Política de Seguridad Física y Seguridad Lógica

Q MAS IT S. de R.L. de C.V.

Código: POL-SI-002
Versión: 1.1
Fecha de emisión: Enero 2026
Elaboró: Dirección General
Revisión: Anual

1. Objetivo

1.1 Objetivo General

La presente Política de Seguridad Física y Seguridad Lógica tiene como finalidad establecer los principios, controles y lineamientos que permitan proteger de manera integral los activos de Q MAS IT S. de R.L. de C.V., garantizando la confidencialidad, integridad y disponibilidad de la información, así como la protección de las personas, las instalaciones, los equipos tecnológicos y la continuidad de las operaciones de la empresa.

Como organización dedicada a la comercialización de soluciones tecnológicas, integración de infraestructura de TI, reparación de equipos en garantía, soporte técnico e implementación de proyectos tecnológicos, Q MAS IT S. reconoce que la seguridad constituye un elemento estratégico para generar confianza en sus clientes y asegurar la prestación continua de sus servicios.

Esta política busca minimizar los riesgos derivados de amenazas internas y externas, tales como:

- Accesos físicos no autorizados.
- Robo o pérdida de equipos tecnológicos.
- Daños a la infraestructura.
- Manipulación indebida de información.
- Ataques informáticos.
- Fugas de información confidencial.
- Errores humanos.
- Sabotaje.
- Desastres naturales.
- Fallas eléctricas.
- Ciberataques.
- Uso indebido de los recursos tecnológicos.

Asimismo, esta política establece las responsabilidades de todo el personal respecto a la protección de los activos de información y de la infraestructura física de la empresa, fomentando una cultura organizacional basada en la prevención, la gestión del riesgo y la mejora continua.

La implementación de esta política permitirá que Q MAS IT S. de R.L. de C.V.:

- Proteja la información propia y la de sus clientes.
- Garantice la continuidad de sus operaciones.
- Mantenga la confianza de clientes, proveedores y socios comerciales.
- Cumpla con requisitos legales, contractuales y regulatorios aplicables.
- Disminuya pérdidas económicas derivadas de incidentes de seguridad.
- Fortalezca sus procesos internos mediante controles preventivos y correctivos.
- Impulse una cultura organizacional orientada a la seguridad de la información y la protección de activos.

1.2 Objetivos Específicos

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

Protección de los activos físicos

Implementar controles que garanticen la protección de las instalaciones, mobiliario, herramientas, equipos tecnológicos, refacciones y demás activos físicos propiedad de la empresa o bajo su custodia, reduciendo la probabilidad de robo, daño, pérdida o uso no autorizado.

Protección de la información

Preservar la confidencialidad, integridad y disponibilidad de toda la información administrada por la empresa, incluyendo información comercial, financiera, técnica, administrativa y aquella proporcionada por clientes y proveedores.

Control de accesos

Establecer mecanismos de autenticación y autorización que aseguren que únicamente el personal autorizado pueda acceder a instalaciones, sistemas, aplicaciones, bases de datos y recursos tecnológicos conforme a sus funciones y responsabilidades.

Prevención de incidentes

Reducir la probabilidad de incidentes de seguridad mediante la implementación de controles preventivos, monitoreo continuo, capacitación al personal y procedimientos de respuesta ante emergencias.

Gestión de riesgos

Identificar, evaluar y tratar los riesgos relacionados con la seguridad física y lógica mediante un enfoque preventivo basado en la mejora continua.

Cumplimiento normativo

Asegurar el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables, así como de las políticas internas y las mejores prácticas internacionales en materia de seguridad de la información.

Continuidad del negocio

Establecer medidas que permitan mantener la operación de la empresa ante incidentes que afecten la disponibilidad de los recursos tecnológicos o de la infraestructura física.

Cultura de seguridad

Promover entre todo el personal una cultura de responsabilidad respecto a la protección de la información, el uso adecuado de los recursos tecnológicos y el cumplimiento de las políticas de seguridad.

2. Alcance

2.1 Alcance Organizacional

La presente política es de cumplimiento obligatorio para todas las áreas de Q MAS IT S. de R.L. de C.V., independientemente de su ubicación física o modalidad de trabajo.

Esta política aplica a:

- Dirección General.
- Administración.
- Área Comercial.
- Área de Compras.
- Área de Soporte Técnico.
- Taller de Reparación.
- Ingeniería.
- Implementación de Proyectos.
- Logística y Almacén.
- Personal administrativo.
- Técnicos de campo.
- Personal remoto.
- Consultores externos.
- Subcontratistas.
- Prestadores de servicios.
- Personal temporal.
- Becarios.
- Visitantes que ingresen a las instalaciones.

Toda persona que tenga acceso a información o activos de la empresa deberá cumplir esta política.

2.2 Alcance de la Información

Esta política protege toda la información administrada por la empresa, independientemente del medio en que se encuentre almacenada.

INCLUYE, ENTRE OTROS:

- INFORMACIÓN IMPRESA.
- DOCUMENTACIÓN ELECTRÓNICA.
- BASES DE DATOS.
- CORREOS ELECTRÓNICOS.
- CONTRATOS.
- COTIZACIONES.
- LICENCIAS.
- INFORMACIÓN FINANCIERA.
- EXPEDIENTES DE CLIENTES.
- INFORMACIÓN TÉCNICA.
- MANUALES DE SERVICIO.
- DIAGRAMAS.
- CONFIGURACIONES.
- INFORMACIÓN ALMACENADA EN SERVIDORES.
- INFORMACIÓN EN PLATAFORMAS EN LA NUBE.
- INFORMACIÓN CONTENIDA EN DISPOSITIVOS MÓVILES.

2.3 ALCANCE TECNOLÓGICO

LOS CONTROLES ESTABLECIDOS APLICAN A TODOS LOS RECURSOS TECNOLÓGICOS PROPIEDAD DE LA EMPRESA O ADMINISTRADOS POR ELLA, INCLUYENDO:

- COMPUTADORAS DE ESCRITORIO.
- LAPTOPS.
- SERVIDORES.
- EQUIPOS DE ALMACENAMIENTO.
- SWITCHES.
- ROUTERS.
- FIREWALLS.
- ACCESS POINTS.
- IMPRESORAS.
- EQUIPOS DE DIAGNÓSTICO.
- EQUIPOS DE LABORATORIO.
- EQUIPOS DE CLIENTES BAJO RESGUARDO.
- DISPOSITIVOS MÓVILES CORPORATIVOS.
- SISTEMAS DE VIDEOVIGILANCIA.
- SISTEMAS DE CONTROL DE ACCESO.
- PLATAFORMAS SAAS.
- SERVICIOS EN MICROSOFT 365 O EQUIVALENTES.
- SISTEMAS ERP, CRM Y PLATAFORMAS DE GESTIÓN.

2.4 ALCANCE FÍSICO

La política aplica a todas las instalaciones donde Q MAS IT S. desarrolla actividades, incluyendo:

- Oficinas administrativas.
- Talleres de reparación.
- Almacenes.
- Centros de distribución.
- Áreas de recepción.
- Áreas de carga y descarga.
- Salas de juntas.
- Áreas de servidores.
- Vehículos utilizados para actividades laborales.
- Sitios de clientes durante la ejecución de proyectos.

2.5 Alcance Temporal

La presente política será aplicable durante todo el tiempo que exista una relación laboral, contractual o comercial con Q MAS IT S. de R.L. de C.V., incluso después de la terminación de dicha relación cuando existan obligaciones de confidencialidad o protección de información.

---

3. Principios y Objetivos de la Seguridad

La estrategia de seguridad de Q MAS IT S. de R.L. de C.V. se basa en principios que orientan todas las decisiones relacionadas con la protección de los activos de la organización.

3.1 Confidencialidad

Toda la información generada, administrada o resguardada por la empresa será accesible únicamente para las personas autorizadas.

Se implementarán controles que impidan la divulgación, modificación o acceso no autorizado a información sensible de clientes, proveedores y de la propia organización.

3.2 Integridad

La empresa garantizará que la información permanezca completa, exacta y protegida contra modificaciones accidentales o intencionales.

Para ello se utilizarán controles de acceso, respaldos, registros de cambios y mecanismos de validación que permitan detectar alteraciones no autorizadas.

3.3 Disponibilidad

Los sistemas, aplicaciones e información deberán estar disponibles para los usuarios autorizados cuando sean requeridos para el desempeño de sus funciones.

La empresa implementará mecanismos de respaldo, redundancia y recuperación que reduzcan el impacto de fallas técnicas o incidentes de seguridad.

3.4 Gestión basada en riesgos

Las decisiones relacionadas con la seguridad física y lógica se fundamentarán en la identificación, análisis y tratamiento de riesgos, priorizando la protección de los activos críticos del negocio.

3.5 Responsabilidad compartida

La seguridad es responsabilidad de todas las personas que colaboran con Q MAS IT S. de R.L. de C.V.

Cada colaborador deberá proteger los activos bajo su responsabilidad, cumplir las políticas establecidas y reportar cualquier incidente o condición que represente un riesgo para la organización.

3.6 Mejora continua

La organización revisará periódicamente la eficacia de sus controles de seguridad, considerando los resultados de auditorías, incidentes, cambios tecnológicos y nuevas amenazas, con el propósito de fortalecer continuamente su sistema de gestión de seguridad.

3.7 Objetivos Estratégicos de Seguridad

Para materializar estos principios, la empresa establece los siguientes objetivos estratégicos:

- Mantener un índice de cumplimiento del 100 % en los controles de acceso físico y lógico establecidos.
- Proteger todos los equipos propiedad de clientes que permanezcan bajo custodia de la empresa mediante controles de identificación, almacenamiento y trazabilidad.
- Garantizar que el 100 % de los equipos corporativos cuenten con antivirus, actualizaciones de seguridad y mecanismos de autenticación configurados.
- Realizar respaldos periódicos de la información crítica y verificar regularmente la posibilidad de su recuperación.
- Capacitar anualmente a todo el personal en temas de seguridad física, ciberseguridad, protección de datos e ingeniería social.
- Investigar y documentar todos los incidentes de seguridad, implementando acciones correctivas para evitar su recurrencia.
- Revisar y actualizar esta política al menos una vez al año o cuando existan cambios relevantes en la organización, la tecnología o los requisitos legales y contractuales.

Estos principios y objetivos constituyen la base sobre la cual Q MAS IT S. de R.L. de C.V. desarrolla e implementa los controles específicos de seguridad física y lógica descritos en los apartados posteriores de esta política.

4. Definiciones

4.1 Introducción

Con el propósito de asegurar una correcta interpretación y aplicación de la presente política, Q MAS IT S. de R.L. de C.V. establece las siguientes definiciones. Estos conceptos constituyen la base para la implementación de los controles de seguridad física y lógica, permitiendo que todos los colaboradores comprendan el alcance de las medidas de protección adoptadas por la organización.

4.2 Seguridad Física

La Seguridad Física comprende el conjunto de políticas, procedimientos, controles y mecanismos destinados a proteger las instalaciones, los activos materiales, las personas y la infraestructura tecnológica de la empresa contra amenazas internas y externas que puedan comprometer su integridad, disponibilidad o funcionamiento.

Su finalidad es prevenir eventos como:

- Robo de equipos.
- Hurto de herramientas.
- Daños a instalaciones.
- Sabotaje.
- Accesos no autorizados.
- Actos de vandalismo.
- Incendios.
- Inundaciones.

- Fenómenos naturales.
- Fallas eléctricas.
- Pérdida de equipos bajo resguardo.

Para lograr estos objetivos, la empresa implementará controles como:

- Sistemas de control de acceso.
- Cerraduras de seguridad.
- Llaves controladas.
- Videovigilancia (CCTV).
- Alarmas.
- Iluminación perimetral.
- Señalización.
- Protección contra incendios.
- Sistemas de energía ininterrumpida (UPS).
- Inventarios físicos.
- Etiquetado patrimonial.
- Procedimientos de ingreso y salida de equipos.

La seguridad física deberá considerar tanto la protección de los activos propios como aquellos pertenecientes a clientes que permanezcan temporalmente bajo la custodia de la empresa.

4.3 Seguridad Lógica

La Seguridad Lógica comprende el conjunto de controles tecnológicos, administrativos y organizacionales destinados a proteger la información y los recursos informáticos contra accesos no autorizados, pérdida, alteración, destrucción o divulgación indebida.

Su objetivo principal es preservar los tres principios fundamentales de la seguridad de la información:

- Confidencialidad.
- Integridad.
- Disponibilidad.

La seguridad lógica contempla controles tales como:

- Gestión de usuarios.
- Contraseñas seguras.
- Autenticación multifactor.
- Antivirus.
- Firewalls.
- Cifrado de información.
- Respaldos.
- Monitoreo de eventos.
- Actualizaciones de seguridad.
- Gestión de privilegios.
- Control de dispositivos externos.

- Protección del correo electrónico.

Estos controles aplican tanto a los sistemas internos como a las plataformas utilizadas por la organización en modalidad local o en la nube.

4.4 Activo

Se considera activo cualquier recurso que tenga valor para la organización y cuya pérdida, alteración o indisponibilidad pueda afectar el cumplimiento de sus objetivos.

Los activos pueden clasificarse como:

Activos físicos

- Edificios.
- Oficinas.
- Mobiliario.
- Herramientas.
- Vehículos.
- Computadoras.
- Servidores.
- Equipos de diagnóstico.
- Equipos de clientes.

Activos tecnológicos

- Software.
- Sistemas operativos.
- Licencias.
- Aplicaciones.
- Plataformas SaaS.
- Infraestructura de red.

Activos de información

- Bases de datos.
- Contratos.
- Expedientes.
- Información financiera.
- Manuales técnicos.
- Cotizaciones.
- Información de clientes.

Activos humanos

- Conocimientos del personal.
- Capacidades técnicas.
- Experiencia.
- Procedimientos documentados.

4.5 Información Confidencial

Se considera información confidencial toda aquella cuyo acceso, modificación o divulgación no autorizada pueda ocasionar perjuicios económicos, legales, operativos o reputacionales a Q MAS IT S. de R.L. de C.V. o a sus clientes.

Entre ella se encuentra:

- Información financiera.
- Estados de cuenta.
- Información bancaria.
- Contratos.
- Propuestas comerciales.
- Listas de precios.
- Información de clientes.
- Información de proveedores.
- Diagramas de red.
- Credenciales.
- Contraseñas.
- Configuraciones.
- Planes estratégicos.
- Información técnica.
- Reportes de servicio.
- Documentación de proyectos.

Toda la información confidencial deberá tratarse conforme a los controles definidos por la empresa.

4.6 Incidente de Seguridad

Se considera incidente de seguridad cualquier evento que afecte o tenga el potencial de afectar la confidencialidad, integridad o disponibilidad de la información, los sistemas o los activos físicos.

Ejemplos:

- Robo de computadoras.
- Pérdida de laptops.
- Acceso no autorizado.
- Malware.

- Ransomware.
- Phishing.
- Daño a servidores.
- Eliminación accidental de información.
- Fallas críticas de infraestructura.
- Acceso físico indebido.

Todos los incidentes deberán reportarse inmediatamente.

---

5. Activos Protegidos

5.1 Generalidades

Q MAS IT S. de R.L. de C.V. reconoce que la protección de los activos constituye un elemento fundamental para garantizar la continuidad del negocio y la confianza de sus clientes.

Todos los activos deberán contar con un responsable claramente identificado, quien será responsable de su uso adecuado, protección y conservación.

La empresa implementará mecanismos de clasificación, inventario, identificación y control para cada uno de ellos.

5.2 Infraestructura Física

Se consideran activos protegidos las instalaciones utilizadas por la empresa para el desarrollo de sus actividades.

Incluyen:

- Oficinas administrativas.
- Talleres de reparación.
- Almacenes.
- Área de recepción.
- Áreas de carga y descarga.
- Sala de juntas.
- Área de servidores.
- Centros de servicio.
- Estacionamientos.
- Áreas restringidas.

Estas áreas deberán mantenerse limpias, ordenadas y protegidas mediante controles físicos apropiados.

5.3 Equipos Tecnológicos

Son activos protegidos todos los equipos tecnológicos propiedad de la empresa o bajo su resguardo.

Entre ellos:

- Computadoras.
- Laptops.
- Servidores.
- Monitores.
- Impresoras.
- Equipos de diagnóstico.
- Switches.
- Routers.
- Firewalls.
- Access Points.
- Tablets.
- Smartphones corporativos.
- Equipos de laboratorio.
- Equipos de clientes.

Cada equipo deberá:

- Estar inventariado.
- Contar con número patrimonial.
- Tener responsable asignado.
- Mantener registro de mantenimiento.
- Contar con respaldo documental.

5.4 Herramientas y Equipamiento Técnico

La empresa protegerá todas las herramientas utilizadas durante la instalación y mantenimiento de equipos.

Ejemplos:

- Multímetros.
- Taladros.
- Crimpadoras.
- Probadores de cableado.
- Escaleras.
- Equipos de medición.
- Herramientas especializadas.
- Equipos de soldadura.
- Instrumentos electrónicos.

El préstamo y devolución de herramientas deberá registrarse.

5.5 Información

Toda la información generada por la organización será considerada un activo estratégico.

Incluye:

- Información administrativa.
- Información financiera.
- Información fiscal.
- Bases de datos.
- Contratos.
- Cotizaciones.
- Manuales.
- Reportes técnicos.
- Información de clientes.
- Fotografías de proyectos.
- Diagramas.
- Configuraciones.
- Licencias de software.

La empresa establecerá mecanismos para garantizar su confidencialidad, integridad y disponibilidad.

5.6 Servicios en la Nube

Se consideran activos protegidos los servicios contratados con proveedores externos.

Entre ellos:

- Correo electrónico empresarial.
- Microsoft 365.
- Plataformas SaaS.
- Sistemas CRM.
- Sistemas ERP.
- Servicios de respaldo.
- Repositorios documentales.
- Plataformas de colaboración.

La empresa garantizará el uso seguro de estos servicios mediante controles de autenticación, respaldo y administración de usuarios.

5.7 Equipos de Clientes

Debido al giro comercial de Q MAS IT S. de R.L. de C.V., los equipos propiedad de los clientes representan uno de los activos más críticos bajo custodia.

Cada equipo recibido deberá:

- Registrarse en el sistema.
- Identificarse mediante número de servicio.
- Documentar su estado físico.
- Permanecer bajo resguardo seguro.
- Mantener trazabilidad durante todo el proceso de reparación.
- Entregarse únicamente a personal autorizado.

---

6. Política de Seguridad Física

6.1 Objetivo

La Seguridad Física tiene como propósito proteger las instalaciones, el personal, la infraestructura tecnológica, los equipos propios y los activos de clientes mediante la implementación de controles preventivos, detectivos y correctivos que reduzcan los riesgos derivados de amenazas físicas.

Todos los colaboradores son responsables de contribuir al mantenimiento de un ambiente seguro.

6.2 Control de Accesos

El acceso a las instalaciones será controlado mediante procedimientos que permitan identificar a toda persona que ingrese.

Las medidas podrán incluir:

- Cerraduras de alta seguridad.
- Llaves controladas.
- Tarjetas de proximidad.
- Biometría.
- Registro de visitantes.
- Videovigilancia.
- Personal autorizado.

Las llaves deberán permanecer bajo control de la Dirección o del responsable designado. Cualquier pérdida deberá reportarse de inmediato para evaluar el cambio de cerraduras o la anulación de accesos.

6.3 Recepción y Control de Visitantes

Toda persona ajena a la empresa deberá:

- Registrarse al ingresar.
- Presentar una identificación oficial cuando sea requerido.

- Indicar el motivo de su visita.
- Permanecer acompañada por personal autorizado durante toda su estancia.
- Respetar las normas de seguridad y confidencialidad.

Se limitará el acceso únicamente a las áreas necesarias para el propósito de la visita.

6.4 Protección de Instalaciones

Las instalaciones deberán mantenerse en condiciones que reduzcan riesgos para las personas y los activos.

Se implementarán medidas como:

- Iluminación adecuada.
- Señalización visible.
- Rutas de evacuación despejadas.
- Control de acceso a áreas restringidas.
- Orden y limpieza.
- Mantenimiento preventivo de la infraestructura.
- Protección contra incendios.

6.5 Protección de Equipos

Todos los equipos tecnológicos deberán resguardarse adecuadamente para evitar:

- Robo.
- Manipulación indebida.
- Caídas.
- Daños físicos.
- Exposición al agua.
- Polvo excesivo.
- Temperaturas extremas.

Durante el transporte hacia instalaciones de clientes se utilizarán embalajes y medios adecuados para minimizar riesgos.

6.6 Protección de Equipos de Clientes

Los equipos recibidos para diagnóstico, garantía o reparación deberán almacenarse en áreas específicas, claramente identificadas y con acceso restringido.

Durante todo el proceso se conservará la trazabilidad del equipo, documentando su recepción, diagnóstico, intervención técnica, pruebas funcionales y entrega.

6.7 Protección Eléctrica y Ambiental

La infraestructura tecnológica deberá contar con:

- Sistemas UPS para equipos críticos.
- Reguladores de voltaje.
- Supresores de picos.
- Puesta a tierra conforme a normativa.
- Ventilación adecuada.
- Control de temperatura y humedad cuando sea necesario.

Estas medidas buscan prevenir daños por variaciones eléctricas o condiciones ambientales adversas.

6.8 Monitoreo y Vigilancia

Cuando la naturaleza de las operaciones lo requiera, la empresa podrá utilizar sistemas de videovigilancia (CCTV) y otros mecanismos de monitoreo para proteger las instalaciones y los activos, respetando en todo momento la legislación aplicable en materia de privacidad y protección de datos personales.

6.9 Inspecciones y Mantenimiento

Se realizarán inspecciones periódicas de las instalaciones y de los equipos de seguridad física para verificar su correcto funcionamiento.

Las observaciones detectadas deberán documentarse y corregirse oportunamente mediante acciones preventivas o correctivas.

6.10 Responsabilidades del Personal

Todo colaborador deberá:

- Cuidar los activos bajo su responsabilidad.
- Mantener el orden y limpieza de su área de trabajo.
- Reportar condiciones inseguras o incidentes de seguridad.
- Cumplir los procedimientos establecidos.
- Proteger los equipos e información de clientes durante cualquier actividad técnica.

El incumplimiento de estas disposiciones podrá dar lugar a las acciones disciplinarias previstas por la empresa.

7. Política de Seguridad Lógica

7.1 Objetivo

La Seguridad Lógica en Q MAS IT S. de R.L. de C.V. tiene como finalidad proteger todos los activos de información y los recursos tecnológicos utilizados por la organización mediante la implementación de controles administrativos, técnicos y operativos que reduzcan la probabilidad de accesos no autorizados, pérdida de información, alteración de datos, interrupción de los servicios o ataques informáticos.

La empresa reconoce que gran parte de su operación depende del uso de equipos de cómputo, plataformas en la nube, correo electrónico, aplicaciones empresariales y sistemas de información, por lo que resulta indispensable establecer mecanismos que garanticen la confidencialidad, integridad y disponibilidad de dichos recursos.

La Seguridad Lógica deberá implementarse considerando el principio de "mínimo privilegio", otorgando a cada usuario únicamente los accesos necesarios para desempeñar sus funciones.

Asimismo, todos los sistemas deberán administrarse bajo criterios de trazabilidad, disponibilidad y protección contra amenazas internas y externas.

7.2 Administración de Usuarios y Control de Accesos

Todos los usuarios que requieran acceso a recursos tecnológicos deberán contar con una cuenta individual e intransferible.

La creación, modificación o eliminación de cuentas deberá realizarse únicamente por el responsable de Tecnologías de Información o por el personal autorizado.

La asignación de privilegios deberá considerar:

- Funciones del puesto.
- Responsabilidades laborales.
- Nivel de autorización.
- Necesidad operativa.
- Riesgos asociados al acceso.

Queda estrictamente prohibido:

- Compartir usuarios.
- Compartir contraseñas.
- Utilizar cuentas genéricas sin autorización.
- Utilizar cuentas de otros colaboradores.
- Mantener cuentas activas de personal que ya no labore en la empresa.

Cuando un colaborador cambie de puesto o concluya su relación laboral, sus accesos deberán modificarse o eliminarse de forma inmediata.

7.3 Política de Contraseñas

Las contraseñas constituyen el primer mecanismo de protección contra accesos no autorizados.

Todas las credenciales utilizadas en los sistemas corporativos deberán cumplir con los siguientes criterios mínimos:

- Longitud mínima de 12 caracteres.
- Combinación de letras mayúsculas y minúsculas.
- Inclusión de números.
- Inclusión de caracteres especiales.
- No contener nombres propios.
- No contener información personal.
- No contener palabras de diccionario fácilmente identificables.

Las contraseñas deberán mantenerse en estricta confidencialidad.

Queda prohibido:

- Escribir contraseñas en papel visible.
- Compartir credenciales mediante correo electrónico o mensajería instantánea.
- Almacenarlas en archivos sin protección.
- Reutilizar contraseñas anteriores en sistemas críticos.

La empresa promoverá el uso de gestores de contraseñas aprobados para almacenar credenciales de forma segura.

7.4 Autenticación Multifactor (MFA)

Siempre que la plataforma lo permita, se habilitará autenticación multifactor para servicios críticos.

El MFA será obligatorio para:

- Correo electrónico corporativo.
- Plataformas Microsoft 365.
- VPN.
- Plataformas SaaS.
- Sistemas administrativos.
- Plataformas financieras.
- Consolas de administración.

Los factores adicionales podrán incluir:

- Aplicaciones autenticadoras.
- Tokens físicos.
- Códigos temporales.
- Biometría.

7.5 Protección de Equipos

Todos los equipos utilizados por la organización deberán mantenerse protegidos mediante:

- Antivirus actualizado.
- Firewall habilitado.
- Sistema operativo actualizado.
- Bloqueo automático de pantalla.
- Cifrado del disco duro cuando sea posible.
- Restricción de instalación de software.
- Monitoreo de seguridad.

Los usuarios no podrán modificar las configuraciones de seguridad sin autorización.

7.6 Gestión de Software

Únicamente podrá instalarse software autorizado por la empresa.

Antes de instalar una aplicación deberán verificarse:

- Licenciamiento.
- Compatibilidad.
- Origen del software.
- Riesgos de seguridad.

Queda prohibida la instalación de:

- Software pirata.
- Programas descargados de sitios no confiables.
- Herramientas de hacking.
- Software sin licencia.

7.7 Actualizaciones de Seguridad

Todos los sistemas deberán mantenerse actualizados.

Las actualizaciones incluirán:

- Sistema operativo.
- Antivirus.
- Firmware.
- Navegadores.
- Aplicaciones.

- Drivers.
- Dispositivos de red.

Las actualizaciones críticas deberán instalarse en el menor tiempo posible una vez validadas.

7.8 Protección del Correo Electrónico

El correo corporativo constituye uno de los principales medios de comunicación con clientes y proveedores.

Todo usuario deberá:

- Verificar el remitente antes de abrir archivos.
- Confirmar enlaces sospechosos.
- Reportar correos fraudulentos.
- No compartir información confidencial sin autorización.
- Utilizar únicamente cuentas corporativas para asuntos laborales.

La empresa implementará filtros antispam y mecanismos de protección contra phishing cuando sea técnicamente posible.

7.9 Uso de Dispositivos Externos

El uso de memorias USB, discos externos u otros dispositivos de almacenamiento será restringido.

Antes de utilizar cualquier dispositivo externo deberá:

- Escanearse con antivirus.
- Verificarse su procedencia.
- Contar con autorización cuando almacene información sensible.

7.10 Respaldo de Información

Toda la información considerada crítica deberá respaldarse periódicamente.

Los respaldos deberán:

- Mantener varias versiones.
- Almacenarse en ubicaciones seguras.
- Probarse regularmente.
- Protegerse mediante cifrado cuando sea necesario.

7.11 Monitoreo

La empresa podrá monitorear:

- Accesos.
- Eventos.
- Intentos fallidos.
- Cambios administrativos.
- Actividad en servidores.
- Eventos de red.

El monitoreo tendrá como finalidad detectar oportunamente incidentes de seguridad.

---

8. Seguridad durante la Prestación de Servicios en Sitio

8.1 Objetivo

Debido a que Q MAS IT S. de R.L. de C.V. desarrolla actividades de instalación, mantenimiento, reparación e implementación de soluciones tecnológicas en las instalaciones de sus clientes, es indispensable establecer lineamientos que garanticen la protección de la información y de los activos durante la prestación de dichos servicios.

La seguridad deberá mantenerse durante todas las fases del servicio:

- Planeación.
- Traslado.
- Instalación.
- Configuración.
- Pruebas.
- Puesta en operación.
- Mantenimiento.
- Retiro de equipos.

8.2 Identificación del Personal

Todo técnico deberá identificarse adecuadamente antes de iniciar cualquier actividad.

Podrá utilizar:

- Credencial corporativa.
- Uniforme institucional.
- Orden de servicio.
- Carta de presentación.
- Documento de autorización del cliente.

8.3 Protección de la Información del Cliente

Durante la ejecución de un servicio, el personal podrá tener acceso a información sensible del cliente.

Por ello deberá:

- Mantener absoluta confidencialidad.
- No copiar información sin autorización.
- No tomar fotografías de información sensible.
- No compartir configuraciones del cliente.
- No divulgar información técnica observada.

Las obligaciones de confidencialidad continuarán incluso después de finalizar el servicio.

8.4 Uso de Herramientas

El personal utilizará únicamente herramientas autorizadas por la empresa.

Se prohíbe:

- Utilizar software pirata.
- Conectar dispositivos personales sin autorización.
- Ejecutar programas desconocidos.
- Instalar aplicaciones no solicitadas por el cliente.

8.5 Equipos del Cliente

Cuando un equipo del cliente sea trasladado al taller de Q MAS IT S., deberá:

- Registrarse.
- Etiquetarse.
- Documentarse fotográficamente cuando sea necesario.
- Resguardarse en áreas seguras.
- Mantener trazabilidad durante todo el proceso.

8.6 Accesos Temporales

Cuando el cliente otorgue credenciales temporales para realizar un servicio:

- Sólo deberán utilizarse durante el tiempo autorizado.
- No podrán copiarse.

- No podrán reutilizarse.
- Deberán eliminarse una vez concluido el servicio.

8.7 Protección de Equipos durante el Transporte

Durante el traslado de equipos deberán utilizarse medidas que reduzcan el riesgo de daño físico.

Entre ellas:

- Empaque adecuado.
- Protección contra impactos.
- Protección contra humedad.
- Etiquetado.
- Registro de entrega y recepción.

8.8 Reporte de Incidentes

Cualquier incidente detectado durante la ejecución del servicio deberá reportarse inmediatamente.

Ejemplos:

- Daño accidental.
- Robo.
- Acceso indebido.
- Malware.
- Falla crítica.
- Pérdida de información.

El incidente deberá documentarse para su análisis y seguimiento.

8.9 Cumplimiento de Políticas del Cliente

Cuando un cliente cuente con políticas específicas de seguridad, el personal de Q MAS IT S. deberá cumplirlas siempre que no contravengan la legislación aplicable ni las políticas internas de la empresa.

---

9. Gestión de Incidentes de Seguridad

9.1 Objetivo

La Gestión de Incidentes de Seguridad tiene como finalidad establecer un proceso estructurado para identificar, registrar, analizar, contener, erradicar, recuperar y documentar cualquier evento que afecte o

pueda afectar la seguridad física, la seguridad lógica o la continuidad de las operaciones de Q MAS IT S. de R.L. de C.V.

La empresa reconoce que una respuesta rápida y organizada permite reducir el impacto operativo, financiero, legal y reputacional de los incidentes.

9.2 Definición de Incidente

Se considera incidente cualquier evento que comprometa o tenga el potencial de comprometer:

- La confidencialidad.
- La integridad.
- La disponibilidad.
- La continuidad del negocio.
- La infraestructura física.
- Los activos tecnológicos.

9.3 Ejemplos de Incidentes

Entre otros:

- Robo de computadoras.
- Robo de herramientas.
- Robo de equipos de clientes.
- Accesos no autorizados.
- Malware.
- Ransomware.
- Phishing.
- Pérdida de laptops.
- Eliminación accidental de información.
- Fallas críticas de servidores.
- Daños por incendio.
- Daños por inundación.
- Sabotaje.
- Violaciones de confidencialidad.
- Uso indebido de cuentas.

9.4 Proceso de Atención de Incidentes

La empresa seguirá las siguientes etapas:

Identificación

Detectar el incidente mediante reportes del personal, sistemas de monitoreo, auditorías o avisos de clientes.

Registro

Todo incidente deberá documentarse indicando:

- Fecha.
- Hora.
- Lugar.
- Responsable.
- Descripción.
- Sistemas afectados.
- Evidencias disponibles.

Clasificación

El incidente será clasificado según:

- Criticidad.
- Impacto.
- Urgencia.
- Tipo de activo afectado.

Contención

Se implementarán acciones inmediatas para evitar la propagación del incidente, tales como:

- Desconectar equipos.
- Bloquear usuarios.
- Aislar sistemas.
- Resguardar evidencias.

Erradicación

Eliminar la causa raíz del incidente mediante acciones técnicas u operativas.

Recuperación

Restablecer los servicios utilizando respaldos, reemplazo de equipos, restauración de configuraciones o cualquier otra medida necesaria.

Cierre

Una vez resuelto el incidente se elaborará un informe que incluya:

- Causa raíz.
- Impacto.
- Acciones realizadas.
- Tiempo de recuperación.

- Lecciones aprendidas.
- Acciones preventivas.

9.5 Responsabilidades

Todos los colaboradores tienen la obligación de reportar inmediatamente cualquier incidente o situación sospechosa.

El responsable de Tecnologías de Información coordinará la investigación técnica, mientras que la Dirección General supervisará las decisiones relacionadas con incidentes de alto impacto.

9.6 Conservación de Evidencias

Cuando el incidente pueda derivar en responsabilidades legales o contractuales, se preservarán las evidencias físicas y digitales de manera íntegra, evitando su alteración y documentando la cadena de custodia cuando corresponda.

9.7 Mejora Continua

Todos los incidentes serán analizados para identificar oportunidades de mejora en los controles existentes. Las lecciones aprendidas se incorporarán a los procedimientos, programas de capacitación y evaluaciones de riesgo, fortaleciendo continuamente el sistema de gestión de seguridad de la empresa.

10. Responsabilidades

10.1 Objetivo

La correcta implementación de la presente Política de Seguridad Física y Seguridad Lógica requiere la participación activa de todo el personal de Q MAS IT S. de R.L. de C.V.. Cada colaborador, independientemente de su puesto o nivel jerárquico, es responsable de proteger los activos físicos, tecnológicos y la información bajo su custodia.

La asignación clara de responsabilidades permite asegurar que los controles de seguridad se apliquen de forma consistente, se mantenga la trazabilidad de las acciones realizadas y exista una adecuada rendición de cuentas ante cualquier incidente de seguridad.

10.2 Dirección General

La Dirección General es la máxima autoridad responsable del Sistema de Gestión de Seguridad de la Información dentro de la empresa.

Sus responsabilidades incluyen:

- Aprobar la presente política y sus actualizaciones.
- Promover una cultura organizacional orientada a la seguridad.
- Asignar los recursos humanos, tecnológicos y financieros necesarios para la implementación de los controles de seguridad.
- Asegurar que las políticas de seguridad estén alineadas con los objetivos estratégicos de la empresa.
- Aprobar los planes de respuesta a incidentes y continuidad del negocio.
- Revisar periódicamente los indicadores de seguridad.
- Evaluar los resultados de auditorías internas y externas.
- Autorizar acciones correctivas derivadas de incidentes críticos.
- Garantizar el cumplimiento de los requisitos legales y contractuales relacionados con la seguridad.

Asimismo, la Dirección deberá demostrar liderazgo mediante el cumplimiento de esta política y la promoción de buenas prácticas entre todo el personal.

10.3 Responsable de Tecnologías de Información

El Responsable de TI será el encargado de administrar los controles de seguridad lógica de la organización.

Entre sus principales responsabilidades se encuentran:

Administración de infraestructura tecnológica

- Mantener operativos los servidores.
- Administrar la red informática.
- Supervisar la infraestructura tecnológica.
- Controlar dispositivos de comunicación.

Administración de usuarios

- Crear cuentas.
- Modificar privilegios.
- Eliminar accesos cuando corresponda.
- Revisar permisos periódicamente.

Seguridad informática

- Mantener actualizado el antivirus.
- Supervisar actualizaciones de seguridad.
- Configurar firewalls.
- Gestionar respaldos.
- Supervisar el uso de plataformas en la nube.

Monitoreo

- Revisar registros de eventos.
- Detectar accesos sospechosos.
- Investigar incidentes tecnológicos.
- Generar reportes de seguridad.

Capacitación

- Difundir buenas prácticas.
- Capacitar al personal en temas de ciberseguridad.
- Informar sobre nuevas amenazas.

10.4 Responsables de Área

Cada responsable de área deberá garantizar que el personal bajo su supervisión cumpla con esta política.

Sus responsabilidades incluyen:

- Supervisar el uso adecuado de los activos.
- Reportar incidentes.
- Validar accesos requeridos por el personal.
- Autorizar el préstamo de equipos.
- Verificar el cumplimiento de procedimientos.
- Promover la cultura de seguridad.

También deberán participar en la identificación de riesgos relacionados con sus procesos.

10.5 Personal Técnico

El personal técnico representa uno de los grupos con mayor acceso a equipos e información de clientes, por lo que deberá mantener un alto nivel de responsabilidad.

Entre sus obligaciones se encuentran:

- Proteger los equipos de clientes.
- Mantener la confidencialidad de la información.
- No copiar información sin autorización.
- Utilizar únicamente herramientas autorizadas.
- Seguir los procedimientos técnicos establecidos.
- Mantener identificados los equipos bajo su responsabilidad.
- Documentar adecuadamente los servicios realizados.
- Reportar inmediatamente cualquier incidente.

Asimismo, deberán respetar las políticas de seguridad del cliente cuando presten servicios en sus instalaciones.

10.6 Personal Administrativo

El personal administrativo deberá:

- Proteger la documentación física y electrónica.
- Mantener bajo resguardo expedientes.
- No divulgar información confidencial.
- Utilizar correctamente los sistemas informáticos.
- Resguardar contraseñas.
- Evitar dejar documentos confidenciales visibles.

10.7 Todo el Personal

Todos los colaboradores deberán:

- Conocer esta política.
- Cumplir los procedimientos establecidos.
- Participar en capacitaciones.
- Proteger los activos bajo su responsabilidad.
- Reportar riesgos.
- Reportar incidentes.
- Utilizar adecuadamente los recursos tecnológicos.
- Mantener confidencialidad respecto a la información de clientes y de la empresa.
- Respetar las políticas de seguridad de los clientes durante la prestación de servicios.

El incumplimiento de estas responsabilidades podrá derivar en acciones disciplinarias.

10.8 Proveedores y Subcontratistas

Los proveedores que tengan acceso a información, instalaciones o equipos deberán cumplir los requisitos de seguridad establecidos por Q MAS IT S. de R.L. de C.V.

Cuando sea necesario, deberán firmar acuerdos de confidencialidad y aceptar las políticas de seguridad antes de iniciar actividades.

11. Capacitación y Concientización

11.1 Objetivo

La capacitación constituye uno de los principales mecanismos para reducir riesgos derivados del error humano.

Q MAS IT S. DE R.L. DE C.V. DESARROLLARÁ PROGRAMAS PERMANENTES DE FORMACIÓN CON EL PROPÓSITO DE QUE TODO EL PERSONAL CONOZCA LAS POLÍTICAS DE SEGURIDAD Y ADQUIERA LAS COMPETENCIAS NECESARIAS PARA PROTEGER LA INFORMACIÓN Y LOS ACTIVOS DE LA ORGANIZACIÓN.

11.2 ALCANCE

LOS PROGRAMAS DE CAPACITACIÓN APLICARÁN A:

- DIRECCIÓN.
- PERSONAL ADMINISTRATIVO.
- TÉCNICOS.
- INGENIEROS.
- PERSONAL TEMPORAL.
- PRESTADORES DE SERVICIOS.
- SUBCONTRATISTAS CUANDO CORRESPONDA.

TODA PERSONA QUE TENGA ACCESO A INFORMACIÓN O INSTALACIONES DEBERÁ RECIBIR CAPACITACIÓN ACORDE CON SUS FUNCIONES.

11.3 PROGRAMA DE CAPACITACIÓN

LA EMPRESA DESARROLLARÁ UN PROGRAMA ANUAL QUE PODRÁ INCLUIR, ENTRE OTROS, LOS SIGUIENTES TEMAS:

SEGURIDAD FÍSICA

- CONTROL DE ACCESOS.
- PROTECCIÓN DE INSTALACIONES.
- PROTECCIÓN CONTRA INCENDIOS.
- MANEJO SEGURO DE EQUIPOS.
- CUSTODIA DE ACTIVOS.
- PROTECCIÓN DE HERRAMIENTAS.
- SEGURIDAD DURANTE SERVICIOS EN SITIO.

SEGURIDAD LÓGICA

- GESTIÓN DE CONTRASEÑAS.
- USO SEGURO DEL CORREO ELECTRÓNICO.
- INGENIERÍA SOCIAL.
- PHISHING.
- MALWARE.
- RANSOMWARE.
- USO SEGURO DE INTERNET.
- PROTECCIÓN DE DISPOSITIVOS MÓVILES.
- MANEJO DE INFORMACIÓN CONFIDENCIAL.
- USO DE PLATAFORMAS EN LA NUBE.

- Protección de datos personales.

Gestión de Incidentes

- Cómo identificar incidentes.
- Procedimientos de reporte.
- Conservación de evidencias.
- Contención inicial.
- Comunicación de incidentes.

11.4 Inducción

Todo colaborador de nuevo ingreso deberá recibir capacitación antes de tener acceso a los recursos tecnológicos de la empresa.

La inducción incluirá:

- Presentación de políticas.
- Procedimientos de seguridad.
- Uso adecuado de equipos.
- Manejo de información.
- Responsabilidades individuales.
- Firma de aceptación de políticas.

11.5 Capacitación Periódica

La empresa realizará capacitaciones periódicas para mantener actualizado al personal respecto a:

- Nuevas amenazas.
- Cambios tecnológicos.
- Actualizaciones normativas.
- Incidentes ocurridos.
- Buenas prácticas internacionales.

La frecuencia mínima recomendada será una vez al año, pudiendo incrementarse cuando existan cambios importantes en la infraestructura o en el entorno de riesgos.

11.6 Evaluación

Al finalizar las capacitaciones podrán realizarse:

- Exámenes.
- Evaluaciones prácticas.

- Simulacros.
- Ejercicios de respuesta a incidentes.
- Campañas de phishing controlado.

Los resultados permitirán medir la efectividad del programa de concientización.

11.7 Registros

La empresa conservará evidencia documental de las actividades de capacitación, incluyendo:

- Programas.
- Listas de asistencia.
- Material didáctico.
- Evaluaciones.
- Constancias.
- Resultados obtenidos.

Estos registros servirán como evidencia durante auditorías.

---

12. Auditorías y Verificación del Cumplimiento

12.1 Objetivo

Las auditorías tienen como finalidad verificar que la presente política sea aplicada correctamente y que los controles de seguridad física y lógica sean eficaces para proteger los activos de la organización.

Asimismo, permiten identificar oportunidades de mejora y fortalecer continuamente el sistema de gestión de seguridad.

12.2 Tipos de Auditoría

La empresa podrá realizar:

Auditorías Internas

Realizadas por personal designado por la Dirección para verificar el cumplimiento de políticas, procedimientos y controles internos.

Auditorías Externas

Realizadas por clientes, organismos certificadores, proveedores estratégicos o entidades regulatorias cuando sea aplicable.

Revisiones Técnicas

Evaluaciones específicas sobre:

- Infraestructura tecnológica.
- Equipos.
- Redes.
- Respaldos.
- Seguridad lógica.
- Seguridad física.

12.3 Alcance de las Auditorías

Las auditorías podrán incluir la revisión de:

Seguridad Física

- Control de accesos.
- CCTV.
- Señalización.
- Protección contra incendios.
- Inventarios.
- Estado de instalaciones.
- Protección de equipos.
- Control de visitantes.

Seguridad Lógica

- Usuarios.
- Contraseñas.
- Antivirus.
- Firewalls.
- Actualizaciones.
- Respaldos.
- Registros de acceso.
- Configuración de sistemas.

Documentación

- Políticas.
- Procedimientos.
- Registros.
- Bitácoras.
- Inventarios.
- Reportes de incidentes.
- Evidencias de capacitación.

12.4 Planeación

Las auditorías deberán planificarse considerando:

- Criticidad de los procesos.
- Riesgos identificados.
- Cambios tecnológicos.
- Resultados de auditorías anteriores.
- Incidentes recientes.

La empresa procurará realizar al menos una auditoría interna anual sobre los controles de seguridad.

12.5 Hallazgos

Los hallazgos derivados de las auditorías podrán clasificarse como:

No conformidad crítica

Incumplimiento que representa un riesgo inmediato para la seguridad de la organización o de sus clientes.

No conformidad mayor

Incumplimiento significativo que requiere acciones correctivas prioritarias.

No conformidad menor

Incumplimiento de bajo impacto que debe corregirse en un plazo razonable.

Observación

Oportunidad de mejora que no representa un incumplimiento directo.

12.6 Acciones Correctivas

Todo hallazgo deberá generar un plan de acción que contemple:

- Identificación de la causa raíz.
- Responsable.
- Actividades correctivas.
- Fecha compromiso.
- Evidencias de implementación.
- Verificación de eficacia.

La Dirección dará seguimiento al cumplimiento de estas acciones hasta su cierre.

12.7 Indicadores de Desempeño

Para evaluar la eficacia de esta política, Q MAS IT S. de R.L. de C.V. establecerá indicadores como:

- Porcentaje de cumplimiento de auditorías programadas.
- Número de incidentes de seguridad registrados.
- Tiempo promedio de atención de incidentes.
- Porcentaje de equipos con actualizaciones vigentes.
- Porcentaje de usuarios con autenticación multifactor habilitada.
- Cumplimiento del programa anual de capacitación.
- Porcentaje de acciones correctivas cerradas en tiempo.

Estos indicadores serán revisados periódicamente por la Dirección para apoyar la toma de decisiones y promover la mejora continua del sistema de gestión de seguridad.

13. Incumplimiento de la Política y Régimen Disciplinario

13.1 Objetivo

El objetivo de este apartado es establecer el procedimiento mediante el cual Q MAS IT S. de R.L. de C.V. gestionará los incumplimientos a la presente Política de Seguridad Física y Seguridad Lógica, garantizando que cualquier desviación sea identificada, investigada, documentada y corregida de manera oportuna.

La empresa reconoce que la seguridad de la información y la protección de los activos dependen en gran medida del comportamiento responsable de todos los colaboradores, por lo que el incumplimiento de las políticas puede representar riesgos importantes para la continuidad del negocio, la satisfacción del cliente, el cumplimiento legal y la reputación de la organización.

Las acciones disciplinarias establecidas en este apartado tienen un carácter preventivo y correctivo, buscando fortalecer la cultura de seguridad y reducir la probabilidad de reincidencia.

13.2 Alcance

Las disposiciones de este apartado aplican a:

- Dirección General.
- Personal administrativo.
- Personal operativo.
- Ingenieros.
- Técnicos de campo.
- Personal de almacén.
- Personal temporal.
- Prestadores de servicios.

- Consultores.
- Subcontratistas.
- Visitantes que incumplan las normas de seguridad aplicables.

13.3 Conductas que Constituyen un Incumplimiento

Se considerará incumplimiento cualquier acción u omisión que contravenga lo establecido en esta política o que ponga en riesgo los activos físicos, tecnológicos o de información de la empresa o de sus clientes.

Ejemplos de incumplimientos incluyen, entre otros:

Seguridad Física

- Permitir el acceso a personas no autorizadas.
- No registrar visitantes cuando sea obligatorio.
- Dejar abiertas puertas de áreas restringidas.
- Abandonar equipos sin supervisión.
- No asegurar computadoras portátiles durante traslados.
- Sustraer equipos sin autorización.
- Manipular sistemas de videovigilancia sin permiso.
- No reportar la pérdida de llaves o tarjetas de acceso.
- Dañar deliberadamente instalaciones o equipos.

Seguridad Lógica

- Compartir usuarios o contraseñas.
- Utilizar software sin autorización.
- Desactivar el antivirus o el firewall corporativo.
- Descargar archivos desde sitios no confiables.
- Instalar aplicaciones no autorizadas.
- Utilizar dispositivos USB sin autorización.
- Compartir información confidencial con terceros.
- Enviar información sensible mediante medios no autorizados.
- Omitir la instalación de actualizaciones de seguridad.
- Acceder a información que no corresponda a las funciones asignadas.

Conductas Administrativas

- Ocultar incidentes de seguridad.
- Alterar registros.
- Falsificar evidencias.
- Omitir reportes obligatorios.
- Incumplir procedimientos documentados.

13.4 Clasificación de los Incumplimientos

Con el fin de aplicar medidas proporcionales, los incumplimientos se clasificarán de acuerdo con su gravedad.

Incumplimientos Menores

Son aquellos que representan un riesgo limitado y que normalmente no generan afectaciones significativas.

Ejemplos:

- No bloquear la computadora al ausentarse.
- Retraso en el cambio de contraseña.
- Descuidar el orden del área de trabajo.
- No portar la identificación institucional.

Incumplimientos Mayores

Son aquellos que generan riesgos importantes para la organización.

Ejemplos:

- Compartir contraseñas.
- Permitir el acceso a personas no autorizadas.
- Utilizar software sin licencia.
- Conectar dispositivos externos sin autorización.
- No reportar incidentes relevantes.

Incumplimientos Críticos

Son aquellos que pueden ocasionar pérdidas económicas, legales o reputacionales significativas.

Ejemplos:

- Robo de información.
- Divulgación de información confidencial.
- Sabotaje.
- Alteración intencional de información.
- Acceso deliberado a sistemas sin autorización.
- Fraude.
- Eliminación intencional de registros.
- Robo de equipos de clientes.

13.5 Investigación del Incumplimiento

Todo incumplimiento será investigado siguiendo un proceso estructurado que incluirá:

- Recepción del reporte.
- Registro del incidente.

- Recolección de evidencias.
- Entrevistas con las personas involucradas.
- Análisis de la información disponible.
- Determinación de la causa raíz.
- Evaluación del impacto.
- Definición de acciones correctivas y preventivas.

La investigación deberá realizarse con imparcialidad, confidencialidad y objetividad.

13.6 Medidas Disciplinarias

Dependiendo de la gravedad del incumplimiento, podrán aplicarse una o varias de las siguientes medidas:

- Retroalimentación y capacitación adicional.
- Amonestación verbal.
- Amonestación por escrito.
- Suspensión temporal de privilegios de acceso.
- Suspensión temporal de actividades.
- Reasignación de funciones.
- Terminación de la relación laboral conforme a la legislación aplicable.
- Rescisión del contrato con proveedores o subcontratistas.
- Inicio de acciones legales cuando exista daño patrimonial, fraude o incumplimiento contractual.

La aplicación de las medidas deberá respetar la legislación laboral vigente y el reglamento interno de trabajo.

13.7 Acciones Correctivas y Preventivas

Además de las medidas disciplinarias, la empresa implementará acciones para evitar la repetición del incumplimiento, tales como:

- Actualización de procedimientos.
- Revisión de controles existentes.
- Capacitación específica.
- Incremento del monitoreo.
- Cambios tecnológicos.
- Revisión de permisos de acceso.
- Auditorías extraordinarias.

---

14. Revisión, Actualización y Mejora Continua

14.1 Objetivo

La presente política deberá mantenerse vigente, actualizada y alineada con la evolución de la organización, las amenazas de seguridad, los cambios tecnológicos, los requisitos legales y las necesidades de los clientes.

La mejora continua permitirá que los controles implementados conserven su eficacia y respondan de manera adecuada a los riesgos emergentes.

14.2 Frecuencia de Revisión

La política será revisada como mínimo una vez al año.

No obstante, podrá revisarse antes cuando ocurra cualquiera de las siguientes situaciones:

- Cambios en la estructura organizacional.
- Incorporación de nuevas tecnologías.
- Implementación de nuevos sistemas.
- Apertura de nuevas instalaciones.
- Cambios en los procesos de negocio.
- Requisitos contractuales de clientes.
- Modificaciones a la legislación aplicable.
- Publicación de nuevas versiones de normas internacionales.
- Incidentes de seguridad relevantes.
- Resultados de auditorías que identifiquen oportunidades de mejora.

14.3 Responsables de la Revisión

La revisión será coordinada por la Dirección General con el apoyo del Responsable de Tecnologías de Información y de los responsables de cada área.

Durante el proceso se analizarán:

- Cumplimiento de objetivos.
- Resultados de auditorías.
- Estadísticas de incidentes.
- Indicadores de desempeño.
- Cambios tecnológicos.
- Retroalimentación de clientes.
- Requisitos regulatorios.
- Riesgos emergentes.

14.4 Proceso de Actualización

Cuando sea necesario modificar la política, se seguirá el siguiente proceso:

1. Identificación de la necesidad de cambio.
2. Elaboración de la propuesta de modificación.
3. Revisión técnica por las áreas involucradas.
4. Aprobación por la Dirección General.
5. Actualización del número de versión y fecha de vigencia.
6. Comunicación oficial a todo el personal.
7. Capacitación cuando los cambios sean significativos.
8. Conservación del historial de versiones.

14.5 Mejora Continua

Q MAS IT S. de R.L. de C.V. adoptará un enfoque basado en el ciclo Planificar-Hacer-Verificar-Actuar (PHVA) para fortalecer permanentemente sus controles de seguridad.

Como parte de este proceso se desarrollarán actividades como:

- Evaluaciones periódicas de riesgos.
- Auditorías internas.
- Revisión de indicadores.
- Análisis de incidentes.
- Actualización tecnológica.
- Capacitación continua.
- Simulacros de respuesta a incidentes.
- Revisión de controles de acceso.
- Pruebas de restauración de respaldos.

14.6 Comunicación de Cambios

Toda modificación a esta política será comunicada oportunamente mediante los canales internos de la empresa, tales como:

- Correo electrónico corporativo.
- Reuniones de trabajo.
- Intranet o repositorio documental.
- Sesiones de capacitación.
- Avisos internos.

Cada colaborador deberá confirmar que conoce y comprende los cambios realizados.

---

15. Control Documental

15.1 Objetivo

Establecer los lineamientos para la elaboración, identificación, aprobación, distribución, actualización, almacenamiento, conservación y disposición final de la presente Política de Seguridad Física y Seguridad Lógica, garantizando que todo el personal utilice únicamente la versión vigente y autorizada.

El control documental asegura la trazabilidad de las modificaciones y facilita el cumplimiento de auditorías internas, auditorías de clientes y procesos de certificación.

15.2 Identificación del Documento

Todo documento controlado deberá contener, como mínimo:

- Título del documento.
- Código único.
- Número de versión.
- Fecha de emisión.
- Fecha de revisión.
- Responsable de elaboración.
- Responsable de revisión.
- Responsable de aprobación.
- Estado del documento (Vigente, Obsoleto o En Revisión).

15.3 Aprobación

La presente política deberá ser aprobada por la Dirección General antes de entrar en vigor.

Ninguna modificación podrá implementarse sin la autorización correspondiente.

15.4 Distribución

La versión vigente estará disponible para todo el personal autorizado mediante los medios definidos por la empresa.

Las copias impresas, cuando existan, deberán identificarse como "Copia Controlada" o "Copia No Controlada", según corresponda.

15.5 Control de Versiones

Cada modificación deberá registrarse en una tabla de control que incluya:

Versión	Fecha	Descripción del cambio	Elaboró	Revisó	Aprobó

1.0	Enero 2025	Emisión inicial	Responsable de TI, Alejandro Martinez	Dirección General	Dirección General
1.1	Enero 2026	Actualización de controles y procedimientos	Responsable de TI Alejandro Martinez	Dirección General	Dirección General

Este registro permitirá mantener la trazabilidad de todas las revisiones efectuadas.

15.6 Conservación de Registros

Los registros relacionados con la aplicación de esta política deberán conservarse conforme a los plazos definidos por la empresa o por la legislación aplicable.

Entre ellos:

- Registros de capacitación.
- Reportes de incidentes.
- Bitácoras de acceso.
- Resultados de auditorías.
- Inventarios de activos.
- Evidencias de mantenimiento.
- Acciones correctivas.
- Revisiones de la política.

Estos registros deberán almacenarse de forma segura, con controles que aseguren su confidencialidad, integridad y disponibilidad.

15.7 Resguardo y Protección

La documentación podrá conservarse en formato físico o electrónico, siempre que se implementen controles para evitar:

- Pérdida.
- Alteración no autorizada.
- Acceso indebido.
- Deterioro.
- Eliminación accidental.

Los documentos electrónicos deberán incluirse en los esquemas de respaldo de la empresa.

15.8 Disposición Final

Cuando un documento deje de ser vigente, será identificado como "Documento Obsoleto" y se retirará de los puntos de uso para evitar su utilización.

La eliminación de documentos físicos o electrónicos deberá realizarse de manera segura, asegurando que la información confidencial no pueda ser recuperada por personas no autorizadas. Esto podrá incluir el uso de destructoras de documentos para archivos impresos y el borrado seguro o la destrucción de medios de almacenamiento para archivos digitales.