Informe de Auditoría Física

Titulo:

Informe de Auditoría Física de la cooperativa San Francisco

Resumen:

Objetivos:

Objetivo General:

Realizar una auditoría en la Cooperativa San Francisco con el fin de evaluar y mejorar la eficacia de sus procesos de gestión tributaria, garantizando así el cumplimiento adecuado de las obligaciones fiscales y contribuyendo a un desempeño financiero óptimo y sostenible de la organización.

Objetivos específicos:

- Revisar el marco normativo tributario que afecta a la cooperativa, identificando posibles riesgos y áreas de no conformidad.
- Proponer recomendaciones para fortalecer la gestión fiscal y la adecuada documentación de las transacciones.
- Identificar oportunidades para optimizar la eficiencia en el manejo de registros contables relacionados con aspectos fiscales.

Alcance:

Descripción de la institución:

Introducción:

La auditoría física llevada a cabo en la Cooperativa San Francisco se presenta como un proceso estratégico crucial para evaluar y optimizar la eficacia de las funciones operativas y administrativas de la organización. Este minucioso análisis se centra en examinar la calidad de la gestión de inventario, los procedimientos operativos, la implementación de estrategias logísticas y el cumplimiento normativo, con el propósito de fortalecer la gestión operativa y asegurar la alineación de las acciones con los objetivos operativos y regulatorios. A través de esta auditoría física, se busca no solo identificar áreas de mejora en la gestión operativa y la toma de decisiones logísticas, sino también fomentar una cultura organizacional sólida y alineada con la misión y visión de la cooperativa en el ámbito operativo. Este proceso contribuirá a la creación de una dirección más efectiva, capaz de adaptarse a los desafíos cambiantes del entorno empresarial, mejorar la eficiencia en la gestión de recursos físicos y garantizar el cumplimiento de normativas y prácticas de gobierno corporativo en el ámbito de la logística y operaciones.

Metodología:

Revisión de la unidad presentar Hasta ahora, la informática se ha centrado más en lo virtual que en lo físico, tratando las partes tangibles (como CPU, pantallas, teclados, etc.) como mero soporte de software. Sin embargo, el texto sostiene que la física informática no se limita a esto e incluye todo lo relacionado con el hardware y el entorno físico de un sistema, incluida la seguridad. La auditoría como medio de evaluación de la seguridad física en el ámbito profesional incluye no sólo comprobar la existencia de los medios físicos, sino también comprobar su funcionalidad, racionalidad y seguridad. Esto resultó en la necesidad de una "auditoría de seguridad física".

El documento señala que los límites entre los tipos de seguridad relacionada con la informática (seguridad lógica, seguridad física y seguridad de las comunicaciones) no están claros. Sin embargo, se sigue enfatizando la importancia de garantizar la integridad de los activos humanos, lógicos y físicos del Centro de Procesamiento de Datos (CPD). El texto enumera los tres pasos seguidos en orden cronológico después del error:

• Mantener un nivel adecuado de seguridad física, incluidas medidas para prevenir y mitigar errores.

• Se mencionan una serie de aspectos importantes como la ubicación del edificio, CPD, zonificación, elementos arquitectónicos, electricidad, sistema de protección contra incendios, control de acceso, dotación de personal, seguridad de los medios y duplicación de medios.

• Implementar planes de contingencia apropiados para responder a desastres que puedan perturbar el negocio.

• Se debe desarrollar un plan de recuperación de desastres que defina las tolerancias del sistema, los períodos críticos de recuperación y las prioridades de los procesos.

• También se mencionó la importancia de establecer centros de procesamiento de datos alternativos y servicios de comunicación y soporte seguros.

• Los contratos de seguro pueden cubrir pérdidas, gastos o responsabilidades que puedan surgir si el CPD falla.

• Enumera varios tipos de seguros, como centro de proceso y equipos, reconstrucción de medios de software, recargos, interrupción del negocio, documentos y registros valiosos, errores y omisiones, seguro de confiabilidad, transporte de medios, contratos de proveedores y mantenimiento. el campo de la seguridad física El texto señala la necesidad de abordar tres actividades relacionadas con la ocurrencia de un error: antes del evento, durante el evento y después del evento. Estas medidas deben tener en cuenta la ubicación del edificio y el entorno interno y externo que afecta al edificio.

Pero el texto subraya que el edificio en sí no está resuelto y cuestiona si los auditores informáticos están cualificados para examinar el estado de la construcción y su infraestructura y diagnosticar los problemas. La conclusión fue que el auditor no era competente ni estaba preparado para hacerlo y se recomendó un experto independiente.

Si una parte del edificio se confía a expertos, los intereses de los auditores se refieren a los aspectos físicos de la seguridad:

• Plan de organización Proporcionar información sobre la estructura organizativa de la empresa, departamentos, puestos y empleados. Permite analizar la separación funcional y la rotación de puestos de trabajo para garantizar la seguridad personal.

• Auditoría interna Los departamentos, ya sean independientes o relacionados con auditorías financieras, deben mantener registros de auditorías, normas, procedimientos y programas anteriores emitidos por órganos corporativos relacionados con la seguridad física.

• Gestion de seguridad Esto incluye los roles y responsabilidades de varios componentes como el director o responsable de la seguridad integral, el responsable de la seguridad informática, el administrador de la red, el administrador de la base de datos y el responsable de la seguridad activa y pasiva en el entorno físico. También se hace referencia a las normas y procedimientos emitidos y controlados por el Departamento.

• Centros e instalaciones de procesamiento de datos Dado el entorno físico del CPD, este debe poder realizar sus funciones computacionales. Las instalaciones adicionales también deberían garantizar la seguridad del personal y los suministros.

• Equipos y comunicación Esto se aplica a elementos clave del CPD, como servidores, terminales, ordenadores personales, almacenamiento de datos, impresoras y sistemas de telecomunicaciones. Se menciona su papel en el control de ubicación y control de acceso.

• computadora personal Se ha destacado la importancia de las computadoras personales, especialmente las computadoras personales en red que pueden acceder a datos, y surgen preocupaciones con respecto al acceso no autorizado y la adquisición de datos (hardware y software).

• Seguridad personal del personal Esto incluye acceso seguro, rutas de escape, sistemas de extinción de incendios, sistemas de bloqueo de puertas y ventanas, áreas de descanso y políticas emitidas por la gerencia con respecto al uso de las instalaciones por parte de los empleados. Fuentes de auditorías físicas CPD sigue esencialmente un modelo organizativo más o menos estándar, aunque por diversos motivos como tipo de negocio, situación financiera, disponibilidad de instalaciones, actitudes de gestión, etc. De hecho, hacen que los CPD sean muy diferentes entre sí. A continuación se detallan algunas de las fuentes a las que cada centro de datos debe tener acceso.

• Políticas, estándares y programas de seguridad emitidos y difundidos por los departamentos de dirección y seguridad de la empresa. • Auditorías previas totales y

parciales relacionadas con la seguridad física y cualquier otro tipo de auditoría. • Contratos de seguros, proveedores y mantenimiento. • Acceso al personal de seguridad, TI y otras actividades.

• Protocolos e informes del personal técnico y consultores. • Planificación de contingencias y evaluación de evidencias.

• Informes de visitas y visitas • Políticas de personal • Inventario de soporte

Propósito de la auditoría física: No existe otra finalidad que un orden basado en una lógica "externa" que determina los siguientes objetivos:

• arquitectura

• Equipo

• Equipos y telecomunicaciones

• datos

• seres humanos

Métodos y herramientas de los auditores:

Capacidad:

• Mantener instalaciones, sistemas y cumplir con estándares y procedimientos.

• Revision analitica:

1. Documentos de construcción y preinstalación.

2. Documentos de seguridad física

3. Políticas y regulaciones operativas locales

4. Normas y procedimientos de seguridad de datos físicos

5. Contratos de seguro y mantenimiento

• Negociaciones con la dirección y empleados permanentes o temporales.

• Consultas con técnicos y expertos en personal. herramienta:

• Cuaderno de campo/grabador de audio

• Cámara/videocámara

Deberes del auditor: Los auditores informáticos, especialmente los auditores internos, no deben dar la impresión a los usuarios de ordenadores ni a otros empleados de que sus actividades son funciones puramente policiales. Esto crea un ambiente tenso e incómodo que no favorece el normal desarrollo de las relaciones ni del trabajo. El auditor debe aparecer como un socio cooperativo que intenta ayudar. Se determina la siguiente responsabilidad de cada tipo de revisor:

Revisor de PC interno:

• Control relativo

• Verifique el procedimiento

• Evaluar el riesgo

• Consulte con la política y estándares de seguridad

• De la revisión planificada

• Revisar y monitorear las recomendaciones

Revisor de computadora externo:

• Consulte la función de los auditores internos

• La misma responsabilidad que los auditores internos • Verifique el plan de seguridad y emergencia

• Informar y sugerir

Fase de revisión física:

Fase 1: El alcance de la revisión Fase 2: mensaje general para obtener Tercera etapa: gestión y plan Fase 4: Plan de auditoría Fase 5: Resultados de las pruebas Sexta etapa: conclusión y comentarios Fase 7: un proyecto de revisión Fase 8: Discusión con las personas responsables del área Fase 9: Mensaje final

Recursos Materiales:

Revisión del plan de emergencia 2. Compra de información de fase • Acuerdo del plan de emergencia del emprendedor En este punto, la pregunta, que tiene como objetivo determinar el nivel general de conocimiento en el plan de emergencia, definió si se estableció la responsabilidad del plan y cómo consultar el presupuesto de la compañía sobre el presupuesto de la compañía en un plan de emergencia cuando el plan también estaba también implementado. • Acepte el proceso de reserva En este punto, debe recopilar información sobre el centro alternativo, así como si tiene un acuerdo legal cuando se mantiene un desastre, además de determinar si toda la propiedad cumple con los requisitos del Centro de datos y si cumple con el nivel de mantenimiento de las funciones, pruebas y evalúalos. • Protección de Datos En esta fase, recopile información sobre el estado de las copias de seguridad de los centros de datos externos que tienen copias de seguridad, cómo se obtuvieron esas copias de seguridad y si están respaldando todos los datos o solo algunos datos y, de ser así, en función de sus características, almacenamiento y prioridades de restablecimiento, tienen una clase. Verifique que la copia de seguridad tenga una periodicidad, la hora de la última copia de seguridad y que la copia de seguridad contenga copias de los archivos más recientes debido a su importancia. • Manual del plan de emergencia Esta etapa recopila información sobre el manual de emergencia, si incluye personas responsables de las diferentes fases y diferentes partes del plan, si ha sido simulado y probado y qué tan específico es para el nivel y la naturaleza del plan. desastre. Además de especificar cómo continuarán las operaciones luego de adquirir un

nuevo centro de operaciones o restaurar un centro de operaciones anterior. Es importante preguntar qué tan actualizado está el plan y la información que contiene.

Resultados:

Ejecución de la Auditoría Física:

Código A001 - Enrique Ortiz: Enrique Ortiz lideró la auditoría centrada en la seguridad física de documentos, comenzando el 15/02/2023 a las 09:00 y finalizando el 17/02/2023 a las 16:00. La calificación resultó en "Aprobado", indicando que se implementaron mejoras sugeridas durante la evaluación, demostrando un cumplimiento satisfactorio de las medidas de seguridad física.

Código A002 - Christian Chico: Christian Chico, del EQUIPO2, inició pruebas de phishing el 20/02/2023 a las 10:30, con la expectativa de finalizar el 24/02/2023 a las 15:00. La calificación está "Pendiente" hasta que se obtengan los resultados esperados para el 25/02/2023. Este enfoque en pruebas de seguridad refleja la evaluación continua de posibles vulnerabilidades.

Código A003 - Mauricio Villafuerte: Mauricio Villafuerte, del Equipo 2, está realizando una revisión del cumplimiento normativo desde el 28/02/2023 a las 08:00 hasta el 03/03/2023 a las 14:00. La calificación está "En Proceso", lo que sugiere que la auditoría aún no ha concluido, pero se espera que termine según la fecha programada.

Código A004 - Axel Vargas: Axel Vargas, también del Equipo 2, comenzó pruebas de seguridad en el acceso a documentos físicos el 10/03/2023 a las 11:00, con una estimación de finalización el 15/03/2023 a las 17:30. La calificación está "Pendiente", indicando que la evaluación está en curso y aún no ha concluido.

Código A005 - Enrique Ortiz: Enrique Ortiz, esta vez del Equipo 3, está actualmente revisando las políticas de contraseñas y la seguridad en el acceso a dispositivos de almacenamiento desde el 20/03/2023 a las 09:30. La calificación está "En Proceso", señalando que la auditoría está en curso y aún no se ha completado.

Código A006 - Christian Chico: Christian Chico del Equipo 2 está llevando a cabo pruebas de auditoría de logs desde el 05/04/2023 a las 09:00 hasta el 10/04/2023 a las 16:00. La calificación está "Pendiente", y se espera obtener resultados antes del 12/04/2023, indicando que la evaluación está en curso.

Código A007 - Enrique Ortiz: Enrique Ortiz, nuevamente del Equipo 2, está evaluando la seguridad de los correos electrónicos desde el 15/04/2023 a las 10:30. La calificación está "Pendiente", y se espera finalizar la revisión antes del 22/04/2023, señalando una evaluación en curso.

Código A008 - Axel Vargas: Axel Vargas del Equipo 1 comenzará la revisión de las políticas de contraseñas el 28/04/2023 a las 08:00, con una estimación de finalización el 03/05/2023 a las 14:00. La calificación está "Pendiente", indicando que la auditoría está en curso y aún no se ha completado.

Código A009 - Mauricio Villafuerte: Mauricio Villafuerte del Equipo 2 llevará a cabo pruebas de evaluación de backups desde el 10/05/2023 a las 11:00 hasta el 15/05/2023 a las 17:30. La calificación está "Pendiente", señalando que la evaluación está en curso y aún no ha concluido.

Código A010 - Christian Chico: Christian Chico del Equipo 3 realizará pruebas de phishing y concientización desde el 20/05/2023 a las 09:30 hasta el 24/05/2023 a las 13:00. La calificación está "Pendiente", indicando que la auditoría está en curso y aún no se ha completado.

Conclusiones:

Tras la exhaustiva realización de la auditoría en la Cooperativa San Francisco, se han obtenido valiosas percepciones que ofrecen una visión integral de la organización. La evaluación detallada de los procesos de toma de decisiones, liderazgo, gestión estratégica y salvaguarda de activos ha proporcionado una comprensión profunda de la salud organizacional de la cooperativa.

Recomendaciones:

Firmas de responsabilidad:

Anexos: