**Evidencia No 7.1**

**ISO 27001 (Controles) & Calidad**



**PARTE 1.**

El ***Anexo A*** de la NCh-ISO 27001:2013 contiene una completa lista de objetivos de control y controles.

En la presente actividad cooperativa con equipos de proyectos, realizaremos la revisión del ***Anexo A*** para asegurarse que ningún control necesario se pasó por alto.

Se debe generar una declaración de aplicabilidad que contenga los controles necesarios para implementar en su proyecto formativo además de la justificación de inclusiones.

| -Objetivos de control | Nombre / descripción de control | Control | Justificación de aplicabilidad al proyecto formativo | Tipo Requisito | | | Descripción requisito |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Funcional** | **No Funcional** | |
| **A.9.2.1** | Registro y cancelación de registro de usuario. | Se debe implementar un proceso de registro y cancelación de registro de usuario para habilitar la asignación de derechos de acceso. | Mantener control y seguridad frente a las personas que acceden al software a través de roles y estados de usuarios. | x | |  | Contamos con el registro de usuarios y la implementación de roles los cuales podrán ingresar al sistema por medio de los estados los cuales los podrá habilitar o inhabilitar el administrador o el dueño asignados en el sistema. |
| **A.5.1.2** | Revisión de las políticas de seguridad de la información | Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continuas. | Debemos mejorar el control específico para la información y cambios que se realicen en el sistema. |  | | x | Se tendrá en cuenta las políticas de datos que se cuentan en el sistema para realizar los cambios necesarios para el manejo de datos. |
| **A.6.1.1** | Roles y responsabilidades de la seguridad de la información | Todas las responsabilidades de la seguridad de la información deben ser  definidas y asignadas. | Se cuenta con la asignación de roles específicos los cuales solo ellos tienen acceso a la información asignada. | x | |  | Se maneja el sistema de roles dentro del sistema (Administrador, Dueño, Bodeguero,personal y jefe de inventario), cada uno tiene acceso a la información que les corresponde para llevar a cabo correctamente su función dentro del sistema |
| **A.6.1.2** | Segregación de funciones | Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización. | cada rol mantiene solo sus funciones asignadas no contara con acceso a información que no le corresponda | x | |  | Los roles que mantiene el sistema permiten que los roles solo mantengan el acceso a la información que les corresponda para que no haya fugas de información sin autorización. |
| **A.6.1.5** | Seguridad de la información en la gestión de proyecto | Se debe abordar la seguridad de la información en la gestión de proyecto, sin importar el tipo de proyecto. | se mantiene la seguridad sobre toda la información que entra y sale del proyecto |  | | x | Se mantienen medidas para que la información no esté vulnerable en algún momento que se acceda o se añada información relevante |
| **A.9.1.1** | Política de control de acceso | Se debe establecer, documentar y revisar una política de control de acceso basadas en los requisitos del negocio y de seguridad de la información. | Se debe manejar correctamente una documentación para el control de los accesos a la información. |  | | x | se contará con una documentación específica la cual debe manejar la información proporcionada para su seguridad y respaldo. |
| **A.9.2.2** | Asignación de acceso de usuario | Debe existir un procedimiento formal de asignación de acceso de usuario para asignar o revocar los derechos de acceso para todos los tipos de usuarios, a todos los sistemas y servicios. | Se cuenta con la modificación de estados y roles, los cuales funcionan para dar acceso al sistema. si el rol está pero no el estado este no podrá ingresar al sistema. | x | |  | El sistema debe controlar el acceso de los usuarios mediante dos maneras el rol asignado y el estado del usuario. Para que un usuario pueda ingresar al sistema, debe tener un rol válido y un estado que permita el acceso. Si falta uno de estos dos elementos, el acceso será denegado. |
| **A.9.2.3** | Gestión de derechos de acceso privilegiados | Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado. | La asignación de los derechos para accesos privilegiados se trabaja con los roles dentro del software, pues de esta manera ningún usuario puede acceder a información que no le corresponde saber durante el uso del sistema. | x | |  | El sistema cuenta con restricciones para que los roles tengan acceso a la información que necesitan, de esta manera ninguno cuenta con el acceso a información confidencial. |
| **A.9.2.4** | Gestión de información secreta de autenticación de usuarios | Se debe controlar la asignación de información de autenticación secreta mediante un proceso de gestión formal. | se implementó el uso de los roles para que el usuario solo se le muestre las funciones que tiene dentro del sistema | x | |  | El sistema ha implementado el uso de roles de usuario, de modo que cada usuario solo puede ver y acceder a las funciones específicas que le corresponden según su rol. Esta configuración asegura que la interfaz y las funcionalidades disponibles estén personalizadas según las responsabilidades y permisos de cada usuario, mejorando tanto la seguridad como la eficiencia operativa. |
| **A.9.3.1** | Uso de información de autenticación secreta | Se debe exigir a los usuarios el cumplimiento de las prácticas de la organización en el uso de la información de autenticación secreta. | Para autenticar los usuarios que ingresan se les pide ingresar el usuario y la contraseña registradas en el sistema, de esta manera ningún tercero puede acceder a la información con la que se cuenta. | x | |  | Para implementar la autenticación se realiza a través de un sistema de login donde se le pide proporcionar a la persona su usuario y su contraseña registrada dentro de la base de datos. |
| **A.9.4.1** | Restricción de acceso a la información | Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso. | se manejo el proceso de restringir funciones no correspondientes al rol que ingresó no le aparece por ningún lado las funciones de cualquier otro rol | x | |  | El sistema ha implementado un proceso para restringir las funciones que no corresponden al rol del usuario que ha ingresado. De esta manera, el usuario no puede ver ni acceder a las funciones de otros roles, garantizando que solo se le presenten las opciones y funcionalidades específicas de su rol. Esto mejora la seguridad y la claridad en el uso del sistema, evitando confusiones y accesos no autorizados. |
| **A.9.4.2** | Procedimientos de inicio de sesión seguro | Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro. | Se exige usuario y contraseña para poder acceder al sistema y la información que provee. | x | |  | Se cuenta con los campos de Usuario y Contraseña para todo usuario que quiera acceder al sistema, para esto se realiza la verificación de los datos comparándolos con lo que se tiene registrado en la base de datos |
| **A.9.4.3** | Sistema de gestión de contraseñas | Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad. | se unifica el proceso de validación de contraseña la cual cumpla con los requisitos necesarios para que sea una contraseña segura | x | |  | Se unifica el proceso de validación de contraseñas para asegurar que todas las contraseñas cumplan con los requisitos necesarios para ser consideradas seguras. Esto incluye criterios como longitud mínima, combinación de caracteres (letras mayúsculas, minúsculas, números y símbolos), Esta validación garantiza que las contraseñas sean robustas y protejan eficazmente contra accesos no autorizados. |
| **A.10.1.1** | Gestión de claves | Se debe desarrollar e implementar una política sobre el uso, protección y vida  útil de las claves criptográficas durante toda su vida útil. | Se debe tener en cuenta la tipografía en las contraseñas encriptadas, para así mantener su confidencialidad y privacidad de los clientes. |  | | x | Cada usuario al registrarse al sistema crea su propia contraseña en donde se guarda en la base de datos, pero para seguridad de nuestros clientes esta contraseña queda guardada encriptada, podríamos mejorarla para si llega actualizar esta contraseña aun así quede guardada encriptadamente. |
| **A.12.1.1** | Procedimientos de operación documentados | Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten. | se está aplicando mediantes los diferentes manuales que se realizan con las instrucciones correspondientes para cada usuario |  | | x | Se realizan los manuales con base a las responsabilidades de cada usuario para así mismo mantener un correcto uso del sistema. |
| **A.12.1.2** | Gestión de cambios | Se deben controlar los cambios a la organización, procesos de negocio, instalaciones de procesamiento de información y los sistemas que afecten la seguridad de la información. | Se aplican los cambios manteniendo la estabilidad del entorno y asegurando que se realicen de una manera controlada y eficiente. | x | |  | Se evalúan y se implementan los cambios de una manera sistemática para que así se pueda minimizar riesgos sin afectar la integridad, disponibilidad y confidencialidad de los datos y del sistema. |
| **A.12.1.3** | Gestión de la capacidad | Se debe supervisar y adaptar el uso de los recursos, y se deben hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema. | se aplicaría mediante las diferentes actualizaciones que se le van realizando al sistema |  | | x | se realizará un monitoreo al sistema para evaluar su rendimiento y asimismo poder realizar los diferentes ajustes, evitando problemas y garantizando un uso al sistema de manera eficiente |
| **A.12.2.1** | Controles contra código malicioso | Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios. | se aplicaron diferentes pruebas al código según su versionamiento para garantizar un uso completo y eficiente en el mismo | x | |  | se tendrán diferentes medidas para proteger el sistema y los datos mediante políticas de seguridad y un monitoreo continuo con el objetivo de prevenir amenazas para el código |
| **A.16.1.1** | Responsabilidades y  procedimientos | Se deben establecer responsabilidades y procedimientos de gestión para  asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información. | Es fundamental tener claras las responsabilidades y procedimientos para gestionar incidentes de seguridad de la información. Esto asegura que cualquier problema que afecte la integridad, disponibilidad o confidencialidad de los datos del inventario sea manejado rápidamente y de manera efectiva. |  | | X | Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información. Esto incluye la definición de roles específicos para la gestión de incidentes y la documentación de procedimientos a seguir en caso de incidentes. |
| **A.16.1.2** | Informe de eventos de  seguridad de la información | Se deben informar, lo antes posible, los eventos de seguridad de la información mediante canales de gestión apropiados. | La capacidad de informar rápidamente sobre eventos de seguridad es crucial para detectar y mitigar amenazas a tiempo. | X | |  | Se deben informar, lo antes posible, los eventos de seguridad de la información mediante canales de gestión apropiados. Esto implica establecer un sistema de reporte donde los usuarios puedan notificar cualquier evento sospechoso o incidente relacionado con la seguridad de la información. |
| **A.16.1.3** | Informe de las debilidades de seguridad de la información | Se debe requerir que los empleados y contratistas que usen los sistemas y servicios de información de la organización, observen e informen cualquier debilidad en la seguridad de la información en los sistemas o servicios, observada o que se sospeche. | Identificar y reportar debilidades en la seguridad de la información permite tomar acciones preventivas antes de que estas debilidades sean explotadas por amenazas externas o internas. | X | |  | Se debe requerir que los empleados y contratistas que usen los sistemas y servicios de información de la organización, observen e informen cualquier debilidad en la seguridad de la información en los sistemas o servicios, observada o que se sospeche. |
| **A.16.1.4** | Evaluación y decisión sobre los eventos de seguridad de la información | Los eventos de seguridad de la información se deben evaluar y decidir su van a ser clasificados como incidentes de seguridad de la información. | Evaluar y clasificar adecuadamente los eventos de seguridad es esencial para determinar su gravedad y la acción necesaria. En un sistema de inventario, esto asegura que se tomen medidas apropiadas según la naturaleza del evento, protegiendo así la continuidad y seguridad de las operaciones. | X | |  | Los eventos de seguridad de la información se deben evaluar y decidir si van a ser clasificados como incidentes de seguridad de la información. Esto implica tener criterios claros y procedimientos establecidos para la evaluación de eventos de seguridad. |
| **A.16.1.5** | Respuesta ante incidentes de seguridad de la información | Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados. | Tener un plan de respuesta documentado para incidentes de seguridad asegura que se actúe de manera consistente y efectiva cuando se presenten problemas. | X | |  | Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados. Esto incluye tener planes de respuesta que describan los pasos a seguir y las acciones a tomar en caso de un incidente de seguridad. |
| **A.16.1.6** | Aprendizaje de los incidentes de seguridad de la información | Se debe utilizar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros. | Aprender de los incidentes pasados y aplicar ese conocimiento ayuda a fortalecer la seguridad del sistema y prevenir futuros incidentes. |  | | X | Se debe utilizar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros. Esto implica documentar los incidentes, analizar las causas y actualizar las políticas y procedimientos de seguridad en consecuencia. |
| **A.16.1.7** | Recolección de evidencia | La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia. | En caso de un incidente de seguridad, tener procedimientos claros para la recolección de evidencia es crucial para cualquier investigación posterior. | X | |  | La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia. Esto incluye procedimientos para asegurar que toda la evidencia sea manejada de manera que se mantenga su integridad y validez. |
| **A.17.1.1** | Planificación de la continuidad de la seguridad de la información | La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre. | Es esencial determinar los requerimientos de seguridad de la información y planificar la continuidad de la gestión de la seguridad en situaciones adversas, como crisis o desastres. |  | | X | La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre. |
| **A.17.1.2** | Implementación de la continuidad de la seguridad de la información | La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa. | Después de planificar, es necesario implementar y mantener procesos, procedimientos y controles que aseguren la continuidad de la seguridad de la información. |  | | X | La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa. |
| **A.17.1.3** | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | La organización debe verificar, de manera periódica, los controles de continuidad de la seguridad de la información definida e implementada para asegurar que son válidos y eficaces durante situaciones adversas. | Para garantizar que los controles de continuidad de la seguridad de la información sean efectivos, es crucial verificarlos, revisarlos y evaluarlos periódicamente. |  | | X | La organización debe verificar, de manera periódica, los controles de continuidad de la seguridad de la información definida e implementada para asegurar que son válidos y eficaces durante situaciones adversas. |
| **A.17.2.1** | Disponibilidad de las instalaciones de procesamiento de la información | Las instalaciones de procesamiento de la información deben ser implementadas con la redundancia suficiente para cumplir con los requisitos de disponibilidad. | Para asegurar la disponibilidad del sistema de inventario, es importante implementar redundancias en las instalaciones de procesamiento de la información. | X | |  | Las instalaciones de procesamiento de la información deben ser implementadas con la redundancia suficiente para cumplir con los requisitos de disponibilidad. |
| **A.18.1.1** | Identificación de la legislación vigente y los requisitos contractuales | Todos los requisitos estatutarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización. | Es esencial identificar y documentar todos los requisitos legales, regulatorios y contractuales pertinentes para asegurar que el sistema de inventario cumpla con las normativas aplicables. Esto incluye leyes de protección de datos, requisitos contractuales con proveedores y otras regulaciones pertinentes al manejo de información del restaurante. |  | | X | Todos los requisitos estatutarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización. |
| **A.18.1.3** | Protección de los registros | Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio. | Los registros del sistema de inventario deben ser protegidos contra pérdida, destrucción, falsificación y acceso no autorizado. Esto asegura la integridad y disponibilidad de la información del inventario, lo cual es crítico para las operaciones del restaurante. | X | |  | Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio. |
| **A.18.1.4** | Privacidad y protección de la información de identificación personal | Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda. | Si el sistema de inventario maneja información de identificación personal (por ejemplo, datos de empleados que ingresan registros), es fundamental asegurar la privacidad y protección de dicha información conforme a la legislación vigente. Esto previene el mal uso o la exposición de datos sensibles. | X | |  | Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda. |
| **A.18.2.1** | Revisión independiente de la seguridad de la información | El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se debe revisar en forma independiente, a intervalos planificados, o cuando ocurran cambios significativos. | Realizar revisiones independientes de la seguridad de la información ayuda a identificar y corregir posibles fallos en la implementación de las políticas de seguridad |  | | X | El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se debe revisar en forma independiente, a intervalos planificados, o cuando ocurran cambios significativos. |
| **A.18.2.2** | Cumplimiento con las políticas y normas de seguridad | Los gerentes deben revisar con regularidad el cumplimiento del procesamiento y los procedimientos de seguridad que están dentro de su área de responsabilidad, de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes. | Es necesario que los gerentes revisen regularmente el cumplimiento de las políticas y normas de seguridad en sus áreas de responsabilidad. |  | | X | Los gerentes deben revisar con regularidad el cumplimiento del procesamiento y los procedimientos de seguridad que están dentro de su área de responsabilidad, de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes. |
| **A.18.2.3** | Verificación del cumplimiento técnico | Se deben verificar regularmente los sistemas de información en cuanto a su  cumplimiento con las políticas y normas de seguridad de la información de la  organización. | Verificar regularmente los sistemas de información respecto a su cumplimiento con las políticas y normas de seguridad asegura que se mantengan actualizados y alineados con los requisitos de seguridad. |  | | X | Se deben verificar regularmente los sistemas de información en cuanto a su cumplimiento con las políticas y normas de seguridad de la información de la organización. |

Ejemplo:



