Tecnológico Nacional de México

Instituto Tecnológico de Puebla

Materia: Auditoria en Tecnologías de la Información

Docente: Norma Álvarez Jiménez

Proyecto Final: Auditoria

Integrantes:

Caballero Morales Fatima Alejandra 19221941

Castro Ortega Veronica Lazarena 19222000

Marín Flores Eldrich 19221960

Morales González Fernando Isaac 19222678

Ramírez Justo Miguel Ángel 19221975

Villa Pérez Emilio Alonso 20222175

Fecha: 06 de diciembre del 2024

Auditoria a MS Autotransportes

Introducción

En la actualidad, la seguridad informática es un pilar fundamental para garantizar la continuidad operativa, la protección de datos y la confianza de los clientes en cualquier sector empresarial es por ello por lo que realizar esta auditoria se busca servir como una guía estratégica para fortalecer la postura de seguridad de la empresa, minimizando riesgos y optimizando la operatividad frente a las crecientes amenazas cibernéticas.

Este documento presenta los resultados de la auditoría de seguridad informática realizada al negocio de transporte **MS Autotransportes**, con el **objetivo de evaluar la eficacia de sus sistemas, identificar vulnerabilidades y proponer medidas correctivas alineadas con las mejores prácticas de la industria.** La auditoría abarcó aspectos clave como la infraestructura tecnológica, los controles de acceso, la protección de datos, la resiliencia ante incidentes y el cumplimiento normativo aplicable al sector.

La evaluación se llevó a cabo considerando las especificidades del negocio, incluyendo el manejo de información sensible de clientes y operaciones, así como la interdependencia tecnológica entre los sistemas de gestión y las plataformas de comunicación.

A continuación, se detallan los objetivos, metodología, hallazgos y recomendaciones derivadas de este proceso de auditoría.

Objetivos de la auditoria

1. **Evaluar el estado actual de la seguridad informática:**
    - Analizar la infraestructura tecnológica, incluyendo servidores, redes y dispositivos, para detectar brechas de seguridad.

2. **Identificar vulnerabilidades y riesgos asociados:**
    - Verificar que los sistemas de seguridad esten funcionando y dando respuestas como pueden ser camaras de seguridad con la hora y fecha correspondientes, alarmas de seguridad, documentos o lugares con pases de personal autorizado.

3. **Revisar la protección de datos sensibles:**
    - Evaluar las medidas implementadas para proteger información confidencial de clientes, socios y operaciones del negocio.

4. **Garantizar el cumplimiento de normativas y estándares aplicables:**
    - Asegurar que las operaciones del negocio se alinean con regulaciones legales y estándares internacionales aplicables al sector transporte.

5. **Analizar la gestion de accesos y control de usuarios:**
    - Comprobar que los permisos y roles están adecuadamente definidos y alineados con las funciones de los empleados.

Alcance

1. **Sistemas evaluados:**
    a. **Plataformas de gestión de transporte:** Análisis de sistemas de rastreo de flotas, seguimiento de envíos y gestión logística.
    b. **Sistemas de gestión interna:** Revisión de software de gestión empresarial, contabilidad y facturación.
    c. **Aplicaciones de terceros:** Verificación de seguridad en herramientas externas integradas en los procesos.

2. **Infraestructura cubierta:**
    a. **Redes:** Análisis de la seguridad en redes internas, conexiones externas, y redes inalámbricas, cableado de la red y archivos de docuemntación de la red.
    b. **Dispositivos:** Inspección de computadoras, impresoras en red, laptops y equipos asociados al negocio (dispositivos de rastreo de transportes).

3. **Protección de Datos:**
    a. **Confidencialidad de información sensible:** Verificación del cifrado de datos y acceso seguro a bases de datos.
    b. **Respaldo y recuperación:** Evaluación de las políticas y prácticas de backups, incluyendo su periodicidad y almacenamiento seguro.
    c. **Manejo de datos de clientes:** Análisis de los procesos de recolección, almacenamiento y procesamiento de información personal.

4. **Limitaciones:**
    a. **Revisión de regulaciones locales e internacionales:** Evaluación del cumplimiento de normativas como GDPR, ISO 27001, y estándares de protección de datos relevantes al sector transporte.
    b. **Contratos con terceros:** Análisis de cláusulas relacionadas con la seguridad informática en acuerdos con proveedores y socios tecnológicos o medidas de seguridad en la empresa se esten cumpliendo

5. **Gestión de Accesos y Usuarios:**
    - **Políticas de autenticación:** Revisión de contraseñas, uso de autenticación multifactor y gestión de sesiones y tiempo de duración de una contraseña
    - **Roles y permisos:** Evaluación de la asignación de permisos a usuarios según sus funciones.
    - **Registros de actividad:** Análisis de los logs para detectar accesos no autorizados o comportamientos anómalos.

Normas

En el marco de la auditoría del área de TI, es crucial identificar y describir las normas y estándares que servirán como referencia para evaluar la seguridad, los equipos, la infraestructura y los procesos. A continuación, se enumeran y describen las normativas y estándares más relevantes que aplican a esta auditoría.

Normas Internacionales y Estándares de Seguridad

- ISO/IEC 27001: Es el estándar internacional para la gestión de seguridad de la información. Proporciona un marco para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Su implementación garantiza la protección de la confidencialidad, integridad y disponibilidad de la información dentro de la organización.
- NIST SP 800-53: Proporciona un catálogo de controles de seguridad y privacidad desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST). Es una guía ampliamente utilizada para garantizar la seguridad de sistemas informáticos en organizaciones gubernamentales y privadas.

Normativas de Protección de Datos

- Ley General de Protección de Datos Personales (LGPD): En el caso de México, la LGPD regula cómo las organizaciones públicas y privadas manejan los datos personales, estableciendo principios como el consentimiento informado, la transparencia y la responsabilidad.

Estándares de Gestión y Gobierno de TI

- COBIT (Control Objectives for Information and Related Technologies): Desarrollado por ISACA, este marco está diseñado para garantizar que las TI estén alineadas con los objetivos estratégicos de la organización. Se utiliza para evaluar la efectividad, eficiencia y alineación estratégica de los procesos de TI.

Elaboración del programa

Plan de auditoria

Participantes clave:

José Alberto Sanchez Trejo

Director operativo

Fernando Jahzeel Lopez Vera

Encargado del área de Sistemas y TI

Sistemas TI y Desarrollo.

Metodología

Métodos utilizados

Para llevar a cabo la auditoría, se utilizaron los siguientes métodos:

1. **Entrevistas**
    a. Objetivo: Obtener información directa del personal clave sobre los procesos, políticas y controles en las áreas auditadas.
    b. Aplicación: Se realizaron entrevistas estructuradas y semi-estructuradas con responsables de las áreas auditadas para identificar fortalezas, debilidades y riesgos.
    c. Ventaja: Permite profundizar en temas específicos y aclarar dudas en tiempo real.
2. **Encuestas**
    a. Objetivo: Recopilar información y percepciones de manera anónima para evaluar la efectividad de los procesos y la satisfacción del personal con las herramientas y políticas de TI.
    b. Aplicación: Las encuestas se diseñaron con preguntas cerradas y abiertas, enfocándose en aspectos como la seguridad de la información, el uso de equipos y la gestión operativa.
    c. Ventaja: Facilita la obtención de datos cuantitativos y cualitativos, asegurando una mayor participación y honestidad en las respuestas.

3. **Observación Directa**
    a. Objetivo: Examinar el estado real de los equipos y procesos en su entorno operativo habitual.
    b. Aplicación: Se observaron actividades diarias y el uso de recursos tecnológicos para identificar posibles desviaciones de los procedimientos documentados.
    c. Ventaja: Proporciona una visión práctica y no mediada sobre el desempeño real de los equipos y procesos.

Estos métodos fueron seleccionados para garantizar que la recopilación de información fuera integral y basada tanto en la percepción del personal como en la evidencia objetiva.

Herramientas

Durante la auditoría, se emplearon las siguientes herramientas para estructurar y sistematizar la evaluación:

1. **Listas de Verificación**
    a. Propósito: Evaluar de manera ordenada el cumplimiento de normativas, estándares y políticas internas.
    b. Uso: Se elaboraron listas adaptadas a cada área, cubriendo aspectos como la seguridad de la información, el estado de los equipos, y los procesos operativos.
    c. Ventaja: Asegura que todos los puntos clave sean revisados, minimizando el riesgo de omisiones.
2. **Cuestionarios**
    a. Propósito: Recolectar información detallada y estructurada sobre los procesos y controles implementados en las áreas auditadas.
    b. Uso: Diseñados de acuerdo con los objetivos de la auditoría, se aplicaron a los responsables de las áreas evaluadas. Incluyeron preguntas abiertas y cerradas para abarcar tanto datos cuantitativos como cualitativos.
    c. Ventaja: Facilita la comparación de respuestas y permite identificar patrones o discrepancias en los procesos.

3. **Documentación de Soporte**
    a. Propósito: Validar información y proporcionar evidencia que respalde los hallazgos de la auditoría.
    b. Uso: Se recopilaron manuales, políticas internas, bitácoras de mantenimiento, reportes de incidentes, y otros documentos relevantes.
    c. Ventaja: Proporciona un marco de referencia para contrastar la práctica operativa con los estándares establecidos.

Estas herramientas aseguraron que la auditoría se realizara de manera sistemática, objetiva y alineada con las mejores prácticas.

Estándares

En la auditoría se emplearon estándares específicos para garantizar una recopilación y evaluación de información confiable y estructurada. A continuación, se describen los principales instrumentos utilizados:

1. Listas de Verificación
    a. Función: Actuar como guías estructuradas para evaluar el cumplimiento de requisitos específicos en las áreas auditadas.
    b. Uso: Estas listas se basaron en estándares internacionales y políticas internas, abarcando aspectos como la seguridad de la información, la infraestructura tecnológica, y los procedimientos operativos.
2. Cuestionarios
    a. Función: Capturar información detallada sobre los procesos y prácticas de las áreas auditadas.
    b. Uso: Dirigidos a los responsables de cada área, estos cuestionarios incluían preguntas relacionadas con el uso y mantenimiento de equipos, cumplimiento normativo, y gestión de la seguridad.
3. Documentos de Soporte
    a. Función: Validar y corroborar las respuestas obtenidas durante las entrevistas y los cuestionarios.

   b. Uso: Se revisaron manuales operativos, políticas internas, registros de mantenimiento y reportes de incidentes para evaluar el cumplimiento normativo y la correcta gestión de los recursos tecnológicos.

4. Observaciones Directas
   a. Función: Documentar hallazgos durante el análisis en sitio de los procesos y el estado de los equipos tecnológicos.
   b. Uso: Se registraron aspectos como el estado físico de los equipos, el cumplimiento de las medidas de seguridad, y la adecuación de los procedimientos operativos a las normativas vigentes.

Estos instrumentos facilitaron la recopilación de datos relevantes y contribuyeron a una evaluación integral de las áreas auditadas, respaldando cada hallazgo con evidencia tangible.

Procedimientos para la auditoría

En la auditoria al realizar los procedimientos para una revisión sistemática de diferentes aspectos relacionados con la operación, el mantenimiento y la gestión de la flota para garantizar la seguridad, la eficiencia y el cumplimiento de normativas legales.

1. Planificación

A. Identificar qué se auditará: vehículos, conductores, rutas, o procesos generales.
B. Establecer objetivos específicos, como mejorar la seguridad, reducir costos o garantizar el cumplimiento normativo.
C. Crear un checklist con los aspectos clave (documentos, mantenimiento, inspección física).
D. Reunir herramientas necesarias como formatos de inspección, herramientas de medición o acceso a sistemas de monitoreo (GPS).

2. Revisión Documental

A. Licencias de conductores: Verificar su vigencia y que sean del tipo adecuado (como licencia federal para transporte de carga pesada).
B. Permisos y seguros: Confirmar que los permisos de circulación están actualizados y que las pólizas de seguro cubren daños, responsabilidad civil y mercancías.
C. Solicitar y analizar los documentos de cada unidad y conductor.
D. Comparar los registros con las normativas vigentes y los requerimientos internos de la empresa.

3. Identificación de Hallazgos

A. Críticos: Riesgos que afectan la seguridad o el cumplimiento normativo inmediato (frenos dañados, licencias vencidas).
B. Moderados: Problemas que aumentan los costos o generan ineficiencias (rutas mal planificadas, desgaste prematuro).
C. Documentar cada hallazgo con evidencia (fotos, registros).
D. Asignar prioridad según el impacto y la urgencia.

4. Seguimiento

A. Realizar una auditoría de seguimiento.
B. Monitorear indicadores clave (reducción de fallas, cumplimiento normativo, costos).
C. Comparar los resultados con los hallazgos iniciales.
D. Ajustar estrategias si persisten problemas.

5. Generación de Informe

A. Resumen de hallazgos: Lista detallada de problemas detectados.
B. Recomendaciones: Acciones específicas para resolver cada hallazgo.
C. Plan de acción: Definir plazos, responsables y recursos necesarios para implementar las mejoras.

Instrumentos de Recopilación de información

En la auditoria los instrumentos de recopilación de información son esenciales para garantizar la seguridad, eficiencia y cumplimiento de regulaciones. Algunos de los más comunes son:

1. GPS (Sistema de Posicionamiento Global): Utilizados en la empresa que permite conocer la ubicación exacta de los vehículos en tiempo real, lo que ayuda a optimizar las rutas, controlar el uso del vehículo y garantizar la seguridad.

2. Tacógrafo: Un dispositivo que registra la velocidad, tiempo de conducción y descanso del conductor, asegurando que se cumplan las regulaciones de tiempos de manejo y descanso, como las establecidas por las autoridades de transporte.

3. Sensores de Combustible: Miden el nivel de combustible en el vehículo y monitorean el consumo de este, lo que ayuda a optimizar el uso de combustible y detectar posibles fugas o problemas mecánicos.

4. Cámaras de Seguridad: Se instalan en el interior y/o exterior del vehículo para monitorear el comportamiento del conductor, los pasajeros y la carga, mejorando la seguridad y proporcionando pruebas en caso de incidentes.

5. Software de Gestión de Flotas: Este software es fundamental para centralizar los datos provenientes de los vehículos (ubicación, rutas, tiempos, etc.) y analizar el desempeño de la flota en tiempo real.

Estos instrumentos ayudaran tanto en la gestión operativa como en la mejora de la seguridad y la eficiencia del transporte.

Técnicas de evaluación y técnicas especiales

Técnicas de Evaluación

1. Análisis de Documentos Financieros: Revisión de estados financieros, balances y reportes contables relacionados con el autotransporte. Esto ayuda a identificar problemas financieros y evaluar la rentabilidad y eficiencia operativa.

2. Auditoría de Costos: Evaluar los costos asociados a la operación del autotransporte (combustible, mantenimiento de vehículos, salarios, seguros, etc.). Esto permite detectar áreas de mejora y optimizar recursos.

3. Revisión de Cumplimiento Normativo: Verificación del cumplimiento de leyes y normativas locales, nacionales e internacionales sobre transporte de carga o pasajeros. Esto incluye licencias, seguros, permisos de circulación, y regulaciones ambientales.

4. Inspección de Seguridad Vial: Evaluación de las condiciones físicas de los vehículos para asegurar que estén en cumplimiento con los estándares de seguridad establecidos por las autoridades.

5. Análisis de Procesos: Evaluación de los procesos de gestión de transporte, como la programación de rutas, mantenimiento preventivo de vehículos, y procesos de carga y descarga.

Técnicas Especiales

1. Análisis de Uso de Combustible: Técnicas avanzadas para evaluar la eficiencia en el consumo de combustible de la flota, como la instalación de sistemas de telemetría que rastrean el rendimiento de cada vehículo en tiempo real.

2. Monitoreo GPS y Telemática: Utilizar sistemas de rastreo y telemetría para auditar el uso de las rutas, los tiempos de conducción y las condiciones operativas de los vehículos. Permite mejorar la eficiencia y la seguridad de las operaciones.

3. Evaluación de Mantenimiento Predictivo: Uso de tecnologías avanzadas para monitorear el estado de los vehículos en tiempo real, previendo fallos o necesidades de mantenimiento antes de que ocurran. Esto reduce costos por mantenimiento correctivo.

4. Cumplimiento Ambiental: Verificar el cumplimiento de las regulaciones ambientales, como la reducción de emisiones, el uso de vehículos menos contaminantes y la disposición adecuada de residuos.

5. Análisis de Datos de Accidentes y Seguridad: Estudiar los incidentes o accidentes ocurridos en la flota para determinar causas comunes y oportunidades de mejora en la seguridad de la operación.

Áreas de auditoría

1. **Cumplimiento Normativo:**

   - Cumple con las leyes y regulaciones de transporte terrestre, como las normas de seguridad, licencias, impuestos y regulaciones de tráfico.

2. **Gestión de Flota:**

   - La administración de vehículos, asegurando que estén bien mantenidos, asegurados y operando dentro de los límites establecidos por las normativas.

3. **Seguridad y Salud Ocupacional:**

   - Tomar las medidas necesarias para la seguridad de los conductores y el personal, incluyendo la capacitación adecuada, equipos de protección y prevención de accidentes.

4. **Costos Operativos:**

   - Evaluar los costos asociados con la operación de la flota, tales como mantenimiento, seguros, peajes, salarios de los conductores y otros gastos relacionados.

5. **Facturación y Control de Ingresos:**

   - Verificar que los ingresos generados por los servicios de transporte estén correctamente facturados, registrados y auditados.

6. **Contratos y Proveedores:**

   - Revisar los acuerdos con clientes y proveedores, incluyendo los contratos de servicios de transporte, arrendamiento de vehículos, seguros y otros contratos relacionados.

7. **Tecnología y Sistemas de Gestión:**

   - Evaluar los sistemas informáticos utilizados para el monitoreo de la flota, la gestión de órdenes, la facturación y otros procesos operativos.

Minuta de Reunión de apertura

Fecha: 10/12/24

Asistentes:

Director operativo.

Encargado de Sistemas de TI

Auditor líder y equipo

Temas tratados

1: Presentación del equipo auditor: explicación de roles y experiencia.

2: Objetivo de la Auditoria: verificar procesos de seguridad y eficiencia en el área de TI.

3: Alcance: Revisión de sistemas de TI, desarrollo web y mantenimiento de equipos.

4:Cronograma:

-Inicio [02/12/24]
-Revisión preliminar: [03/12/24]
-Informe final: [06/12/24]

5: Metodos y Técnicas: inspección, entrevistas, cuestionarios y pruebas tecnicas.

6: Solicitud de Documentación Inicial: Políticas, procedimientos y registros relevantes .

Acuerdos

-Colaboración y acceso a información por parte del equipo de TI
-Agendar para entrevistas y sesiones tecnicas

FIRMA DE ASISTENCIA

_____ _____

Recolección de información y documentación de las áreas auditadas

Informe con los hallazgos y conclusiones

Principales hallazgos:

1. Fortalezas:

- Existencia de políticas de seguridad básicas en TI.
- Uso de sistemas de encriptación como Script para datos sensibles.
- Procedimientos documentados para la gestión de activos y eliminación segura de datos.
- Licencias vigentes de software antivirus.

2. Áreas de oportunidad:

- Control de accesos: Falta de herramientas para monitoreo avanzado de accesos a sistemas críticos.
- Autenticación multifactorial: Solo se utiliza encriptación de contraseñas, sin MFA para accesos sensibles.
- Gestión de incidentes: No se cuenta con un equipo responsable ni con un plan integral para incidentes físicos o lógicos.
- Respaldo de información: No se evidenció la revisión periódica de los procedimientos de recuperación ante desastres.
- Auditoría de logs: Las revisiones de logs son esporádicas, lo que limita la identificación de patrones anómalos.

Conclusiones:

La empresa presenta un nivel básico de seguridad y gestión de TI, pero necesita implementar medidas más robustas en áreas críticas, como control de accesos, gestión de incidentes y monitoreo de sistemas. Se recomienda priorizar estas acciones para garantizar la continuidad operativa y la protección de los datos sensibles.

Recomendaciones:

- Implementar autenticación multifactorial (MFA).
- Adquirir herramientas para monitoreo y registro continuo de accesos.
- Capacitar al personal en respuesta a incidentes de TI.
- Establecer un plan anual de auditorías internas.

Minuta de Reunión de cierre

Fecha: [06/12/24]

Asistentes:
Director operativo.
Encargado de sistemas de TI.
Auditor líder y equipo.

Temas tratados:

1. Presentación de hallazgos:

- Resumen de las fortalezas y áreas de oportunidad identificadas en la auditoría.
- Ejemplos específicos de deficiencias, como la falta de autenticación multifactorial y monitoreo de accesos.

2. Recomendaciones clave:

- Implementar mejoras en seguridad de TI, incluyendo herramientas de monitoreo y autenticación avanzada.
- Revisión y actualización semestral de políticas de seguridad.
- Establecimiento de un equipo responsable para la gestión de incidentes.

3. Cronograma sugerido para la implementación de mejoras:

- Corto plazo (3 meses): Revisión de procedimientos de respaldo y adquisición de herramientas básicas de monitoreo.
- Mediano plazo (6 meses): Capacitación del personal y establecimiento de MFA.
- Largo plazo (12 meses): Plan integral de gestión de incidentes y auditorías regulares.

4. Resolución final:

- Acuerdo sobre los próximos pasos y compromiso por parte de los responsables de TI para aplicar las recomendaciones.

Acuerdos:

- Se programará una auditoría de seguimiento dentro de 6 meses para evaluar los avances.
- El equipo auditor proporcionará soporte técnico en la implementación de herramientas sugeridas.

Firma de asistencia:

_____ _____

Nombre y Firma Nombre y Firma

Presentación final

Título: Informe Final de Auditoría de Seguridad de TI en MS Autotransportes

Secciones del informe:

1. Introducción:
   - Objetivos, alcance y metodología de la auditoría.
2. Hallazgos:
   - Fortalezas y áreas de oportunidad con ejemplos específicos.
3. Recomendaciones:
   - Lista priorizada de acciones correctivas y preventivas.
4. Cronograma sugerido:
   - Tiempos estimados para la implementación de mejoras.
5. Conclusiones:
   - Impacto esperado de las recomendaciones en la seguridad y eficiencia de TI.

Formato de la presentación:

- Duración: x minutos.
- Material:
  - Resumen ejecutivo en diapositivas.
  - Documentación técnica detallada para el área de TI.
- Audiencia: Equipo directivo y área de TI de MS Autotransportes.

Solicitud de fecha para evaluar el seguimiento de mejora

Anexos

Políticas de seguridad de MS autotransportes

Políticas de Seguridad

1. *¿Cuál es el alcance y la cobertura de las políticas de seguridad de la información implementadas en el área de TIC, y cómo se asegura su cumplimiento en sistemas relacionados con la gestión de flotas y operaciones de transporte?*

   R: Nuestro alcance se limita al área interno de sistemas de red y divulgación de información (interna). En la segunda cuestión, manejamos aplicaciones web con las que monitoreamos los movimientos de nuestros empleados con nuestras unidades para poder garantizar el cumplimiento de su trabajo y el buen uso de nuestras unidades. Nuestra personal firma responsivas de confidencialidad con se trata de manejar las bases de datos.

2. *¿Con qué frecuencia se revisan y actualizan las políticas de seguridad de TIC para abordar amenazas específicas, como el acceso no autorizado a sistemas de rastreo o bases de datos de clientes?*

   R: Por lo menos una vez al año, pero de manera regular es semestral.

3. *¿Qué medidas se implementan para proteger los datos sensibles almacenados en los sistemas de TIC, como la información de clientes, rutas y vehículos?*

   R: Se hacen firmar responsivas de confidencialidad a nuestros empleados que tienen acceso, así como se procura que solo 1 o 2 tenga las claves de acceso a bases de datos. Se procura no concentrar información de clientes más allá de sus datos de facturación.

Gestión de Activos

1. *¿Existe un inventario actualizado de todos los activos tecnológicos, incluyendo servidores, estaciones de trabajo, dispositivos móviles, sistemas de GPS y equipos de red?*

   R: Sí, se hace de manera anual.

2. *¿Están designados y documentados los responsables de cada activo tecnológico, y se realiza un seguimiento de su uso en el área de TIC?*

   R: Están designados a sus áreas, el responsable es el responsable de esa área.

3. *¿Se han establecido políticas claras para el uso de sistemas y dispositivos tecnológicos, como el software de gestión de flotas y las aplicaciones de monitoreo?*

   R: Sí, se consultaron con un abogado las políticas y cada vez que alguien nuevo usará dicha aplicación se le capacita y enseñan dichas políticas.

4. *¿Existen protocolos para el retiro de equipos tecnológicos en desuso, garantizando la eliminación segura de datos almacenados?*

   R: Sí, tenemos contenedores de desechos tecnológicos y cada mes los transportamos a centros de desecho electrónico (como por ejemplo en la estación de bomberos).

Control de Accesos

1. *¿Cómo se gestiona el acceso a los sistemas de TIC, como servidores, aplicaciones de rastreo y bases de datos?*

   R: de manera física, no se cuenta con ningún tipo de protección dada el poco tránsito en la oficina que hay, los servicios de rastreo se subcontratan a una empresa y ella lleva a cabo su propia protección (todo mediante contrato.

2. *¿Se utilizan contraseñas seguras y se aplican políticas de autenticación para todos los usuarios de los sistemas de TIC?*

   R: Así es, se manejan modelos de encriptación a la hora de crear contraseñas.

3. *¿Se han implementado restricciones y controles de acceso basados en roles para los sistemas de TIC?*

   R: Sí, el único capaz de hacer grandes cambios es el encargado del área.

4. *¿Existen herramientas para supervisar y administrar los accesos a los sistemas críticos, como el software de monitoreo de vehículos?*

   R: No, aún está en planes adquirir o realizar una aplicación que lo permita.
   Seguridad Física y Ambiental.

5. *¿Se evalúan regularmente los riesgos físicos y ambientales que puedan afectar la infraestructura TIC, como servidores y centros de datos?*

   R: Una vez al año o de manera semestral en el caso de conexiones.

6. *¿Qué medidas físicas se implementan para proteger los equipos de TIC contra accesos no autorizados, robo o daño físico?*

   R: cierre de tráfico de información de nuestras bases de datos, investigación de los hechos ocurridos ese día que se reportó, análisis de las posibles causas y trato de corrección y refuerzo de seguridad en el área encontrada.

7. *¿Existe un plan de respuesta a incidentes para amenazas físicas, como incendios o cortes de energía, que afecten la infraestructura TIC?*

   R: Por el momento no.

Gestión de Incidentes en la Seguridad de la Información

15. *¿Qué herramientas de monitoreo de seguridad se utilizan para supervisar los sistemas TIC, como firewalls, sistemas de detección de intrusos y monitoreo de redes?*

    R: Amazon Web Service, nos notifica del transito en la red interna.

15. *¿Se ha designado un equipo responsable de gestionar la seguridad de la información en el área de TIC?*

    R: No.

15. *¿El plan de gestión de incidentes de seguridad de TIC se actualiza con las lecciones aprendidas tras cada evento?*

    R: Así es.

15. *¿Se guardan y revisan regularmente los registros de eventos de seguridad, como logs de acceso, alertas de sistemas y reportes de fallos?*

    R: Así es.

Seguridad Lógica

Control de Accesos Lógicos

1. *¿Existen políticas definidas para la creación, uso y renovación de contraseñas en los sistemas críticos?*

   R: Como tal solo las encriptamos y procuramos que el usuario solo tenga que usarla como una llave más.

2. *¿Se implementa autenticación multifactor (MFA) en los accesos a sistemas como la base de datos de clientes, software de gestión de flotas y servidores centrales?*

   R: Por el momento solo usamos la contraseña encriptada de la que comentamos.

3. *¿Cómo se controlan y registran los accesos de usuarios a sistemas operativos, bases de datos y aplicaciones críticas?*

   R: Los usuarios se dan de alta con el encargado de RH, mismo que pasa la información para que el encargado de TI los registre en el sistema interno y tengan sus debidos permisos.

Cifrado de Datos

5. *¿Están cifrados los datos sensibles almacenados en servidores, como información de clientes, registros de transporte y datos de vehículos?*

   R: Así es.

5. *¿Se utiliza cifrado en las comunicaciones entre dispositivos GPS, servidores centrales y aplicaciones móviles?*

   R: La empresa subcontratada nos ha comentado de sus sistema y hasta donde tenemos entendido sí manejan esa seguridad.

5. *¿Qué protocolos de cifrado se emplean (por ejemplo, TLS, AES) y están actualizados a estándares seguros?*

   R: Bcrypt (Hash unidireccional)

Protección contra Malware

8. ¿Se encuentran todos los dispositivos tecnológicos protegidos con software antivirus y antimalware actualizado?

   R: contamos con licencias de Macafy y los dispositivos se encuentran actualizados para evitar problemas.

8. ¿Se configuran alertas automáticas para detectar actividades sospechosas o presencia de programa maligno?

   R: solo las que proporciona el antivirus.

Segregación de Redes

13. *¿Se encuentran separadas físicamente o mediante VLANs la red operativa y la red administrativa?*

    R: De ambas maneras, solo contamos con 3 equipos para desarrollo y uno para administración y captura.

13. *¿Cómo se limita el acceso a las redes internas desde dispositivos externos, como laptops o dispositivos móviles?*

    R: Firewalls puestos en nuestro servidor y router de servicio de internet.

1. *¿Se emplean VPNs (redes privadas virtuales) para acceder a sistemas de la empresa desde ubicaciones remotas?*

R: No, para evitar fugas o una amenaza en el sistema adicional.

Monitorización y Registro

1. *¿Qué herramientas de monitoreo se utilizan para supervisar el tráfico de red y detectar actividades sospechosas?*

    R: Amazon web service.

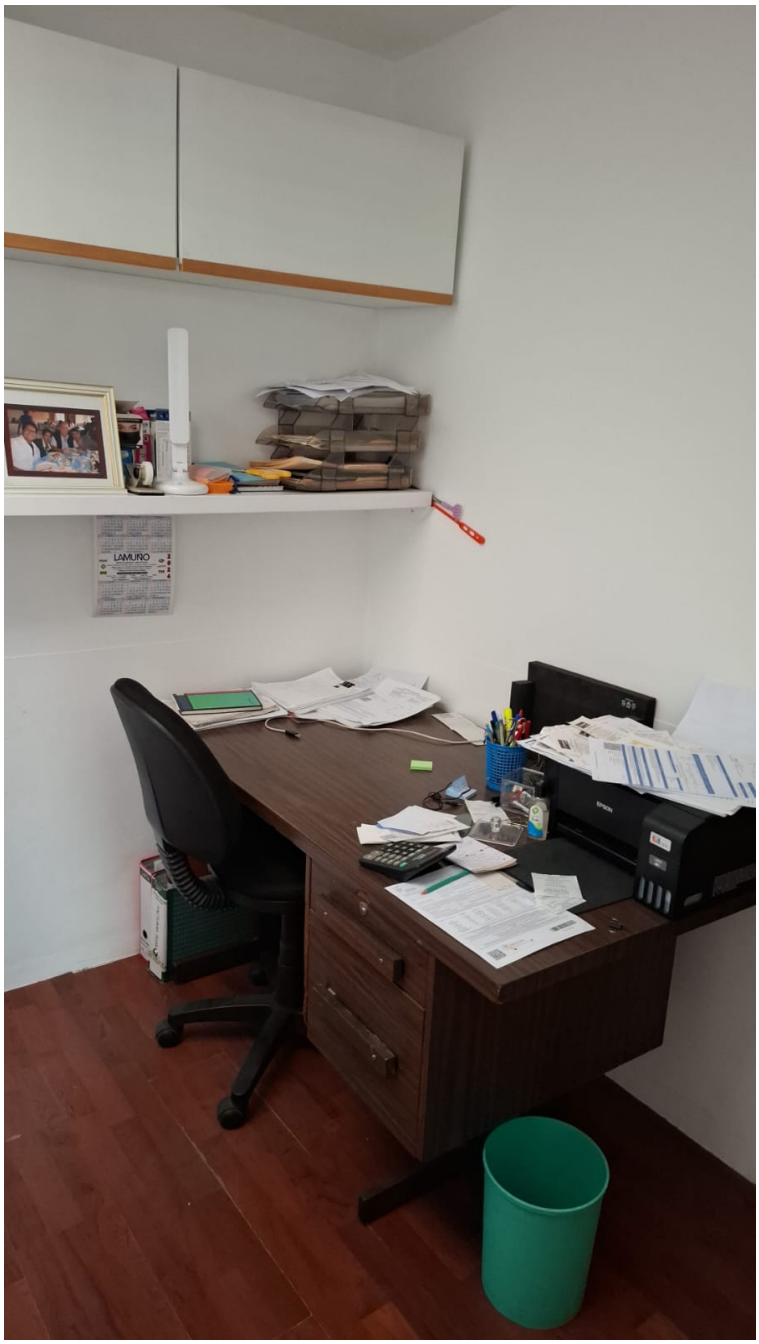
16. *¿Se revisan regularmente los logs de eventos y accesos para identificar posibles incidentes de seguridad?*

    R: No, pero si tenemos registro y es un poco esporádico cuando se realizan.

16. *¿Cómo se asegura la integridad y disponibilidad de los registros de auditoría?*

    R: tenemos un archivo que no se toca más que cuando toca hacer auditoria.

Evidencia Fotográfica




FACTURAS
PAPEL BOND
Offix