveedores se evaluarán aspectos como:

- Solidez financiera.
- Experiencia.
- Capacidad técnica.
- Cumplimiento legal.
- Historial de desempeño.
- Seguridad de la información.
- Continuidad del servicio.
- Cobertura geográfica.

Los proveedores críticos serán evaluados periódicamente.

---

# 5.8 Indicadores de Riesgo (KRI)

Para medir la eficacia del sistema se establecerán indicadores como:

- Número de incidentes de seguridad.
- Tiempo promedio de recuperación.
- Disponibilidad de servicios.
- Equipos extraviados.
- Incidentes informáticos.
- Cumplimiento de respaldos.
- Nivel de cumplimiento de auditorías.
- Incumplimientos contractuales.
- Daños a equipos durante transporte.
- Incidentes de fraude.

## 5.9 Responsabilidades

### Dirección General

- Aprobar la metodología.
- Revisar riesgos críticos.
- Asignar recursos.

### Gerentes

- Identificar riesgos.
- Implementar controles.
- Dar seguimiento.

### Colaboradores

- Reportar riesgos.
- Cumplir procedimientos.
- Participar en evaluaciones.

---

# 6. Seguridad Física

## 6.1 Objetivo

La Seguridad Física tiene como finalidad proteger las personas, instalaciones, equipos, herramientas, inventarios, documentos e infraestructura tecnológica de **Q MAS IT S. de R.L. de C.V.**, evitando pérdidas derivadas de robos, vandalismo, accesos no autorizados, sabotaje, desastres naturales o cualquier otra amenaza que pueda afectar la continuidad del negocio.

La seguridad física constituye la primera línea de defensa para garantizar la protección de los activos y apoyar el cumplimiento de los objetivos estratégicos de la organización.

---

## 6.2 Alcance

Las disposiciones de este apartado aplican a:

- Oficinas administrativas.

- Centros de servicio.
- Talleres de reparación.
- Almacenes.
- Cuartos de servidores.
- Vehículos corporativos.
- Sitios temporales de trabajo.
- Instalaciones de clientes donde el personal de Q MAS IT S. preste servicios.

También aplican a:

- Colaboradores.
- Técnicos.
- Ingenieros.
- Visitantes.
- Clientes.
- Proveedores.
- Contratistas.

---

## 6.3 Control de Acceso

El acceso a las instalaciones deberá controlarse mediante mecanismos que permitan identificar y registrar a todas las personas que ingresen.

Las medidas incluirán:

- Identificación oficial para visitantes.
- Registro de ingreso y salida.
- Gafetes temporales.
- Control de llaves.
- Accesos restringidos.
- Horarios autorizados.
- Acompañamiento de visitantes.
- Restricción de acceso a áreas críticas.

El acceso a cuartos de servidores, almacenes y archivos será exclusivo para personal autorizado.

---

## 6.4 Protección de Instalaciones

Las instalaciones deberán contar con medidas de protección como:

- Iluminación adecuada.

- Señalización.
- Rutas de evacuación.
- Detectores de humo.
- Extintores.
- CCTV.
- Alarmas contra intrusión.
- Botiquines.
- Salidas de emergencia.
- Protección eléctrica.
- Mantenimiento preventivo.

---

## 6.5 Videovigilancia

La empresa podrá utilizar sistemas CCTV para:

- Protección de activos.
- Supervisión de accesos.
- Investigación de incidentes.
- Prevención del robo.
- Monitoreo del almacén.
- Protección del personal.

Las grabaciones serán administradas conforme a la legislación aplicable en materia de protección de datos personales y únicamente serán consultadas por personal autorizado.

---

## 6.6 Protección del Almacén

El almacén constituye un área crítica debido al resguardo de equipos tecnológicos de alto valor.

Se implementarán controles como:

- Inventarios cíclicos.
- Conteos físicos.
- Registro de entradas y salidas.
- Etiquetado de activos.
- Control de préstamos.
- Áreas delimitadas.
- Monitoreo mediante cámaras.
- Accesos restringidos.
- Bitácoras de movimiento.

## 6.7 Seguridad durante Transporte

Cuando se transporten equipos o refacciones se deberán aplicar controles como:

- Vehículos autorizados.
- Rutas planificadas.
- Documentación de entrega.
- Evidencia fotográfica cuando aplique.
- Embalaje adecuado.
- Protección contra golpes y humedad.
- Confirmación de recepción por el cliente.
- Custodia reforzada para equipos de alto valor cuando sea necesario.

---

## 6.8 Protección de Equipos en Sitio

Durante la prestación de servicios en instalaciones del cliente, el personal deberá:

- Mantener bajo resguardo las herramientas.
- No dejar equipos desatendidos.
- Identificar claramente los equipos intervenidos.
- Registrar entradas y salidas de activos.
- Solicitar autorización antes de retirar equipos del cliente.
- Cumplir los protocolos de seguridad del sitio.

---

## 6.9 Inspecciones de Seguridad Física

Se realizarán inspecciones periódicas para verificar:

- Estado de cerraduras.
- Funcionamiento de cámaras.
- Estado de alarmas.
- Iluminación.
- Señalización.
- Integridad del almacén.
- Estado de extintores.
- Condiciones del cuarto de servidores.
- Cumplimiento de controles de acceso.

Las desviaciones identificadas deberán documentarse y corregirse mediante acciones correctivas.

## 6.10 Respuesta ante Incidentes de Seguridad Física

Ante cualquier incidente, como robo, intento de intrusión, vandalismo, incendio o daño a instalaciones, el personal deberá:

1. Proteger la integridad de las personas.
2. Notificar inmediatamente a su jefe directo y a la Dirección.
3. Preservar la escena cuando sea necesario.
4. Registrar el incidente en la bitácora correspondiente.
5. Recopilar evidencias disponibles (fotografías, videos, testimonios).
6. Colaborar con las autoridades competentes cuando aplique.
7. Participar en la investigación del incidente.
8. Implementar acciones correctivas para evitar su repetición.

La Dirección evaluará el impacto del incidente y, en caso de afectar la operación, activará el Plan de Continuidad del Negocio para restablecer los procesos críticos en el menor tiempo posible.

# 7. Seguridad del Personal

## 7.1 Objetivo

La Seguridad del Personal tiene como objetivo establecer los lineamientos, responsabilidades y controles necesarios para proteger la integridad física, psicológica y profesional de todos los colaboradores de **Q MAS IT S. de R.L. de C.V.**, así como asegurar que cada persona desempeñe sus funciones de manera segura, ética y conforme a los procedimientos establecidos.

La empresa reconoce que el recurso humano constituye su activo más valioso y que la seguridad del negocio depende en gran medida del comportamiento, compromiso y nivel de preparación de quienes participan en las operaciones.

Por ello, Q MAS IT S. promoverá una cultura organizacional basada en la prevención, el cumplimiento de las normas, la responsabilidad individual y colectiva, el respeto a los derechos humanos y la mejora continua.

# 7.2 Alcance

Las disposiciones de este capítulo aplican a:

- Dirección General.

- Personal administrativo.
- Ingenieros de preventa.
- Ingenieros de proyectos.
- Técnicos de instalación.
- Técnicos de soporte.
- Personal de garantías.
- Personal de almacén.
- Personal de logística.
- Compradores.
- Vendedores.
- Contratistas.
- Prestadores de servicios.
- Personal temporal.
- Becarios.
- Visitantes que permanezcan dentro de las instalaciones.

---

# 7.3 Responsabilidades del Personal

Todo colaborador deberá asumir la responsabilidad de contribuir activamente a la seguridad del negocio.

Entre sus obligaciones se encuentran:

- Cumplir la presente Política de Seguridad del Negocio.
- Conocer los procedimientos aplicables a su puesto.
- Participar en las capacitaciones obligatorias.
- Utilizar correctamente las herramientas y equipos asignados.
- Proteger la información confidencial de clientes y de la empresa.
- Resguardar los activos bajo su responsabilidad.
- Reportar inmediatamente cualquier incidente o condición insegura.
- Mantener una conducta ética y profesional.
- Respetar las normas de seguridad de los clientes cuando se trabaje en sus instalaciones.
- Evitar acciones que comprometan la reputación o continuidad del negocio.

El desconocimiento de esta política no exime de su cumplimiento.

---

# 7.4 Proceso de Incorporación del Personal

Antes de iniciar actividades, todo colaborador deberá completar un proceso de inducción que incluya:

### Inducción Organizacional

- Historia de la empresa.
- Misión, visión y valores.
- Código de ética.
- Política de Seguridad del Negocio.
- Políticas de seguridad de la información.
- Procedimientos internos.
- Organigrama.
- Responsabilidades del puesto.

### Capacitación Inicial

El colaborador recibirá capacitación sobre:

- Protección de activos.
- Manejo de información confidencial.
- Ciberseguridad.
- Gestión de incidentes.
- Control de accesos.
- Protección de datos personales.
- Prevención de fraude.
- Continuidad del negocio.
- Seguridad en instalaciones del cliente.

---

# 7.5 Competencia y Capacitación Continua

La empresa desarrollará un programa anual de capacitación que considere:

## Capacitación Técnica

- Equipos comercializados.
- Plataformas tecnológicas.
- Nuevas soluciones.
- Sistemas de seguridad electrónica.
- Redes.
- Infraestructura.
- Soporte técnico.

## Capacitación en Seguridad

- Seguridad física.

- Ciberseguridad.
- Protección de datos.
- Gestión de riesgos.
- Seguridad del negocio.
- Prevención de incidentes.
- Ingeniería social.
- Phishing.
- Protección de activos.

## Capacitación Normativa

- Políticas internas.
- Procedimientos.
- Legislación aplicable.
- Requisitos contractuales.
- Normas del cliente.

Toda capacitación deberá documentarse mediante listas de asistencia, evaluaciones y registros de competencia.

---

# 7.6 Conducta Ética

Los colaboradores deberán actuar conforme a los siguientes principios:

- Honestidad.
- Integridad.
- Responsabilidad.
- Confidencialidad.
- Respeto.
- Profesionalismo.
- Imparcialidad.
- Transparencia.

Está estrictamente prohibido:

- Aceptar sobornos.
- Alterar información.
- Falsificar documentos.
- Manipular inventarios.
- Compartir contraseñas.
- Revelar información confidencial.
- Utilizar recursos de la empresa para fines personales sin autorización.
- Realizar actos de discriminación.

- Incurrir en acoso laboral o sexual.
- Consumir alcohol o drogas durante la jornada laboral o presentarse bajo sus efectos.

Cualquier incumplimiento será investigado y sancionado conforme a la normativa interna y la legislación aplicable.

---

# 7.7 Protección de la Información por Parte del Personal

Cada colaborador será responsable de proteger la información a la que tenga acceso.

Para ello deberá:

- Mantener la confidencialidad de la información.
- Utilizar únicamente equipos autorizados.
- No compartir archivos con terceros sin autorización.
- Bloquear la computadora cuando se ausente de su lugar de trabajo.
- Mantener bajo resguardo documentos impresos.
- Utilizar únicamente plataformas autorizadas para intercambio de información.
- Reportar cualquier sospecha de fuga de información.

---

# 7.8 Uso de Recursos Tecnológicos

Los recursos tecnológicos proporcionados por la empresa deberán utilizarse exclusivamente para actividades laborales.

Incluyen:

- Computadoras.
- Teléfonos corporativos.
- Tablets.
- Servidores.
- Correos electrónicos.
- Software.
- VPN.
- Plataformas SaaS.
- Sistemas ERP.
- Sistemas CRM.

No está permitido:

- Instalar software sin autorización.
- Descargar contenido ilegal.
- Utilizar dispositivos USB no autorizados.
- Conectar equipos personales a la red corporativa sin autorización.
- Compartir credenciales.
- Desactivar antivirus o sistemas de seguridad.

---

# 7.9 Seguridad del Personal en Sitios del Cliente

Cuando un colaborador realice actividades en instalaciones del cliente deberá:

- Identificarse correctamente.
- Cumplir los protocolos del cliente.
- Utilizar el Equipo de Protección Personal requerido.
- Proteger los activos del cliente.
- Respetar la confidencialidad de la información observada.
- No realizar actividades fuera del alcance autorizado.
- Mantener comunicación permanente con su supervisor cuando el proyecto lo requiera.

---

# 7.10 Reporte de Incidentes

Todo colaborador tiene la obligación de reportar inmediatamente:

- Robo.
- Pérdida de equipos.
- Accesos no autorizados.
- Daños a instalaciones.
- Fugas de información.
- Intentos de fraude.
- Ataques informáticos.
- Accidentes.
- Amenazas.
- Conductas sospechosas.

El reporte deberá realizarse sin demora al jefe inmediato o al responsable designado, evitando ocultar o minimizar los hechos.

## 7.11 Medidas Disciplinarias

El incumplimiento de las disposiciones establecidas en este capítulo podrá dar lugar a:

- Amonestación verbal.
- Amonestación escrita.
- Reentrenamiento obligatorio.
- Suspensión temporal.
- Rescisión de la relación laboral.
- Denuncias ante autoridades competentes cuando exista una conducta ilícita.

Las medidas disciplinarias serán proporcionales a la gravedad del incumplimiento y respetarán los derechos laborales del colaborador.

---

# 8. Seguridad Informática y Ciberseguridad

## 8.1 Objetivo

La Seguridad Informática tiene como finalidad proteger los sistemas de información, redes, infraestructura tecnológica, aplicaciones, bases de datos y activos digitales de **Q MAS IT S. de R.L. de C.V.**, garantizando la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

Debido a que la empresa administra información estratégica de clientes, proyectos, contratos, garantías, inventarios y soluciones tecnológicas, la protección frente a amenazas cibernéticas constituye un elemento crítico para asegurar la continuidad del negocio y mantener la confianza de las partes interesadas.

---

## 8.2 Alcance

Este capítulo aplica a:

- Equipos de escritorio.
- Laptops.
- Tablets.
- Teléfonos corporativos.
- Servidores.

- Equipos de almacenamiento.
- Redes LAN y Wi-Fi.
- Equipos de telecomunicaciones.
- Sistemas ERP.
- Plataformas CRM.
- Plataformas SaaS.
- Correo electrónico corporativo.
- Servicios en la nube.
- Aplicaciones móviles.
- Sistemas de respaldo.
- Equipos utilizados por personal remoto.

---

# 8.3 Principios de Seguridad Informática

La gestión de la seguridad informática se basa en los siguientes principios:

- Confidencialidad.
- Integridad.
- Disponibilidad.
- Autenticidad.
- Trazabilidad.
- Mínimo privilegio.
- Defensa en profundidad.
- Gestión del riesgo.
- Mejora continua.

---

# 8.4 Gestión de Identidades y Accesos

Cada usuario contará con credenciales únicas e intransferibles.

Se aplicarán las siguientes medidas:

- Cuentas individuales.
- Contraseñas robustas.
- Renovación periódica de contraseñas.
- Autenticación multifactor (MFA) en sistemas críticos.
- Bloqueo automático por intentos fallidos de autenticación.
- Desactivación inmediata de cuentas de personal que cause baja.
- Revisión periódica de privilegios de acceso.

Los permisos se otorgarán bajo el principio de **mínimo privilegio**, limitando el acceso únicamente a la información necesaria para el desempeño de las funciones asignadas.

---

# 8.5 Protección de Equipos y Redes

Todos los equipos corporativos deberán contar con:

- Antivirus de nivel empresarial.
- Firewall activo.
- Actualizaciones automáticas.
- Software legal y licenciado.
- Cifrado de discos cuando aplique.
- Bloqueo automático de pantalla.
- Herramientas de monitoreo y gestión remota.
- Inventario actualizado de hardware y software.

Las redes deberán protegerse mediante:

- Segmentación lógica.
- Redes Wi-Fi seguras con cifrado WPA3 o superior cuando sea posible.
- VPN para acceso remoto.
- Monitoreo continuo del tráfico de red.
- Restricción de puertos y servicios innecesarios.

---

# 8.6 Gestión de Vulnerabilidades y Actualizaciones

Con el fin de reducir la exposición a amenazas, la empresa realizará:

- Actualizaciones periódicas de sistemas operativos.
- Actualizaciones de firmware de equipos de red y seguridad.
- Aplicación de parches de seguridad para aplicaciones críticas.
- Evaluaciones de vulnerabilidades.
- Revisión de configuraciones seguras.
- Eliminación de software obsoleto o sin soporte.

Las actualizaciones deberán planificarse para minimizar el impacto en la operación del negocio.

---

# 8.7 Protección contra Malware y Ataques Cibernéticos

Se implementarán controles para prevenir y detectar amenazas como:

- Virus.
- Gusanos.
- Troyanos.
- Spyware.
- Ransomware.
- Phishing.
- Ataques de ingeniería social.
- Ataques de denegación de servicio (DoS/DDoS).
- Accesos no autorizados.

Entre los controles se incluyen:

- Filtros de correo electrónico.
- Antivirus y antimalware actualizados.
- Monitoreo de eventos de seguridad.
- Capacitación periódica al personal.
- Bloqueo de archivos ejecutables sospechosos.
- Políticas de navegación segura.

---

# 8.8 Gestión de Respaldos

La empresa realizará respaldos periódicos de la información crítica.

Los respaldos deberán cumplir con los siguientes criterios:

- Programación automática.
- Almacenamiento cifrado.
- Copias en ubicaciones distintas (local y nube).
- Verificación periódica de restauración.
- Conservación según políticas de retención.
- Acceso restringido únicamente a personal autorizado.

---

# 8.9 Monitoreo y Registro de Eventos

Los sistemas críticos deberán generar registros (logs) que permitan:

- Identificar accesos.
- Detectar actividades inusuales.
- Investigar incidentes.
- Rastrear cambios relevantes.
- Facilitar auditorías.

Los registros serán protegidos contra modificaciones no autorizadas y se conservarán durante el tiempo definido por la empresa y la legislación aplicable.

---

# 8.10 Respuesta ante Incidentes de Ciberseguridad

Ante un incidente de seguridad informática se seguirá, como mínimo, el siguiente proceso:

1. Detección del incidente.
2. Contención inmediata para limitar el impacto.
3. Notificación al responsable de TI y a la Dirección.
4. Análisis de la causa raíz.
5. Erradicación de la amenaza.
6. Recuperación de los sistemas afectados.
7. Validación de la operación normal.
8. Documentación del incidente.
9. Implementación de acciones correctivas y preventivas.

Cuando el incidente comprometa información de clientes o pueda afectar significativamente la continuidad del negocio, la Dirección evaluará la necesidad de informar a las partes interesadas y a las autoridades competentes, conforme a las obligaciones legales y contractuales aplicables.

---

# 8.11 Auditoría y Mejora Continua

La eficacia de los controles de seguridad informática será evaluada mediante:

- Auditorías internas.
- Revisiones de configuración.
- Pruebas de restauración de respaldos.
- Evaluaciones de vulnerabilidades.
- Indicadores de desempeño.

- Revisión de incidentes.
- Simulaciones de respuesta a ciberataques.

Los resultados serán utilizados para fortalecer continuamente la postura de ciberseguridad de Q MAS IT S. de R.L. de C.V., adaptando los controles a las nuevas amenazas y a la evolución tecnológica.

# 9. Seguridad en las Operaciones de Campo

## 9.1 Objetivo

El presente apartado tiene como finalidad establecer los lineamientos, controles y responsabilidades que deberán observar todos los colaboradores de **Q MAS IT S. de R.L. de C.V.** durante la ejecución de actividades fuera de las instalaciones de la empresa, con el propósito de proteger la integridad del personal, los activos de la organización, los bienes de los clientes y la continuidad de las operaciones.

Las operaciones de campo representan uno de los procesos de mayor riesgo para la organización debido a que implican el traslado de personal y equipos tecnológicos de alto valor, el acceso a instalaciones de terceros y la interacción con infraestructura crítica. Por ello, se implementarán medidas preventivas que permitan minimizar riesgos de accidentes, pérdidas, robos, daños, fugas de información e incumplimientos contractuales.

---

# 9.2 Alcance

Esta política aplica a todas las actividades realizadas fuera de las instalaciones de Q MAS IT S., incluyendo, entre otras:

- Instalación de sistemas de videovigilancia (CCTV).
- Instalación de controles de acceso.
- Implementación de redes de datos.
- Instalación de fibra óptica.
- Configuración de servidores y equipos de cómputo.
- Mantenimiento preventivo y correctivo.
- Reparación de equipos en garantía.
- Diagnósticos técnicos.
- Levantamientos de información para proyectos.
- Puestas en marcha.
- Capacitaciones en sitio.
- Entregas de equipos.
- Recolección de equipos para reparación.
- Auditorías técnicas.

- Supervisión de proyectos.
- Soporte técnico presencial.

---

# 9.3 Planeación de los Trabajos

Antes de iniciar cualquier servicio en campo, el responsable del proyecto deberá realizar una planificación que considere:

### Información del Cliente

- Nombre del cliente.
- Dirección del sitio.
- Persona de contacto.
- Teléfonos de emergencia.
- Horarios autorizados.
- Restricciones de acceso.

### Alcance Técnico

- Actividades a desarrollar.
- Equipos involucrados.
- Materiales requeridos.
- Herramientas necesarias.
- Personal asignado.
- Tiempo estimado.

### Evaluación de Riesgos

Antes de acudir al sitio deberá identificarse:

- Riesgos eléctricos.
- Riesgos por trabajo en alturas.
- Riesgos ergonómicos.
- Riesgos de tránsito.
- Riesgos ambientales.
- Riesgos de seguridad pública.
- Riesgos por infraestructura deficiente.
- Riesgos de acceso.

---

# 9.4 Requisitos del Personal

Todo colaborador asignado deberá:

- Contar con capacitación técnica.
- Conocer el procedimiento del servicio.
- Portar uniforme institucional.
- Portar identificación oficial de la empresa.
- Contar con el Equipo de Protección Personal requerido.
- Haber recibido inducción en seguridad.
- Estar autorizado por su supervisor.

Cuando el cliente solicite certificaciones específicas, únicamente se asignará personal que cumpla dichos requisitos.

---

# 9.5 Control de Herramientas y Equipos

Antes de salir a un servicio se verificará que:

- Las herramientas se encuentren en buen estado.
- Los equipos de medición estén calibrados cuando aplique.
- Se cuente con el material suficiente.
- Las refacciones correspondan al proyecto.
- Los equipos del cliente estén correctamente identificados.
- Existan documentos de entrega y recepción.

Todo el equipo transportado deberá registrarse en una bitácora de salida.

Al finalizar el servicio deberá verificarse que todas las herramientas regresen al almacén.

---

# 9.6 Transporte Seguro de Equipos

Los equipos tecnológicos representan activos de alto valor económico, por lo que deberán protegerse durante su transporte mediante:

- Embalaje adecuado.
- Protección contra humedad.
- Protección contra impactos.
- Vehículos en buenas condiciones.
- Rutas previamente definidas.
- Documentación de traslado.
- Evidencia fotográfica cuando sea requerida.

En caso de transportar servidores, equipos especializados o mercancía de alto valor, la Dirección podrá autorizar medidas adicionales como:

- Custodia.
- Rastreo GPS.
- Transporte especializado.
- Seguro de mercancía.

---

# 9.7 Acceso a Instalaciones del Cliente

Todo el personal deberá respetar los procedimientos del cliente.

Esto incluye:

- Registro de ingreso.
- Presentación de identificación.
- Firma de bitácoras.
- Uso del gafete temporal.
- Restricciones de fotografía.
- Restricciones de acceso.
- Protocolos de seguridad.
- Horarios autorizados.

Queda prohibido ingresar a áreas distintas de aquellas autorizadas.

---

# 9.8 Protección de la Información del Cliente

Durante los servicios el personal podrá tener acceso a:

- Servidores.
- Equipos de cómputo.
- Información técnica.
- Planos.
- Redes.
- Bases de datos.
- Configuraciones.

Por lo tanto, queda estrictamente prohibido:

- Copiar información del cliente.

- Fotografiar documentación sin autorización.
- Compartir información.
- Utilizar dispositivos USB personales.
- Acceder a información fuera del alcance contratado.
- Modificar configuraciones no autorizadas.

Todo colaborador deberá firmar previamente un Acuerdo de Confidencialidad.

---

# 9.9 Ejecución del Servicio

Durante la ejecución de las actividades el personal deberá:

- Mantener orden en el área de trabajo.
- Delimitar zonas cuando sea necesario.
- Proteger los equipos del cliente.
- Evitar daños a la infraestructura.
- Seguir los procedimientos técnicos.
- Utilizar herramientas adecuadas.
- Documentar cualquier cambio realizado.
- Mantener comunicación con el responsable del proyecto.

---

# 9.10 Entrega del Servicio

Al concluir los trabajos deberá realizarse:

### Revisión Técnica

- Funcionamiento correcto.
- Configuración.
- Pruebas de operación.
- Validación con el cliente.

### Documentación

- Reporte de servicio.
- Evidencia fotográfica.
- Acta de entrega.
- Firma de conformidad.
- Registro de garantías.

## 9.11 Atención de Emergencias

Cuando ocurra un incidente durante el servicio:

- Proteger primero a las personas.
- Suspender actividades si existe riesgo.
- Informar al supervisor.
- Notificar al cliente.
- Documentar el incidente.
- Preservar evidencias.
- Participar en la investigación.

---

## 9.12 Indicadores

La empresa evaluará:

- Servicios realizados sin incidentes.
- Tiempo promedio de atención.
- Daños a equipos.
- Accidentes.
- Reclamos del cliente.
- Retrabajos.
- Cumplimiento del programa de mantenimiento.
- Cumplimiento de tiempos de respuesta (SLA).

---

# 10. Seguridad en la Cadena de Suministro

## 10.1 Objetivo

El objetivo de este apartado es establecer los criterios para asegurar que todos los procesos relacionados con la adquisición, almacenamiento, transporte, distribución y entrega de bienes y servicios se desarrollen bajo condiciones de seguridad, confiabilidad y trazabilidad, minimizando los riesgos que puedan afectar la continuidad operativa de **Q MAS IT S. de R.L. de C.V.**

Dado que la empresa comercializa equipos tecnológicos de alto valor, administra garantías y ejecuta proyectos de integración tecnológica, resulta indispensable controlar los riesgos asociados

con la cadena de suministro para garantizar la entrega oportuna y segura de los productos y servicios ofrecidos a los clientes.

---

# 10.2 Alcance

La presente política aplica a:

- Compras nacionales e internacionales.
- Importaciones.
- Recepción de mercancías.
- Almacén.
- Inventarios.
- Transporte.
- Distribución.
- Proveedores.
- Fabricantes.
- Mayoristas.
- Empresas de mensajería.
- Contratistas logísticos.
- Clientes que entregan equipos para garantía.

---

# 10.3 Selección y Evaluación de Proveedores

La empresa establecerá un proceso formal para seleccionar proveedores, considerando criterios como:

### Aspectos Comerciales

- Experiencia.
- Solidez financiera.
- Cobertura.
- Tiempo de respuesta.
- Historial comercial.

### Aspectos Técnicos

- Calidad de productos.
- Certificaciones.
- Capacidad de suministro.
- Garantías.

- Soporte técnico.

**Aspectos de Seguridad**

- Protección de mercancías.
- Seguridad de la información.
- Continuidad del negocio.
- Cumplimiento normativo.
- Controles logísticos.

Los proveedores críticos deberán ser reevaluados periódicamente mediante indicadores de desempeño.

---

# 10.4 Compras Seguras

Toda adquisición deberá cumplir con un proceso autorizado que incluya:

- Solicitud de compra.
- Cotizaciones.
- Validación presupuestal.
- Aprobación.
- Orden de compra.
- Confirmación del proveedor.
- Seguimiento del embarque.
- Recepción documentada.

No se permitirán compras fuera del procedimiento establecido salvo autorización expresa de la Dirección.

---

# 10.5 Recepción de Mercancías

Al recibir materiales o equipos se verificará:

- Estado físico del embalaje.
- Cantidad recibida.
- Modelo.
- Número de serie.
- Accesorios.
- Documentación.
- Garantías.

- Daños visibles.

Cualquier anomalía deberá documentarse mediante fotografías y registrarse antes de aceptar la mercancía.

---

# 10.6 Control de Inventarios

Todos los activos deberán registrarse en un sistema de inventario que permita conocer:

- Ubicación.
- Responsable.
- Estado.
- Número de serie.
- Fecha de ingreso.
- Fecha de salida.
- Cliente asociado cuando aplique.

Se realizarán inventarios físicos periódicos para verificar la existencia y condición de los bienes.

---

# 10.7 Almacenamiento Seguro

Los almacenes deberán cumplir con condiciones que garanticen la conservación de los equipos:

- Control de acceso.
- Videovigilancia.
- Protección contra incendios.
- Control de humedad y temperatura cuando sea requerido.
- Estanterías adecuadas.
- Separación por categorías.
- Áreas para equipos en garantía, nuevos y en reparación.

Los equipos de alto valor permanecerán en zonas de acceso restringido.

---

# 10.8 Transporte y Distribución

Durante el transporte de mercancías deberán implementarse medidas como:

- Embalaje resistente.
- Etiquetado adecuado.
- Guías de envío.
- Confirmación de entrega.
- Seguimiento del envío.
- Seguro de transporte para equipos de alto valor.
- Empresas de mensajería confiables.
- Control de rutas y tiempos de entrega.

---

# 10.9 Gestión de Equipos en Garantía

Considerando que uno de los principales servicios de Q MAS IT S. es la gestión de garantías, se deberán aplicar controles específicos para asegurar la trazabilidad de cada equipo:

- Registro de ingreso con número de serie.
- Evidencia fotográfica del estado físico.
- Diagnóstico inicial.
- Etiquetado individual.
- Registro del cliente.
- Seguimiento del proceso de reparación.
- Control de refacciones utilizadas.
- Registro de pruebas funcionales.
- Validación de calidad antes de la entrega.
- Acta de entrega al cliente.

Estos controles permiten garantizar la transparencia del proceso y reducir el riesgo de pérdidas, extravíos o reclamaciones.

---

# 10.10 Gestión de Incidentes en la Cadena de Suministro

Ante cualquier incidente que afecte la cadena de suministro, como retrasos, robo, pérdida de mercancía, daño durante el transporte, incumplimiento del proveedor o fallas logísticas, se deberá:

1. Notificar inmediatamente al responsable de Compras y a la Dirección.
2. Documentar el incidente con evidencia disponible.
3. Evaluar el impacto en los proyectos o compromisos con los clientes.
4. Implementar acciones de contención para minimizar afectaciones.
5. Coordinar con el proveedor o empresa transportista las acciones correctivas.

6. Informar oportunamente al cliente cuando exista un impacto en la entrega o servicio.
7. Analizar la causa raíz del incidente.
8. Implementar acciones preventivas para evitar su repetición.

---

# 10.11 Indicadores de Desempeño de la Cadena de Suministro (KPIs)

Con el fin de evaluar la eficacia del proceso, Q MAS IT S. establecerá indicadores como:

- Porcentaje de entregas a tiempo (OTD).
- Nivel de cumplimiento de proveedores.
- Tasa de productos dañados durante el transporte.
- Exactitud del inventario.
- Tiempo promedio de reposición de inventario.
- Tiempo de atención de garantías.
- Número de reclamaciones por errores logísticos.
- Nivel de disponibilidad de productos críticos.
- Índice de devoluciones por errores de suministro.
- Nivel de satisfacción del cliente respecto a la entrega de productos y servicios.

Estos indicadores serán revisados periódicamente por la Dirección para identificar oportunidades de mejora, fortalecer la relación con proveedores estratégicos y asegurar una cadena de suministro resiliente, eficiente y alineada con los objetivos del negocio.

# 11. Prevención del Fraude, Corrupción y Actos Ilícitos

## 11.1 Objetivo

La presente sección tiene como objetivo establecer los principios, controles y mecanismos para prevenir, detectar, investigar y sancionar cualquier acto de fraude, corrupción, soborno, conflicto de intereses, apropiación indebida de activos, falsificación documental o cualquier otra conducta ilícita que pueda afectar los intereses de **Q MAS IT S. de R.L. de C.V.**, sus clientes, proveedores, colaboradores y demás partes interesadas.

La empresa reconoce que el fraude y la corrupción representan riesgos críticos para la continuidad del negocio, la estabilidad financiera, la reputación corporativa y la confianza depositada por sus clientes. Por ello, mantiene una política de **cero tolerancia** frente a cualquier conducta que comprometa la ética, la legalidad o la transparencia en sus operaciones.

# 11.2 Alcance

Esta política aplica a:

- Dirección General.
- Socios.
- Personal administrativo.
- Personal operativo.
- Técnicos de servicio.
- Ingenieros.
- Personal de almacén.
- Compradores.
- Vendedores.
- Contratistas.
- Consultores.
- Proveedores.
- Prestadores de servicios.
- Personal temporal.
- Cualquier persona que actúe en representación de Q MAS IT S.

También aplica a todos los procesos de la organización, incluyendo:

- Compras.
- Ventas.
- Facturación.
- Tesorería.
- Gestión de inventarios.
- Garantías.
- Almacén.
- Recursos Humanos.
- Tecnología de la Información.
- Atención al cliente.
- Logística.
- Servicios técnicos.

# 11.3 Principios Generales

Todos los colaboradores deberán actuar conforme a los siguientes principios:

- Honestidad.

- Integridad.
- Transparencia.
- Legalidad.
- Responsabilidad.
- Imparcialidad.
- Confidencialidad.
- Rendición de cuentas.
- Respeto al patrimonio de la empresa y de los clientes.

La Dirección promoverá un ambiente organizacional donde prevalezcan la ética y el cumplimiento normativo.

---

# 11.4 Definiciones

### Fraude

Toda acción u omisión intencional destinada a obtener un beneficio económico, material o personal mediante engaño, ocultamiento, manipulación o abuso de confianza.

Ejemplos:

- Alteración de facturas.
- Falsificación de reportes.
- Manipulación de inventarios.
- Simulación de servicios.
- Cobros indebidos.

---

### Corrupción

Uso indebido del cargo o funciones para obtener beneficios personales.

Ejemplos:

- Favorecer proveedores.
- Alterar licitaciones.
- Aceptar pagos ilegales.
- Favorecer clientes mediante prácticas indebidas.

---

### Soborno

Ofrecer, prometer, entregar, solicitar o aceptar dinero, regalos, favores o cualquier beneficio para influir indebidamente en una decisión comercial o administrativa.

---

### Conflicto de Interés

Situación donde los intereses personales pueden influir en las decisiones tomadas en representación de la empresa.

Ejemplos:

- Contratar empresas de familiares sin autorización.
- Favorecer proveedores con los que exista relación personal.
- Participar en negociaciones donde exista beneficio propio.

---

# 11.5 Conductas Prohibidas

Queda estrictamente prohibido:

## En Compras

- Manipular cotizaciones.
- Simular procesos de compra.
- Favorecer proveedores.
- Recibir comisiones no autorizadas.
- Alterar órdenes de compra.

---

## En Ventas

- Modificar precios sin autorización.
- Ofrecer descuentos indebidos.
- Alterar contratos.
- Cobrar fuera de los procedimientos establecidos.

---

## En Almacén

- Sustraer mercancía.

- Alterar inventarios.
- Cambiar números de serie.
- Ocultar diferencias de inventario.
- Registrar entradas o salidas falsas.

---

## En Garantías

- Cambiar piezas.
- Sustituir equipos.
- Alterar diagnósticos.
- Emitir reportes falsos.
- Simular reparaciones.

---

## En Recursos Humanos

- Alterar registros de asistencia.
- Simular contrataciones.
- Falsificar documentos laborales.
- Manipular evaluaciones.

---

## En Tecnologías de Información

- Crear usuarios no autorizados.
- Compartir contraseñas.
- Acceder a información sin autorización.
- Alterar bases de datos.
- Eliminar evidencia digital.

---

# 11.6 Controles Antifraude

La empresa implementará controles como:

### Segregación de Funciones

Las actividades críticas deberán distribuirse entre diferentes personas para evitar concentración de responsabilidades.

Ejemplos:

- Quien compra no autoriza el pago.
- Quien recibe mercancía no administra inventarios.
- Quien factura no autoriza descuentos.

---

## Doble Autorización

Las operaciones críticas requerirán al menos dos niveles de autorización.

Ejemplos:

- Compras extraordinarias.
- Transferencias bancarias.
- Ajustes de inventario.
- Cancelaciones de facturas.

---

## Auditorías

Se realizarán auditorías:

- Internas.
- Externas.
- Aleatorias.
- Programadas.

Estas incluirán revisión de:

- Inventarios.
- Facturación.
- Compras.
- Garantías.
- Sistemas.
- Accesos.
- Documentación.

---

## Controles Tecnológicos

Se implementarán mecanismos como:

- Bitácoras electrónicas.
- Registro de accesos.
- CCTV.
- Control de usuarios.
- Trazabilidad de operaciones.
- Monitoreo de sistemas.

---

# 11.7 Regalos, Hospitalidad y Beneficios

Los colaboradores no podrán:

- Solicitar regalos.
- Aceptar dinero.
- Recibir comisiones.
- Aceptar viajes o beneficios personales que puedan comprometer su imparcialidad.

Solo podrán aceptarse obsequios promocionales de valor simbólico cuando no influyan en decisiones comerciales y estén permitidos por la normativa interna.

---

# 11.8 Canal de Denuncias

La empresa establecerá un mecanismo confidencial para que cualquier persona pueda reportar:

- Fraudes.
- Sobornos.
- Corrupción.
- Robo.
- Abuso de confianza.
- Manipulación documental.
- Conflictos de interés.
- Violaciones al Código de Ética.

Las denuncias podrán realizarse de forma anónima y serán tratadas con estricta confidencialidad.

La empresa prohíbe cualquier tipo de represalia contra quienes denuncien de buena fe.

---

# 11.9 Investigación de Casos

Toda denuncia será investigada mediante un proceso formal que incluirá:

1. Recepción del reporte.
2. Registro del caso.
3. Evaluación preliminar.
4. Recolección de evidencia.
5. Entrevistas.
6. Análisis documental.
7. Informe de resultados.
8. Determinación de responsabilidades.
9. Implementación de acciones correctivas.
10. Seguimiento del caso.

Las investigaciones se realizarán respetando los principios de imparcialidad, confidencialidad y debido proceso.

---

# 11.10 Sanciones

Las personas que incurran en actos de fraude o corrupción podrán ser sujetas a:

- Amonestación escrita.
- Suspensión temporal.
- Rescisión del contrato laboral.
- Terminación de contratos comerciales.
- Reclamación por daños y perjuicios.
- Denuncia ante las autoridades competentes cuando corresponda.

---

# 11.11 Indicadores de Control

La Dirección dará seguimiento a indicadores como:

- Número de denuncias recibidas.
- Casos confirmados de fraude.
- Tiempo promedio de investigación.
- Monto de pérdidas recuperadas.
- Incidencias por conflicto de interés.
- Cumplimiento de auditorías.
- Hallazgos recurrentes.
- Nivel de implementación de acciones correctivas.

# 12. Gestión de Incidentes de Seguridad del Negocio

## 12.1 Objetivo

La Gestión de Incidentes tiene como finalidad establecer un proceso estructurado para identificar, reportar, registrar, analizar, contener, investigar, resolver y documentar cualquier incidente que pueda afectar la seguridad de las personas, la información, los activos, las instalaciones, los sistemas tecnológicos o la continuidad de las operaciones de **Q MAS IT S. de R.L. de C.V.**

El objetivo principal es minimizar el impacto operativo, financiero, legal y reputacional de los incidentes, garantizar una respuesta oportuna y fortalecer la capacidad de la organización para prevenir su recurrencia mediante la mejora continua.

## 12.2 Alcance

Este procedimiento aplica a todos los incidentes relacionados con:

### Seguridad Física

- Robo.
- Intrusión.
- Vandalismo.
- Daños a instalaciones.
- Pérdida de activos.

### Seguridad Informática

- Malware.
- Ransomware.
- Phishing.
- Fuga de información.
- Accesos no autorizados.
- Caída de servidores.
- Ataques de red.

### Seguridad Operacional

- Daños durante instalaciones.
- Accidentes.
- Errores técnicos.
- Fallas de equipos.
- Interrupción de servicios.

---

### Seguridad de la Información

- Pérdida de documentos.
- Divulgación no autorizada.
- Eliminación accidental de información.
- Manipulación de bases de datos.

---

### Continuidad del Negocio

- Fallas eléctricas.
- Desastres naturales.
- Interrupciones de Internet.
- Indisponibilidad de proveedores.
- Emergencias sanitarias.

---

# 12.3 Clasificación de Incidentes

Los incidentes serán clasificados de acuerdo con su gravedad:

### Nivel 1 – Bajo

Incidentes sin impacto significativo en la operación.

Ejemplos:

- Daño menor a herramienta.
- Error administrativo corregido inmediatamente.
- Acceso fallido sin compromiso de seguridad.

---

### Nivel 2 – Medio

Incidentes que afectan parcialmente un proceso.

Ejemplos:

- Falla temporal de un servidor.
- Retraso importante en una entrega.
- Pérdida de un equipo de bajo valor.

---

### Nivel 3 – Alto

Incidentes que afectan varios procesos o generan pérdidas relevantes.

Ejemplos:

- Robo de equipos.
- Ataque de ransomware contenido.
- Daños importantes a instalaciones.
- Fuga de información no crítica.

---

### Nivel 4 – Crítico

Incidentes que comprometen la continuidad del negocio.

Ejemplos:

- Incendio en instalaciones.
- Ciberataque masivo.
- Pérdida de información crítica.
- Interrupción total de operaciones.
- Robo de servidores o bases de datos.

---

# 12.4 Proceso de Gestión de Incidentes

## Etapa 1. Detección

Los incidentes pueden detectarse mediante:

- Colaboradores.
- Clientes.
- Sistemas de monitoreo.
- CCTV.
- Alarmas.
- Auditorías.
- Herramientas de ciberseguridad.
- Proveedores.

Todo incidente deberá reportarse inmediatamente al responsable designado.

---

## Etapa 2. Registro

Se abrirá un expediente que incluirá:

- Fecha y hora.
- Lugar.
- Persona que reporta.
- Tipo de incidente.
- Descripción detallada.
- Activos afectados.
- Evidencias disponibles.
- Nivel de criticidad.
- Responsable de la atención.

---

## Etapa 3. Contención

Se implementarán acciones inmediatas para evitar la propagación del incidente.

Ejemplos:

- Aislar equipos comprometidos.
- Suspender accesos.
- Recuperar mercancía.
- Evacuar instalaciones.
- Bloquear cuentas de usuario.
- Activar sistemas de respaldo.

---

## Etapa 4. Investigación

La investigación deberá determinar:

- Qué ocurrió.
- Cuándo ocurrió.
- Dónde ocurrió.
- Quién estuvo involucrado.
- Cómo ocurrió.
- Por qué ocurrió.
- Qué controles fallaron.
- Qué impacto tuvo.

Se recopilarán evidencias documentales, fotográficas, electrónicas y testimoniales.

---

## Etapa 5. Recuperación

Una vez controlado el incidente se procederá a:

- Restaurar servicios.
- Recuperar información desde respaldos.
- Reparar infraestructura.
- Validar la integridad de los sistemas.
- Reanudar operaciones de forma controlada.

---

## Etapa 6. Cierre

El cierre del incidente incluirá:

- Informe final.
- Acciones correctivas implementadas.
- Acciones preventivas.
- Lecciones aprendidas.
- Validación de la eficacia de las medidas adoptadas.

---

# 12.5 Comunicación del Incidente

Dependiendo de la gravedad, se informará a:

- Dirección General.

- Cliente afectado.
- Fabricante.
- Proveedor.
- Compañía de seguros.
- Autoridades competentes, cuando aplique.
- Titulares de datos personales, si existe una obligación legal o contractual.

Toda comunicación deberá ser clara, oportuna y autorizada por la Dirección.

---

# 12.6 Conservación de Evidencias

Para facilitar las investigaciones, toda evidencia deberá preservarse adecuadamente:

- Fotografías.
- Videos de CCTV.
- Registros de acceso.
- Bitácoras.
- Correos electrónicos.
- Archivos de registro (logs).
- Reportes técnicos.
- Declaraciones del personal.
- Documentación contractual.

La evidencia será almacenada de forma segura y con acceso restringido para garantizar su integridad.

---

# 12.7 Acciones Correctivas y Preventivas

Una vez concluida la investigación, se establecerán acciones para eliminar la causa raíz del incidente y evitar su repetición. Estas acciones podrán incluir:

- Actualización de procedimientos.
- Refuerzo de controles físicos o tecnológicos.
- Capacitación adicional al personal.
- Modificación de configuraciones de seguridad.
- Sustitución de equipos o infraestructura.
- Revisión de contratos con proveedores.
- Incremento del monitoreo de procesos críticos.

Cada acción deberá contar con un responsable, un plazo de implementación y un mecanismo para verificar su eficacia.

---

## 12.8 Indicadores de Desempeño (KPIs)

La organización evaluará el desempeño de la gestión de incidentes mediante indicadores como:

- Número total de incidentes registrados por periodo.
- Tiempo promedio de detección.
- Tiempo promedio de respuesta.
- Tiempo promedio de recuperación (MTTR).
- Porcentaje de incidentes resueltos dentro del tiempo objetivo.
- Número de incidentes repetitivos.
- Porcentaje de acciones correctivas implementadas en tiempo.
- Pérdidas económicas asociadas a incidentes.
- Disponibilidad de los sistemas críticos.
- Nivel de satisfacción del cliente respecto a la atención de incidentes.

La revisión periódica de estos indicadores permitirá a Q MAS IT S. fortalecer su capacidad de respuesta, mejorar sus controles y aumentar la resiliencia de sus operaciones frente a riesgos futuros.

# 13. Capacitación, Concientización y Desarrollo de Competencias en Seguridad del Negocio

## 13.1 Objetivo

El presente capítulo tiene como objetivo establecer los lineamientos para asegurar que todos los colaboradores de **Q MAS IT S. de R.L. de C.V.** cuenten con los conocimientos, habilidades, competencias y actitudes necesarias para desempeñar sus funciones de manera segura, ética y eficiente, contribuyendo a la protección de los activos de la organización, la continuidad del negocio y el cumplimiento de los requisitos legales, contractuales y normativos.

La empresa reconoce que la capacitación continua es uno de los controles preventivos más eficaces para reducir incidentes, minimizar errores operativos, fortalecer la cultura organizacional y mejorar la capacidad de respuesta ante situaciones de riesgo.

La formación del personal deberá orientarse no sólo al desarrollo técnico, sino también al fortalecimiento de una cultura de seguridad basada en la prevención, la responsabilidad y la mejora continua.

---

# 13.2 Alcance

Este programa aplica a:

- Dirección General.
- Gerencias.
- Coordinadores.
- Personal administrativo.
- Personal de ventas.
- Personal de compras.
- Técnicos de soporte.
- Ingenieros de proyectos.
- Técnicos de reparación.
- Personal de almacén.
- Personal de logística.
- Personal de garantías.
- Contratistas.
- Proveedores críticos cuando así lo establezcan los contratos.
- Personal de nuevo ingreso.
- Personal temporal.

---

# 13.3 Política de Capacitación

Q MAS IT S. se compromete a:

- Garantizar que el 100 % del personal reciba capacitación relacionada con la seguridad del negocio.
- Evaluar periódicamente las competencias del personal.
- Actualizar los contenidos conforme evolucionen los riesgos tecnológicos y operativos.
- Mantener registros documentados de todas las actividades de capacitación.
- Fomentar una cultura de aprendizaje continuo.
- Promover certificaciones técnicas y profesionales que aporten valor al negocio.

---

# 13.4 Detección de Necesidades de Capacitación (DNC)

Anualmente se realizará un análisis para identificar las necesidades de capacitación considerando:

**Cambios organizacionales**

- Nuevos procesos.
- Nuevos servicios.
- Reestructuración organizacional.

**Cambios tecnológicos**

- Nuevos equipos.
- Nuevos sistemas.
- Plataformas SaaS.
- Infraestructura de red.
- Soluciones de ciberseguridad.

**Cambios legales**

- Reformas legales.
- Nuevas NOM.
- Requisitos de clientes.
- Normas internacionales.

**Resultados operativos**

- Accidentes.
- Incidentes.
- Hallazgos de auditoría.
- Errores recurrentes.
- Reclamaciones de clientes.

---

# 13.5 Programa Anual de Capacitación

El programa anual incluirá, entre otros, los siguientes temas:

## Seguridad del Negocio

- Política de Seguridad del Negocio.
- Gestión de riesgos.
- Continuidad del negocio.
- Gestión de incidentes.
- Protección de activos.

---

## Seguridad Física

- Control de accesos.
- Protección del almacén.
- Seguridad en campo.
- Transporte seguro.
- Respuesta a emergencias.

---

## Seguridad Informática

- Ciberseguridad.
- Phishing.
- Ingeniería social.
- Protección de contraseñas.
- Uso seguro del correo electrónico.
- Manejo seguro de dispositivos móviles.
- Clasificación de la información.
- Uso de VPN.
- Respaldo de información.

---

## Protección de Datos

- Datos personales.
- Información confidencial.
- Clasificación documental.
- Manejo seguro de expedientes.
- Eliminación segura de información.

---

## Ética Empresarial

- Código de Ética.
- Prevención del fraude.
- Prevención del soborno.
- Conflictos de interés.
- Canal de denuncias.

---

## Seguridad Operacional

- Trabajo seguro en instalaciones del cliente.
- Manejo de herramientas.
- Transporte de equipos.
- Protección de activos.
- Gestión documental.

---

## Continuidad del Negocio

- Plan de Continuidad del Negocio (BCP).
- Plan de Recuperación ante Desastres (DRP).
- Recuperación de información.
- Manejo de contingencias.

---

# 13.6 Modalidades de Capacitación

La empresa podrá impartir capacitación mediante:

### Presencial

Cursos impartidos en las instalaciones de la empresa o del cliente.

---

### Virtual

Mediante plataformas de capacitación en línea.

---

### Autoaprendizaje

Materiales digitales.

Manual del colaborador.

Videos.

Procedimientos.

---

### Entrenamiento en Campo

Capacitación práctica durante la ejecución de proyectos.

---

### Simulacros

Ejercicios prácticos relacionados con:

- Evacuación.
- Incendios.
- Ataques informáticos.
- Recuperación de información.
- Continuidad operativa.
- Atención de incidentes.

---

# 13.7 Evaluación de la Competencia

La eficacia de la capacitación será evaluada mediante:

## Evaluaciones Teóricas

- Exámenes escritos.
- Cuestionarios.
- Entrevistas.

---

## Evaluaciones Prácticas

- Observación en campo.

- Ejercicios.
- Simulaciones.
- Casos prácticos.

---

## Indicadores

- Calificación promedio.
- Número de capacitaciones.
- Horas de capacitación por colaborador.
- Porcentaje de aprobación.
- Reducción de incidentes.
- Cumplimiento del programa anual.

---

# 13.8 Registros

La empresa conservará registros que incluyan:

- Programa anual.
- Lista de asistencia.
- Evaluaciones.
- Constancias.
- Certificados.
- Evidencias fotográficas.
- Resultados.
- Competencias adquiridas.

Estos registros serán administrados por Recursos Humanos y estarán disponibles para auditorías internas y externas.

---

# 13.9 Responsabilidades

## Dirección General

- Aprobar el programa anual.
- Asignar presupuesto.
- Revisar resultados.

## Recursos Humanos

- Coordinar las capacitaciones.
- Mantener registros.
- Evaluar indicadores.
- Gestionar instructores.

---

## Responsables de Área

- Identificar necesidades.
- Supervisar la participación.
- Evaluar el desempeño.

---

## Colaboradores

- Asistir puntualmente.
- Participar activamente.
- Aplicar los conocimientos adquiridos.
- Cumplir con las evaluaciones.

---

# 13.10 Indicadores de Desempeño (KPIs)

La empresa evaluará, como mínimo, los siguientes indicadores:

- % de cumplimiento del Programa Anual de Capacitación.
- % de colaboradores capacitados.
- Horas promedio de capacitación por colaborador.
- % de aprobación en evaluaciones.
- Número de incidentes atribuibles a falta de capacitación.
- Número de simulacros realizados.
- % de acciones de mejora implementadas derivadas de evaluaciones.
- Índice de satisfacción de los participantes.

---

# 14. Cumplimiento Legal, Normativo y Contractual

## 14.1 Objetivo

El objetivo de este capítulo es establecer los lineamientos que permitan garantizar que todas las actividades desarrolladas por **Q MAS IT S. de R.L. de C.V.** se ejecuten en estricto apego a la legislación vigente, las normas aplicables, los requisitos contractuales adquiridos con clientes y proveedores, así como las políticas internas de la organización.

El cumplimiento legal constituye uno de los pilares fundamentales de la seguridad del negocio, ya que reduce riesgos de sanciones, pérdidas económicas, incumplimientos contractuales, daños reputacionales y afectaciones a la continuidad de las operaciones.

La empresa se compromete a identificar, evaluar y cumplir de manera permanente con todas las obligaciones que le resulten aplicables conforme a su giro comercial y de servicios tecnológicos.

---

# 14.2 Alcance

Este apartado aplica a todos los procesos de la empresa, incluyendo:

- Dirección General.
- Administración.
- Recursos Humanos.
- Finanzas.
- Compras.
- Ventas.
- Logística.
- Almacén.
- Soporte Técnico.
- Ingeniería.
- Garantías.
- Tecnología de la Información.
- Servicios en campo.
- Contratistas.
- Proveedores.

---

# 14.3 Marco Legal Aplicable

Sin limitarse a ellas, Q MAS IT S. observará el cumplimiento de las siguientes disposiciones cuando sean aplicables a sus operaciones:

## Legislación Laboral

- Constitución Política de los Estados Unidos Mexicanos.
- Ley Federal del Trabajo.
- Reglamento Federal de Seguridad y Salud en el Trabajo.

---

## Seguridad y Salud

- NOM-STPS aplicables.
- Programas de Protección Civil.
- Reglamentos municipales.

---

## Protección de Datos

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Reglamento correspondiente.
- Aviso de Privacidad.

---

## Comercio

- Código de Comercio.
- Ley General de Sociedades Mercantiles.
- Legislación fiscal vigente.
- Normatividad aduanera cuando aplique.

---

## Tecnologías de Información

- Licenciamiento de software.
- Derechos de autor.
- Propiedad intelectual.
- Contratos de uso de plataformas.

---

## Medio Ambiente

Cuando las actividades lo requieran, la empresa observará la legislación ambiental aplicable para la correcta gestión de residuos electrónicos, baterías, componentes y materiales derivados de sus operaciones.

---

# 14.4 Identificación de Requisitos

La empresa mantendrá una **Matriz de Requisitos Legales y Contractuales** que contendrá, como mínimo:

- Disposición legal o contractual.
- Autoridad emisora.
- Área responsable.
- Obligaciones específicas.
- Evidencias de cumplimiento.
- Periodicidad de revisión.
- Estado de cumplimiento.

Esta matriz será revisada al menos una vez al año o cuando exista un cambio relevante en la legislación o en los contratos.

---

# 14.5 Cumplimiento Contractual

Todos los contratos celebrados con clientes, proveedores y socios comerciales deberán revisarse antes de su firma para identificar obligaciones relacionadas con:

- Niveles de servicio (SLA).
- Confidencialidad.
- Protección de datos.
- Propiedad intelectual.
- Seguridad de la información.
- Continuidad del servicio.
- Garantías.
- Tiempos de respuesta.
- Penalizaciones.
- Requisitos de acceso a instalaciones del cliente.

Las áreas responsables deberán asegurar el cumplimiento de cada obligación durante la ejecución del contrato.

## 14.6 Gestión de Licencias, Permisos y Certificaciones

La organización mantendrá vigentes todas las licencias, permisos y certificaciones requeridas para el desarrollo de sus actividades.

Cuando aplique, se dará seguimiento a:

- Licencias de software.
- Certificaciones técnicas del personal.
- Certificaciones de fabricantes.
- Permisos municipales.
- Seguros.
- Registros fiscales.
- Documentación laboral.

Se llevará un calendario de vencimientos para evitar incumplimientos por falta de renovación.

---

## 14.7 Auditorías de Cumplimiento

Periódicamente se realizarán auditorías internas y, cuando corresponda, auditorías externas para verificar el cumplimiento de:

- Legislación aplicable.
- Políticas internas.
- Contratos.
- Procedimientos.
- Requisitos de clientes.
- Controles de seguridad.

Los hallazgos deberán registrarse, analizarse y atenderse mediante acciones correctivas y preventivas.

---

## 14.8 Gestión de Incumplimientos

Cuando se detecte un incumplimiento legal o contractual, se deberá:

1. Registrar el incumplimiento.
2. Evaluar el riesgo asociado.
3. Informar a la Dirección General.
4. Implementar acciones inmediatas para contener el impacto.
5. Analizar la causa raíz.
6. Definir acciones correctivas y preventivas.
7. Dar seguimiento hasta verificar su eficacia.
8. Documentar el cierre del caso.

En caso de que el incumplimiento pueda afectar a un cliente o generar una obligación de notificación a una autoridad, la Dirección determinará las acciones correspondientes conforme a la legislación y a los compromisos contractuales aplicables.

---

# 14.9 Responsabilidades

### Dirección General

- Aprobar la política de cumplimiento.
- Asignar recursos.
- Revisar los resultados de auditorías y cumplimiento.

### Responsables de Área

- Identificar las obligaciones aplicables a sus procesos.
- Mantener evidencia documental del cumplimiento.
- Implementar acciones correctivas cuando sea necesario.

### Recursos Humanos

- Asegurar el cumplimiento de obligaciones laborales.
- Mantener expedientes del personal.
- Coordinar la capacitación en materia legal y de cumplimiento.

### Área de Tecnologías de la Información

- Administrar licencias de software.
- Garantizar el cumplimiento de las políticas de seguridad informática.
- Mantener controles sobre el uso de sistemas y activos tecnológicos.

### Colaboradores

- Conocer y cumplir las disposiciones legales, normativas y contractuales aplicables a sus funciones.

- Reportar cualquier incumplimiento detectado.
- Participar en las actividades de capacitación relacionadas con el cumplimiento.

---

## 14.10 Indicadores de Cumplimiento (KPIs)

Para evaluar la eficacia del sistema de cumplimiento, la empresa establecerá indicadores como:

- Porcentaje de requisitos legales identificados y actualizados.
- Porcentaje de cumplimiento de obligaciones legales.
- Número de incumplimientos legales detectados.
- Número de incumplimientos contractuales.
- Tiempo promedio de atención de hallazgos.
- Porcentaje de licencias y certificaciones vigentes.
- Porcentaje de auditorías ejecutadas conforme al programa.
- Número de sanciones o multas recibidas.
- Porcentaje de acciones correctivas cerradas en el plazo establecido.
- Nivel de satisfacción de los clientes respecto al cumplimiento de los acuerdos contractuales.

La revisión periódica de estos indicadores permitirá a Q MAS IT S. fortalecer su sistema de cumplimiento, reducir riesgos regulatorios y contractuales, y demostrar ante clientes, autoridades y partes interesadas el compromiso permanente de la organización con la legalidad, la ética y la excelencia operativa.

# 15. Mejora Continua del Sistema de Seguridad del Negocio

## 15.1 Objetivo

El objetivo de este capítulo es establecer los lineamientos para asegurar la mejora continua del **Sistema de Gestión de Seguridad del Negocio (SGSN)** de **Q MAS IT S. de R.L. de C.V.**, mediante la evaluación permanente del desempeño, la identificación de oportunidades de mejora, el análisis de riesgos emergentes, la implementación de acciones correctivas y preventivas y la revisión periódica de los procesos.

La mejora continua es un principio fundamental para garantizar que el Sistema de Seguridad del Negocio permanezca vigente, eficaz y alineado con:

- Los objetivos estratégicos de la organización.
- Los cambios tecnológicos.
- Las necesidades de los clientes.

- La evolución de las amenazas físicas y cibernéticas.
- Los requisitos legales y contractuales.
- Las mejores prácticas internacionales en materia de gestión de riesgos y seguridad.

La Dirección General considera la mejora continua como una actividad permanente que permite fortalecer la resiliencia organizacional y mantener la competitividad de la empresa.

---

# 15.2 Alcance

La mejora continua aplica a todos los procesos, áreas y actividades desarrolladas por **Q MAS IT S. de R.L. de C.V.**, incluyendo:

- Dirección General.
- Administración.
- Recursos Humanos.
- Compras.
- Ventas.
- Logística.
- Almacén.
- Ingeniería.
- Servicios Técnicos.
- Garantías.
- Tecnologías de la Información.
- Seguridad Informática.
- Atención al Cliente.
- Finanzas.
- Proyectos.
- Servicios en campo.
- Gestión documental.
- Proveedores críticos.

---

# 15.3 Principios de la Mejora Continua

La empresa desarrollará la mejora continua bajo los siguientes principios:

- Liderazgo de la Alta Dirección.
- Participación activa de todo el personal.
- Enfoque basado en riesgos.
- Toma de decisiones sustentada en evidencia.
- Aprendizaje organizacional.

- Innovación tecnológica.
- Prevención antes que corrección.
- Transparencia.
- Medición objetiva del desempeño.
- Satisfacción del cliente.

---

# 15.4 Ciclo de Mejora Continua (PHVA)

El Sistema de Seguridad del Negocio se desarrollará bajo la metodología **Planear – Hacer – Verificar – Actuar (PHVA)**.

## PLANEAR

Consiste en:

- Identificar riesgos.
- Definir objetivos.
- Establecer políticas.
- Elaborar procedimientos.
- Asignar recursos.
- Diseñar controles.
- Definir indicadores.

---

## HACER

Implica:

- Implementar controles.
- Ejecutar procedimientos.
- Capacitar al personal.
- Administrar riesgos.
- Proteger activos.
- Operar los procesos.
- Atender incidentes.

---

## VERIFICAR

Incluye:

- Auditorías.
- Inspecciones.
- Indicadores.
- Revisión documental.
- Seguimiento de objetivos.
- Evaluación del cumplimiento legal.
- Evaluación del desempeño.

---

## ACTUAR

Comprende:

- Acciones correctivas.
- Acciones preventivas.
- Actualización de políticas.
- Revisión de procedimientos.
- Nuevos controles.
- Mejoras tecnológicas.
- Capacitación adicional.

---

# 15.5 Fuentes de Mejora

La organización identificará oportunidades de mejora mediante:

## Auditorías

- Auditorías internas.
- Auditorías externas.
- Auditorías de clientes.
- Auditorías de fabricantes.

---

## Incidentes

Toda investigación deberá identificar oportunidades para mejorar procesos y controles.

---

## Quejas de Clientes

Se analizarán:

- Reclamos.
- Retrabajos.
- Incumplimientos.
- Observaciones.
- Encuestas de satisfacción.

---

## Indicadores

Se evaluarán:

- Tendencias.
- Variaciones.
- Desviaciones.
- Incumplimientos.
- Riesgos emergentes.

---

## Cambios Tecnológicos

La empresa evaluará continuamente nuevas tecnologías relacionadas con:

- Ciberseguridad.
- Videovigilancia.
- Control de acceso.
- Protección de información.
- Automatización.
- Inteligencia Artificial aplicada a la seguridad.

---

# 15.6 Gestión de Acciones Correctivas

Cuando se detecte una desviación, deberá implementarse el siguiente proceso:

**Paso 1**

Registrar la no conformidad.

**Paso 2**

Evaluar el impacto.

---

**Paso 3**

Analizar la causa raíz utilizando herramientas como:

- Diagrama de Ishikawa.
- 5 ¿Por qué?
- Árbol de causas.
- AMEF cuando sea necesario.

---

**Paso 4**

Definir acciones correctivas.

---

**Paso 5**

Asignar responsables.

---

**Paso 6**

Definir fechas compromiso.

---

**Paso 7**

Verificar la eficacia.

---

**Paso 8**

Cerrar formalmente la acción.

---

# 15.7 Gestión de Acciones Preventivas

Además de corregir problemas existentes, la empresa desarrollará acciones preventivas mediante:

- Evaluaciones de riesgo.
- Inspecciones.
- Observaciones de comportamiento.
- Revisión de indicadores.
- Cambios tecnológicos.
- Recomendaciones de auditoría.
- Lecciones aprendidas.

El objetivo será eliminar causas potenciales antes de que generen incidentes.

---

# 15.8 Innovación Tecnológica

Q MAS IT S. promoverá la incorporación de nuevas tecnologías que incrementen la seguridad del negocio.

Entre ellas:

- Sistemas de monitoreo remoto.
- Inteligencia Artificial.
- Plataformas de gestión de activos.
- Herramientas SIEM.
- EDR/XDR.
- Plataformas de respaldo.
- Automatización de procesos.
- Plataformas SaaS.
- Sistemas biométricos.
- Reconocimiento de placas vehiculares.
- Plataformas de gestión documental.

Toda nueva tecnología deberá evaluarse considerando:

- Riesgos.
- Beneficios.
- Compatibilidad.

- Costo-beneficio.
- Impacto operativo.

---

# 15.9 Gestión del Cambio

Todo cambio significativo deberá evaluarse previamente.

Esto incluye:

- Cambios organizacionales.
- Nuevos servicios.
- Nuevos clientes.
- Nuevos proveedores.
- Nuevas tecnologías.
- Cambios regulatorios.
- Cambios de infraestructura.
- Reubicación de instalaciones.

Antes de implementarse deberán evaluarse:

- Riesgos.
- Recursos.
- Capacitación requerida.
- Impacto en procesos.
- Controles necesarios.

---

# 15.10 Revisión por la Dirección

Al menos una vez por año la Dirección General revisará el desempeño del Sistema de Seguridad del Negocio considerando:

**Entradas**

- Resultados de auditorías.
- Incidentes.
- Riesgos.
- Indicadores.
- Cumplimiento legal.
- Retroalimentación de clientes.
- Estado de acciones correctivas.

- Cambios organizacionales.
- Nuevas amenazas.

**Salidas**

- Nuevos objetivos.
- Recursos.
- Cambios de política.
- Nuevos controles.
- Actualización de procedimientos.
- Proyectos de mejora.
- Programas de capacitación.

---

# 15.11 Indicadores de Mejora Continua

Como mínimo se monitorearán los siguientes indicadores:

- % de objetivos cumplidos.
- % de acciones correctivas cerradas.
- % de acciones preventivas implementadas.
- Número de incidentes repetitivos.
- Tiempo promedio de cierre de no conformidades.
- Nivel de satisfacción del cliente.
- Cumplimiento del programa de auditorías.
- Disponibilidad de los servicios críticos.
- Madurez del Sistema de Seguridad del Negocio.
- Nivel de cumplimiento del Plan de Mejora.

---

# 15.12 Beneficios Esperados

La mejora continua permitirá:

- Incrementar la resiliencia del negocio.
- Reducir incidentes.
- Mejorar la eficiencia operativa.
- Fortalecer la satisfacción del cliente.
- Reducir costos por fallas.
- Incrementar la competitividad.
- Adaptarse rápidamente a nuevas amenazas.
- Optimizar los procesos internos.

- Proteger mejor los activos de la organización.

---

# 16. Roles, Responsabilidades y Autoridades

## 16.1 Objetivo

El presente capítulo establece las funciones, responsabilidades y niveles de autoridad de todas las personas que participan en la implementación, operación, mantenimiento y mejora del **Sistema de Seguridad del Negocio** de **Q MAS IT S. de R.L. de C.V.**

La correcta definición de responsabilidades garantiza una adecuada coordinación entre las áreas de la organización, fortalece la toma de decisiones y asegura que los controles de seguridad sean aplicados de forma consistente en todos los procesos.

Cada colaborador es responsable de la seguridad dentro del ámbito de sus funciones y deberá actuar conforme a esta política, los procedimientos internos y la legislación aplicable.

---

# 16.2 Estructura Organizacional

Para efectos de esta política, las principales responsabilidades recaen en:

- Dirección General.
- Gerencias y Coordinaciones.
- Responsables de Área.
- Personal Administrativo.
- Personal Técnico.
- Área de Tecnologías de la Información.
- Recursos Humanos.
- Compras.
- Almacén.
- Logística.
- Personal de Campo.
- Todos los colaboradores.
- Contratistas y proveedores.

---

## 16.3 Responsabilidades de la Dirección General

La Dirección General es la máxima autoridad del Sistema de Seguridad del Negocio y será responsable de:

- Aprobar la Política de Seguridad del Negocio.
- Definir la estrategia de seguridad.
- Asignar recursos humanos, tecnológicos y financieros.
- Aprobar objetivos e indicadores.
- Revisar el desempeño del sistema.
- Promover la cultura de seguridad.
- Autorizar proyectos de mejora.
- Tomar decisiones ante incidentes críticos.
- Aprobar planes de continuidad del negocio.
- Representar a la organización ante clientes y autoridades en asuntos relacionados con la seguridad del negocio.

---

## 16.4 Responsabilidades de los Responsables de Área

Cada responsable de área deberá:

- Implementar esta política en su proceso.
- Identificar riesgos.
- Supervisar el cumplimiento de procedimientos.
- Reportar incidentes.
- Gestionar acciones correctivas.
- Evaluar indicadores.
- Proponer mejoras.
- Capacitar a su personal.
- Verificar el cumplimiento de los controles de seguridad.

---

## 16.5 Responsabilidades del Área de Tecnologías de la Información

El área de TI será responsable de:

- Administrar la infraestructura tecnológica.
- Gestionar usuarios y accesos.
- Implementar controles de ciberseguridad.
- Administrar respaldos.
- Mantener servidores.
- Gestionar redes.
- Supervisar el monitoreo de seguridad.
- Atender incidentes informáticos.
- Garantizar la disponibilidad de los servicios tecnológicos.
- Controlar licencias de software.

---

# 16.6 Responsabilidades del Área de Recursos Humanos

Recursos Humanos deberá:

- Coordinar programas de capacitación.
- Mantener expedientes del personal.
- Gestionar la inducción de nuevos colaboradores.
- Promover la cultura organizacional.
- Administrar evaluaciones de desempeño.
- Coordinar campañas de concientización.
- Asegurar que el personal conozca las políticas de seguridad.

---

# 16.7 Responsabilidades del Área de Compras

El área de Compras deberá:

- Seleccionar proveedores confiables.
- Verificar requisitos legales y contractuales.
- Supervisar el desempeño de proveedores.
- Garantizar compras transparentes.
- Mantener evidencia documental.
- Gestionar contratos con proveedores.

---

# 16.8 Responsabilidades del Área de Almacén

El responsable del almacén deberá:

- Custodiar los inventarios.
- Controlar entradas y salidas.
- Realizar inventarios físicos.
- Proteger los activos.
- Reportar diferencias.
- Supervisar condiciones de almacenamiento.
- Mantener la trazabilidad de los equipos.

---

# 16.9 Responsabilidades del Personal Técnico

Los ingenieros y técnicos deberán:

- Cumplir procedimientos.
- Utilizar herramientas autorizadas.
- Proteger los equipos del cliente.
- Mantener la confidencialidad.
- Reportar incidentes.
- Documentar servicios.
- Respetar normas de seguridad.
- Verificar la correcta operación de los equipos intervenidos.
- Resguardar adecuadamente las herramientas y materiales asignados.

---

# 16.10 Responsabilidades de Todo el Personal

Independientemente del puesto, cada colaborador deberá:

- Cumplir esta política.
- Participar en capacitaciones.
- Reportar riesgos.
- Proteger activos.
- Mantener confidencialidad.
- Actuar con ética.
- Cumplir procedimientos.
- Colaborar en auditorías.
- Participar en simulacros.

- Apoyar las investigaciones de incidentes cuando sea requerido.

---

# 16.11 Responsabilidades de Proveedores y Contratistas

Los proveedores deberán:

- Cumplir los requisitos de seguridad establecidos por la empresa.
- Respetar la confidencialidad.
- Proteger la información.
- Cumplir contratos.
- Reportar incidentes.
- Permitir auditorías cuando así se establezca contractualmente.
- Garantizar la seguridad de los bienes y servicios suministrados.

---

# 16.12 Autoridad para la Toma de Decisiones

La Dirección General tendrá la autoridad para:

- Aprobar excepciones a esta política.
- Suspender operaciones cuando exista un riesgo grave.
- Autorizar inversiones en seguridad.
- Declarar la activación del Plan de Continuidad del Negocio.
- Aprobar acciones extraordinarias derivadas de incidentes críticos.
- Designar responsables para la atención de emergencias o investigaciones.

Los responsables de área podrán tomar decisiones operativas dentro de su ámbito de competencia, siempre que estas sean consistentes con la presente política y no comprometan la seguridad del negocio.

---

# 16.13 Comunicación de Responsabilidades

Las responsabilidades definidas en este capítulo deberán comunicarse a todo el personal mediante:

- Inducción a nuevos colaboradores.
- Manuales y procedimientos internos.

- Reuniones de trabajo.
- Programas de capacitación.
- Publicación en los medios internos de comunicación.
- Actualizaciones cuando existan cambios organizacionales.

Cada colaborador deberá conocer claramente su función dentro del Sistema de Seguridad del Negocio y comprender cómo sus actividades contribuyen a la protección de la organización y al cumplimiento de los objetivos estratégicos.

# 17. Incumplimiento de la Política de Seguridad del Negocio, Régimen Disciplinario y Acciones Correctivas

## 17.1 Objetivo

El presente capítulo tiene como finalidad establecer los lineamientos para la atención, investigación y tratamiento de cualquier incumplimiento a la **Política de Seguridad del Negocio** de **Q MAS IT S. de R.L. de C.V.**, garantizando que todas las desviaciones sean tratadas de manera objetiva, imparcial, documentada y conforme a la legislación vigente.

La organización reconoce que el incumplimiento de las políticas de seguridad puede comprometer la integridad de las personas, afectar la continuidad de las operaciones, ocasionar pérdidas económicas, generar incumplimientos contractuales, dañar la reputación corporativa y poner en riesgo la información de clientes y proveedores.

Por ello, la empresa establece un sistema disciplinario basado en la prevención, la investigación objetiva, la proporcionalidad de las sanciones y la mejora continua.

---

# 17.2 Alcance

Las disposiciones del presente capítulo aplican a:

- Dirección General.
- Personal administrativo.
- Ingenieros.
- Técnicos.
- Personal de almacén.
- Personal de logística.
- Recursos Humanos.
- Compras.

- Contratistas.
- Proveedores.
- Consultores.
- Personal temporal.
- Prestadores de servicios.
- Cualquier persona que actúe en representación de Q MAS IT S.

---

# 17.3 Principios del Régimen Disciplinario

Toda actuación derivada de un incumplimiento deberá observar los siguientes principios:

### Legalidad

Toda medida disciplinaria deberá apegarse a la legislación laboral vigente, al Reglamento Interior de Trabajo y a los contratos celebrados con colaboradores, proveedores o contratistas.

### Imparcialidad

Las investigaciones se realizarán sin prejuicios ni favoritismos, garantizando la objetividad y el derecho de audiencia de las personas involucradas.

### Confidencialidad

La información relacionada con investigaciones será tratada como confidencial y sólo será compartida con las personas autorizadas.

### Proporcionalidad

Las medidas disciplinarias serán acordes con la gravedad de la falta, el impacto ocasionado y los antecedentes del responsable.

### Trazabilidad

Todo incumplimiento deberá quedar documentado desde su detección hasta el cierre del caso, conservando la evidencia correspondiente.

### Mejora Continua

Cada incumplimiento será analizado para identificar oportunidades de mejora en los procesos, procedimientos o controles existentes.

---

# 17.4 Clasificación de Incumplimientos

Para efectos de esta política, los incumplimientos se clasifican en cuatro niveles.

## Nivel I – Incumplimientos Leves

Son aquellos que no generan afectaciones significativas a la operación ni comprometen la seguridad del negocio.

Ejemplos:

- No portar gafete institucional.
- Retraso en el registro de actividades.
- Omisión de procedimientos administrativos menores.
- Falta de actualización de registros internos.
- Descuidos sin consecuencias operativas.

---

## Nivel II – Incumplimientos Moderados

Aquellos que afectan parcialmente los procesos o generan riesgos controlables.

Ejemplos:

- No seguir procedimientos establecidos.
- Uso inadecuado de herramientas.
- Incumplimiento de controles documentales.
- No realizar respaldos conforme al procedimiento.
- Accesos indebidos por negligencia.

---

## Nivel III – Incumplimientos Graves

Conductas que generan pérdidas económicas, riesgos importantes o incumplimientos contractuales.

Ejemplos:

- Daño a equipos del cliente por negligencia.
- Manipulación indebida de inventarios.
- Revelación de información confidencial.
- Desobediencia a instrucciones de seguridad.

- Reincidencia en faltas moderadas.

---

## Nivel IV – Incumplimientos Críticos

Aquellos que ponen en riesgo la continuidad del negocio o constituyen una conducta ilícita.

Ejemplos:

- Robo.
- Fraude.
- Soborno.
- Sabotaje.
- Manipulación intencional de información.
- Alteración de evidencias.
- Acceso deliberado a sistemas sin autorización.
- Sustracción de equipos.
- Violación deliberada de acuerdos de confidencialidad.

---

# 17.5 Detección del Incumplimiento

Los incumplimientos podrán detectarse mediante:

- Auditorías internas.
- Auditorías externas.
- Supervisión directa.
- Reportes de clientes.
- Denuncias.
- Sistemas de monitoreo.
- Videovigilancia.
- Revisiones documentales.
- Evaluaciones de desempeño.
- Herramientas de ciberseguridad.

Todo colaborador tiene la obligación de reportar cualquier incumplimiento del que tenga conocimiento.

---

# 17.6 Investigación

Toda investigación deberá seguir un proceso estructurado:

**Paso 1**

Recepción del reporte.

**Paso 2**

Registro del caso.

**Paso 3**

Designación del responsable de la investigación.

**Paso 4**

Recopilación de evidencias.

**Paso 5**

Entrevistas.

**Paso 6**

Análisis de la información.

**Paso 7**

Determinación de responsabilidades.

**Paso 8**

Emisión del informe final.

Durante el proceso se garantizará el derecho de audiencia de las personas involucradas y la confidencialidad de la información.

---

# 17.7 Medidas Disciplinarias

Dependiendo de la gravedad del incumplimiento, la empresa podrá aplicar una o varias de las siguientes medidas:

## Medidas Preventivas

- Reentrenamiento.
- Capacitación adicional.
- Supervisión reforzada.
- Actualización de procedimientos.

---

## Medidas Administrativas

- Llamado de atención verbal.
- Amonestación escrita.
- Suspensión temporal de actividades.
- Restricción de accesos.
- Cambio temporal de funciones.

---

## Medidas Contractuales

- Terminación de contratos con proveedores.
- Rescisión de contratos de prestación de servicios.
- Aplicación de penalizaciones previstas en los contratos.

---

## Medidas Legales

Cuando los hechos puedan constituir un delito o una infracción legal, la empresa podrá:

- Presentar denuncias ante las autoridades competentes.
- Reclamar daños y perjuicios.
- Ejercer las acciones legales que correspondan.

---

# 17.8 Acciones Correctivas y Preventivas

Una vez concluida la investigación, deberán establecerse acciones para evitar la repetición del incumplimiento, tales como:

- Modificación de procedimientos.
- Implementación de nuevos controles.
- Actualización de políticas.
- Capacitación específica.
- Adquisición de herramientas o tecnologías.
- Revisión de responsabilidades.
- Fortalecimiento de controles de acceso.
- Incremento de auditorías o supervisiones.

Cada acción deberá contar con un responsable, una fecha de implementación y un mecanismo para verificar su eficacia.

---

# 17.9 Gestión Documental

Todo expediente relacionado con un incumplimiento deberá contener, como mínimo:

- Reporte inicial.
- Evidencias.
- Declaraciones.
- Análisis de causa raíz.
- Informe de investigación.
- Medidas disciplinarias aplicadas.
- Acciones correctivas.
- Evidencia del cierre del caso.

Los expedientes serán resguardados conforme a la política de gestión documental y protección de datos personales.

---

# 17.10 Indicadores (KPIs)

La Dirección dará seguimiento, entre otros, a los siguientes indicadores:

- Número de incumplimientos por tipo.
- Incumplimientos por área.
- Tiempo promedio de investigación.
- Tiempo promedio de cierre.
- Reincidencia de incumplimientos.

- Porcentaje de acciones correctivas implementadas.
- Número de sanciones aplicadas.
- Tendencia anual de incumplimientos.
- Costos asociados a incumplimientos.
- Nivel de cumplimiento de la política.

Estos indicadores serán revisados periódicamente para fortalecer los controles internos y prevenir futuras desviaciones.

---

# 18. Vigencia, Revisión, Actualización y Aprobación de la Política

## 18.1 Objetivo

El presente capítulo establece los criterios para la entrada en vigor, administración, revisión, actualización, difusión y aprobación de la **Política de Seguridad del Negocio** de **Q MAS IT S. de R.L. de C.V.**, asegurando que el documento permanezca vigente, actualizado y alineado con la estrategia de la organización, los cambios regulatorios, los requisitos de los clientes y las mejores prácticas en materia de seguridad del negocio.

La empresa reconoce que la seguridad es un proceso dinámico y, por lo tanto, esta política deberá evolucionar conforme cambien las amenazas, los riesgos, la infraestructura tecnológica y las necesidades del negocio.

---

# 18.2 Entrada en Vigor

La presente política entrará en vigor a partir de la fecha de su aprobación por la Dirección General y será obligatoria para todas las personas comprendidas dentro de su alcance.

Desde ese momento, sustituirá cualquier política o lineamiento previo relacionado con la seguridad del negocio que resulte incompatible con este documento.

---

# 18.3 Difusión

Con el fin de asegurar su correcta implementación, la empresa comunicará esta política mediante:

- Inducción al personal de nuevo ingreso.
- Programas de capacitación.
- Reuniones internas.
- Publicación en la intranet o medios internos.
- Entrega digital o impresa.
- Sesiones de sensibilización.

Cada colaborador deberá confirmar que ha leído, comprendido y aceptado cumplir las disposiciones de la política, dejando evidencia de dicha aceptación cuando sea requerido.

---

# 18.4 Revisión Periódica

La política será revisada, como mínimo, una vez al año.

Adicionalmente, podrá revisarse cuando ocurra cualquiera de los siguientes eventos:

- Cambios en la legislación aplicable.
- Modificaciones en la estructura organizacional.
- Nuevos procesos o servicios.
- Cambios tecnológicos relevantes.
- Resultados de auditorías.
- Incidentes graves de seguridad.
- Requisitos de clientes o autoridades.
- Incorporación de nuevas sedes o centros de operación.
- Cambios significativos en el análisis de riesgos.

---

# 18.5 Actualización del Documento

Cuando se identifique la necesidad de modificar la política, se seguirá el siguiente proceso:

1. Identificación de la necesidad de cambio.
2. Elaboración de la propuesta de actualización.
3. Revisión técnica por las áreas involucradas.
4. Evaluación de impactos operativos, legales y tecnológicos.
5. Aprobación por la Dirección General.
6. Asignación de una nueva versión del documento.
7. Comunicación y difusión de los cambios.
8. Capacitación al personal cuando corresponda.
9. Resguardo de la versión anterior conforme al procedimiento de control documental.

# 18.6 Control de Versiones

La empresa mantendrá un historial de versiones que incluirá, como mínimo:

- Número de versión.
- Fecha de emisión.
- Fecha de revisión.
- Descripción de los cambios realizados.
- Responsable de la elaboración.
- Responsable de la revisión.
- Responsable de la aprobación.

Únicamente la versión vigente podrá utilizarse para fines operativos.

# 18.7 Conservación de Registros

Se conservarán como evidencia, entre otros:

- Versiones históricas de la política.
- Actas de aprobación.
- Registros de revisión.
- Evidencia de difusión.
- Listas de asistencia a capacitaciones relacionadas.
- Acuses de recibido por parte del personal.
- Registros de auditorías asociadas a la política.

Los registros se conservarán durante el tiempo establecido en la política de gestión documental de la empresa y conforme a los requisitos legales aplicables.

# 18.8 Aprobación

La presente **Política de Seguridad del Negocio** deberá ser aprobada formalmente por la Dirección General antes de su entrada en vigor.

La aprobación implica el compromiso de la Alta Dirección de:

- Proporcionar los recursos necesarios para su implementación.

- Promover una cultura organizacional de seguridad.
- Supervisar el cumplimiento de la política.
- Revisar periódicamente su eficacia.
- Impulsar la mejora continua del Sistema de Seguridad del Negocio.

---

# 18.9 Declaración de Compromiso de la Dirección

La Dirección General de **Q MAS IT S. de R.L. de C.V.** manifiesta su compromiso permanente con la protección de las personas, la información, los activos, la infraestructura tecnológica y la continuidad del negocio.

Asimismo, se compromete a:

- Liderar con el ejemplo en el cumplimiento de esta política.
- Promover una cultura basada en la ética, la transparencia y la prevención.
- Proporcionar los recursos humanos, tecnológicos y financieros necesarios para mantener un Sistema de Seguridad del Negocio eficaz.
- Revisar periódicamente la política para asegurar su vigencia y pertinencia.
- Fomentar la participación de todo el personal en la identificación de riesgos y oportunidades de mejora.
- Mantener una comunicación abierta con clientes, proveedores y demás partes interesadas en materia de seguridad del negocio.

La presente política refleja el compromiso institucional de **Q MAS IT S. de R.L. de C.V.** con la excelencia operativa, la protección de sus activos y la generación de confianza con sus clientes y socios comerciales.

---

# 18.10 Hoja de Aprobación

| Cargo | Nombre | Firma | Fecha |
|---|---|---|---|
| Director General | _____ | _____ | _____ |
| Responsable del Sistema de Seguridad del Negocio | _____ | _____ | _____ |
| Responsable de Tecnologías de la Información | _____ | _____ | _____ |
| Responsable de Recursos Humanos | _____ | _____ | _____ |

---

## Nota para una auditoría

Con el desarrollo de los **18 capítulos** que hemos elaborado, este documento tiene el nivel de detalle que normalmente se presenta como un **Manual de Política de Seguridad del Negocio** de aproximadamente **90 a 100 páginas**, adecuado para auditorías de clientes corporativos y alineado con buenas prácticas de gestión de riesgos y continuidad del negocio. Si posteriormente deseas certificarte en **ISO 28000 (Seguridad de la Cadena de Suministro)** o **ISO 22301 (Continuidad del Negocio)**, esta política puede utilizarse como documento base y complementarse con procedimientos específicos, formatos y registros.