# Anexo G – Declaración de aplicabilidad.

En la siguiente tabla se recoge la relación de controles de la ISO/IEC 27002:2013 y se especifica si es de aplicabilidad para Ícaro S.A. Además, se detalla la Descripción de exclusión del control en caso de no aplicarse o la descripción de cómo se implementa en caso de que se vaya a aplicar.

| **5. Políticas de seguridad de la información** | | | | |
|---|---|---|---|---|
| **Punto** | **Control ISO/IEC 27002:2013** | **Aplica** | **Estado Actual** | **Descripción** |
| 5.1. Directrices de gestión de la seguridad de la información | | | | |
| 5.1.1 | Políticas para la seguridad de la información | SI | 1.Ejecutado | Se tienen que definir las políticas de seguridad de la información que sean aprobadas por la dirección y comunicadas a todos los trabajadores. |
| 5.1.2 | Revisión de las políticas para la seguridad de la información | SI | 1.Ejecutado | Las políticas de seguridad deben ser revisadas con cierta frecuencia o cuando ocurran cambios significativos. |
| **6. Organización de la seguridad de la información** | | | | |
| 6.1. Organización interna | | | | |
| 6.1.1 | Roles y responsabilidades en seguridad de la información | SI | 1.Ejecutado | Deben definirse y asignarse todas las responsabilidades relativas a la seguridad de la información. |
| 6.1.2 | Segregación de tareas | SI | 1.Ejecutado | Las funciones y tareas se deben segregar para reducir las modificaciones no autorizadas, no intencionadas o usos indebidos |
| 6.1.3 | Contacto con las autoridades | SI | 1.Ejecutado | Se deben mantener los contactos apropiados con las autoridades pertinentes en los casos necesarios. |
| 6.1.4 | Contacto con grupos de interés especial | SI | 0.Incompleto | Se deben mantener contactos con grupos de interés especial para la mejora del conocimiento. |
| 6.1.5 | Seguridad de la información en la gestión de proyectos. | SI | 0.Incompleto | Se tiene que integrar para identificar los riesgos en el marco de cada proyecto. |

| 6.2. Los dispositivos móviles y el teletrabajo | | | | |
|---|---|---|---|---|
| **Punto** | **Control ISO/IEC 27002:2013** | **Aplica** | **Estado Actual** | **Descripción** |
| 6.2.1 | Política de dispositivos móviles | SI | 0.Incompleto | Adoptar política de seguridad de dispositivos móviles para asegurar que no comprometen la seguridad de la información de la empresa. |
| 6.2.2 | Teletrabajo | SI | 0.Incompleto | Se deben implementar política y medios técnicos para proteger la información accedida desde fuera del centro de trabajo. |
| **7. Seguridad relativa a los RRHH** | | | | |
| 7.1. Antes del empleo | | | | |
| 7.1.1 | Investigación de antecedentes | SI | 0.Incompleto | Se deben comprar los antecedentes de las nuevas incorporaciones de acuerdo a la ley |
| 7.1.2 | Términos y condiciones del empleo | SI | 1.Ejecutado | Se deben establecer los términos y condiciones del contrato en lo que respecta a seguridad de la información para protegerla. |
| 7.2. Durante el empleo | | | | |
| 7.2.1 | Responsabilidad de gestión | SI | 1.Ejecutado | La dirección debe exigir cumplir las normas de seguridad a contratistas y empleados. |
| 7.2.2 | Concienciación, educación y capacitación en seguridad de la información | SI | 0.Incompleto | Los empleados y contratistas deben recibir la formación adecuada. |
| 7.2.3 | Poder disciplinario | SI | 0.Incompleto | Debe existir un proceso disciplinario formal que recoja las acciones a tomar en caso de que se haya provocado una brecha de seguridad que sirva de formula preventiva. |
| 7.3. Finalización del empleo o cambio de puesto de trabajo | | | | |
| 7.3.1 | Responsabilidades ante la finalización o cambio | SI | 0.Incompleto | Se deben definir, comunicar y cumplir las responsabilidades una vez finalizado el contrato o el cambio para proteger los intereses de la empresa. |

| 8. Gestión de activos | | | | |
|---|---|---|---|---|
| **Punto** | **Control ISO/IEC 27002:2013** | **Aplica** | **Estado Actual** | **Descripción** |
| 8.1. Responsabilidad sobre los activos | | | | |
| 8.1.1 | Inversión sobre los activos | SI | 1.Ejecutado | Los activos deben estar claramente identificados y debería crearse y mantenerse un inventario de los mismos para identificar las medidas de protección adecuadas y su responsabilidad, |
| 8.1.2 | Propiedad de los activos | SI | 0.Incompleto | Todos los activos del inventario deberían tener un propietario. |
| 8.1.3 | Uso aceptable de los activos | SI | 1.Ejecutado | Se deben identificar, documentar e implementar las reglas de uso aceptable de los activos. |
| 8.1.4 | Devolución de activos | SI | 1.Ejecutado | Todos los empleados y terceros deben entregar todos los activos. |
| 8.2. Clasificación de la información | | | | |
| 8.2.1 | Clasificación de la información | SI | 0.Incompleto | La información debe ser clasificada según la importancia con objeto de que reciba un adecuado nivel de protección. |
| 8.2.2 | Etiquetado de la información | SI | 0.Incompleto | Se debe desarrollar e implantar un método de etiquetado de la información. |
| 8.2.3 | Manipulado de la información | SI | 0.Incompleto | Se debe desarrollar e implantar un conjunto adecuado de procedimientos para la manipulación de la información. |
| 8.3. Manipulación de los soportes | | | | |
| 8.3.1 | Gestión de los soportes extraíbles | SI | 0.Incompleto | Se deben implantar los procedimientos para la gestión de soportes extraíbles según el esquema de clasificación adoptado. |
| 8.3.2 | Eliminación de soportes | SI | 0.Incompleto | Los soportes deben eliminarse de forma segura para evitar fugas de información |
| 8.3.3 | Soportes físicos en tránsito | SI | 0.Incompleto | Los soportes en tránsito deben estar protegidos frente a accesos no autorizados. |

| 9. Control de acceso | | | | |
|---|---|---|---|---|
| **Punto** | **Control ISO/IEC 27002:2013** | **Aplica** | **Estado Actual** | **Descripción** |
| 9.1. Requisitos de negocio para el control de acceso | | | | |
| 9.1.1 | Política de control de acceso | SI | 0.Incompleto | Se debe implementar una política de control de acceso para limitar el mismo a los recursos y a la información |
| 9.1.2 | Accesos a las redes y a los servicios de red | SI | 2.Gestionado | Solo se debe proporcionar acceso a las redes y servicios a los usuarios autorizados. |
| 9.2. Gestión de acceso de usuario | | | | |
| 9.2.1 | Registro y baja de usuario | SI | 1.Ejecutado | Se debe implantar un procedimiento que haga posible la asignación de derechos de acceso. |
| 9.2.2 | Provisión de acceso a usuarios | SI | 1.Ejecutado | Se debe implantar un procedimiento que haga posible la asignación de derechos de acceso. |
| 9.2.3 | Gestión de privilegios de acceso | SI | 1.Ejecutado | La asignación y el uso de privilegios debe estar restringida y controlada. |
| 9.2.4 | Gestión de la información secreta de autenticación de usuario | SI | 1.Ejecutado | La asignación de la información secreta debe ser controlada a través de un proceso forma de gestión. |
| 9.2.5 | Revisión de los derechos de acceso de usuario | SI | 0.Incompleto | Los propietarios de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares |
| 9.2.6 | Retirada o reasignación de los derechos de acceso | SI | 1.Ejecutado | Los derechos de acceso a la información y a sus recursos deben ser retirados al finalizar la relación |
| 9.3. Responsabilidad del usuario | | | | |
| 9.3.1 | Uso de la información secreta de autenticación. | SI | 1.Ejecutado | Se debe requerir a los usuarios el uso de la información secreta de autenticación para que sean responsables de salvaguardar la información |

| 9.4. Control de acceso a sistemas y aplicaciones | | | | |
|---|---|---|---|---|
| **Punto** | **Control ISO/IEC 27002:2013** | **Aplica** | **Estado Actual** | **Descripción** |
| 9.4.1 | Restricción del acceso a la información | SI | 1.Ejecutado | Se debe restringir el acceso a la información y a las funciones de las aplicaciones para prevenir el acceso no autorizado. |
| 9.4.2 | Procedimientos seguros de inicio de sesión | SI | 1.Ejecutado | Se debe controlar el acceso a los sistemas de forma controlada mediante inicio de sesión. |
| 9.4.3 | Sistema de gestión de contraseñas | SI | 1.Ejecutado | Los procesos de gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas. |
| 9.4.4 | Uso de utilidades con privilegios del sistema | SI | 0.Incompleto | Se debe controlar el uso de utilidades que pueden ser capaces de invalidar los sistemas con accesos privilegiados. |
| 9.4.5 | Control de acceso al código fuente de los programas | SI | 0.Incompleto | Se debe restringir el código acceso a los programas para evitar su manipulación y filtración. |
| **10. Criptografía** | | | | |
| 10.1. Controles criptográficos | | | | |
| 10.1.1 | Política de uso de los controles criptográficos | SI | 0.Incompleto | Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información. |
| 10.1.2 | Gestión de claves | SI | 0.Incompleto | Se debe desarrollar e implantar una política sobre el ciclo de vida de claves |
| **11. Seguridad física y del entorno** | | | | |
| 11.1. Áreas seguras | | | | |
| 11.1.1 | Perímetro de seguridad física | SI | 0.Incompleto | Se deben utilizar sistemas para proteger el perímetro de seguridad para proteger áreas que contienen información sensible. |
| 11.1.2 | Controles físicos de entrada | SI | 0.Incompleto | Las áreas seguras deben estar protegidas mediante controles de entrada adecuados. |
| 11.1.3 | Seguridad de oficinas, despachos y recursos. | SI | 0.Incompleto | Se debe aplicar métodos de seguridad física para estos entornos. |

| Punto | Control ISO/IEC 27002:2013 | Aplica | Estado Actual | Descripción |
|---|---|---|---|---|
| 11.1.4 | Protección contra las amenazas externas ambientales | SI | 0.Incompleto | Se debe implementar protección física contra desastres naturales, ataques provocados por el hombre o accidentes. |
| 11.1.5 | El trabajo en áreas seguras | SI | 0.Incompleto | Se debe implementar procedimientos de trabajos en áreas seguras como el centro de datos. |
| 11.1.6 | Áreas de carga y descarga | SI | 0.Incompleto | Se deben controlar las áreas de carga y descarga para prevenir accesos no autorizados. |
| 11.2. Seguridad de los equipos | | | | |
| 11.2.1 | Emplazamiento y protección de equipos | SI | 0.Incompleto | Los equipos se deben proteger de forma que se reduzcan los riesgos de pérdida, daño o robo. |
| 11.2.2 | Instalación de suministros | SI | 3.Establecido | Los equipos deberán estar protegidos contra fallos de alimentación |
| 11.2.3 | Seguridad del cableado | SI | 1.Ejecutado | El cableado eléctrico y de telecomunicaciones deberá estar protegido frente intercepciones, interferencias o daños. |
| 11.2.4 | Mantenimiento de los equipos | SI | 2.Gestionado | Se debe implantar un correcto mantenimiento sobre los equipos y sistemas. |
| 11.2.5 | Retiradas de materiales propiedad de la empresa | SI | 0.Incompleto | Sin autorización no se deben sacar los equipos y sistemas de las instalaciones de la empresa. |
| 11.2.6 | Seguridad de los equipos fuera de las instalaciones | SI | 0.Incompleto | Se debe aplicar medidas de seguridad para los equipos situados fuera de las instalaciones. |
| 11.2.7 | Reutilización o eliminación segura de equipos | SI | 0.Incompleto | Se debe comprobar que todos los soportes con información sensible de elimine de manera segura. |
| 11.2.8 | Equipo de usuario desatendido | SI | 1.Ejecutado | Los usuarios deben asegurarse que el equipo queda bloqueado cuando esté desatendido. |
| 11.2.9 | Política de puesto de trabajo despejado y pantalla limpia | SI | 0.Incompleto | Se debe mantener el puesto de trabajo libre de información confidencial, así como soportes de almacenamiento. |

| 12. Seguridad de las operaciones | | | | |
|---|---|---|---|---|
| **Punto** | **Control ISO/IEC 27002:2013** | **Aplica** | **Estado Actual** | **Descripción** |
| 12.1. Procedimientos y responsabilidades operacionales | | | | |
| 12.1.1 | Documentación de procedimientos de las operaciones | SI | 0.Incompleto | Se deben documentar y mantener la documentación de las operaciones y ponerla a disposición de los usuarios que la necesiten |
| 12.1.2 | Gestión de cambios | SI | 0.Incompleto | Los cambios que afecten a la seguridad de la información deben ser controlados |
| 12.1.3 | Gestión de capacidades | SI | 1.Ejecutado | Se debe supervisar y ajustar la utilización de los recursos a la demanda de capacidad presente y de proyectos futuros. |
| 12.1.4 | Separación de los recursos de desarrollo, prueba y producción | SI | 1.Ejecutado | Se deben separar estos entornos para evitar riesgos de acceso no autorizados o cambios. |
| 12.2. Protección contra software malicioso | | | | |
| 12.2.1 | Controles contra código malicioso | SI | 2. Gestionado | Se deben implantar sistemas de control contra malware en los sistemas |
| 12.3. Copias de seguridad | | | | |
| 12.3.1 | Copias de seguridad de la información | SI | 1.Establecido | Se deben realizar copias de seguridad de la información crítica con la política de seguridad acordada. |
| 12.4. Registros y supervisión | | | | |
| 12.4.1 | Registros de eventos | SI | 0.Incompleto | Se deben registras los eventos de los sistemas, protegerlos y revisarlos periódicamente. |
| 12.4.2 | Protección de la información de registro | SI | 0.Incompleto | Los dispositivos de registro y la información afín deben ser correctamente protegida. |
| 12.4.3 | Registros de administración y operación | SI | 0.Incompleto | Se deben registrar, proteger y revisar los registros de administración de los sistemas |
| 12.4.4 | Sincronización de reloj | SI | 0.Incompleto | Los relojes de todos los sistemas de la empresa deben estar sincronizados desde una fuente única y precisa |

| 12.5. Seguridad de las operaciones | | | | |
|---|---|---|---|---|
| **Punto** | **Control ISO/IEC 27002:2013** | **Aplica** | **Estado Actual** | **Descripción** |
| 12.5.1 | Instalación del software en explotación | SI | 0.Incompleto | Se deben implementar procedimientos para controla la instalación de software en explotación |
| 12.6. Gestión de la vulnerabilidad técnica | | | | |
| 12.6.1 | Gestión de las vulnerabilidades técnicas | SI | 0.Incompleto | Se debe obtener información de las vulnerabilidades técnicas de los sistemas, evaluarlas y adoptar medidas de seguridad para mitigar el riesgo. |
| 12.6.2 | Restricción en la instalación de software | SI | 1.Ejecutado | Se deben aplicar reglas que rijan la instalación de software por parte de los empleados. |
| 12.7. Consideraciones sobre la auditoria de sistemas de información | | | | |
| 12.7.1 | Controles de auditorías de sistemas de información. | SI | 0.Incompleto | Se deberán planificar y ejecutar las auditorias pactadas en la política de seguridad |
| **13. Seguridad de las comunicaciones** | | | | |
| 13.1. Gestión de la seguridad de redes | | | | |
| 13.1.1 | Controles de red | SI | 2.Gestionado | Se deben implantar sistemas para gestionar, controlar y proteger la red de la empresa. |
| 13.1.2 | Seguridad de los servicios de red | SI | 0.Incompleto | Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red |
| 13.1.3 | Segregación de redes | SI | 2.Gestionado | Los grupos de servicios de información, sistemas y usuarios deben estar segregados en redes distintas |
| 13.2. Intercambio de información | | | | |
| 13.2.1 | Políticas y procedimientos de intercambio de información | SI | 0.Incompleto | Se deben implantar políticas que protejan la información cuando sea trasferida |
| 13.2.2 | Acuerdos de intercambio de información | SI | 0.Incompleto | Se deben establecer acuerdos para el intercambio seguro de información con terceros. |
| 13.2.3 | Mensajería electrónica | SI | 1.Ejecutado | La información objeto de mensajería electrónica debe estar adecuadamente protegida. |

| Punto | Control ISO/IEC 27002:2013 | Aplica | Estado Actual | Descripción |
|---|---|---|---|---|
| 13.2.4 | Acuerdos de confidencialidad o no revelación. | SI | 0.Incompleto | Se deben implementar y revisar acuerdos de no revelación de la información con terceros. |
| **14. Adquisición, desarrollo y mantenimiento de los sistemas de información.** | | | | |
| 14.1. Requisitos de seguridad en sistemas de información | | | | |
| 14.1.1 | Análisis de requisitos y especificaciones de seguridad de la información | SI | 0.Incompleto | Los nuevos sistemas implementados deben cumplir los requisitos de seguridad de la información. |
| 14.1.2 | Asegurar los servicios de aplicaciones en redes públicas | SI | 1.Ejecutado | Se debe proteger la información que se transmite a través de redes públicas |
| 14.1.3 | Protección de las transacciones de servicios de aplicaciones | SI | 0.Incompleto | Se debe proteger las transacciones de servicios de aplicaciones |
| 14.2. Seguridad en el desarrollo y en los procesos de soporte | | | | |
| 14.2.1 | Política de desarrollo seguro | SI | 0.Incompleto | Se deben establecer y aplicar normas para el desarrollo seguro de las aplicaciones de la empresa |
| 14.2.2 | Procedimiento de control de cambios en sistemas | SI | 1.Ejecutado | La implantación de cambios debe controlarse a lo largo del ciclo de vida mediante procedimientos formales. |
| 14.2.3 | Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo | SI | 0.Incompleto | Cuando se realicen cambios en los Sistemas Operativos las aplicaciones de negocio críticas deben ser revisadas y probadas. |
| 14.2.4 | Restricciones a los cambios en los paquetes software | SI | 0.Incompleto | Por norma no se permiten modificaciones en los paquetes software |
| 14.2.5 | Principios de ingeniería de sistemas seguros | SI | 0.Incompleto | Se deberían establecer, documentar, mantener y aplicarse principios de ingeniería seguros a todos los sistemas de información de la empresa. |
| 14.2.6 | Entorno de desarrollo seguro | SI | 1.Ejecutado | Se deben proteger adecuadamente los entornos de desarrollo seguro |
| 14.2.7 | Externalización del desarrollo de software | NO | | |

| Punto | Control ISO/IEC 27002:2013 | Aplica | Estado Actual | Descripción |
|---|---|---|---|---|
| 14.2.8 | Pruebas funcionales de seguridad de sistemas | SI | 2.Gestionado | Se deben llevar a cabo pruebas funciones durante el desarrollo de aplicaciones |
| 14.2.9 | Pruebas de aceptación de sistemas | SI | 2.Gestionado | Se deben establecer baterías de pruebas de aceptación y criterios relacionados para nuevos sistemas que pasen a producción |
| 14.3. Datos de prueba | | | | |
| 14.3.1 | Protección de los datos de prueba | SI | 0.Incompleto | Los datos de prueba se deben seleccionar con cuidado |
| 14.1.2 | Asegurar los servicios de aplicaciones en redes públicas | SI | 1.Ejecutado | Se debe proteger la información que se transmite a través de redes públicas |
| 14.1.3 | Protección de las transacciones de servicios de aplicaciones | SI | 0.Incompleto | Se debe proteger las transacciones de servicios de aplicaciones, ser protegidos y controlados. |
| **15. Relación con proveedores** | | | | |
| 15.1. Seguridad en las relaciones con proveedores | | | | |
| 15.1.1 | Política de seguridad de la información en las relaciones con los proveedores | SI | 0.Incompleto | Se deben acordar las políticas de acceso de los proveedores a los sistemas de información de la empresa y a los activos. |
| 15.1.2 | Requisitos de seguridad en contratos con terceros | SI | 0.Incompleto | Se deben establecer y acordar con cada proveedor los requisitos relacionados con la seguridad. |
| 15.1.3 | Cadena de suministro de tecnología de la información y de las comunicaciones | SI | 0.Incompleto | La cadena de suministros acordada con los proveedores debe incluir requisitos ante los riesgos relacionados con las TIC |
| 15.2. Gestión de la provisión de servicios del proveedor | | | | |
| 15.2.1 | Control y revisión de la provisión de servicios del proveedor | SI | 0.Incompleto | Se debe controlar, revisar y auditar los servicios de proveedor |
| 15.2.2 | Gestión de cambios en la provisión del servicio del proveedor | SI | 0.Incompleto | Se deben gestionar los cambios en la provisión del servicio proporcionado por lo profesores teniendo en cuenta la criticidad del sistema. |

| 16. Gestión de incidentes de seguridad de la información | | | | |
|---|---|---|---|---|
| **Punto** | **Control ISO/IEC 27002:2013** | **Aplica** | **Estado Actual** | **Descripción** |
| 16.1. Gestión de incidentes de seguridad de la información y mejoras | | | | |
| 16.1.1 | Responsabilidades y procedimientos | SI | 0.Incompleto | Se deben establecer responsabilidades y procesos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes |
| 16.1.2 | Notificación de los eventos de seguridad de la información | SI | 0.Incompleto | Los eventos de seguridad de la información se deberán notificar por los canales de gestión adecuados lo antes posible |
| 16.1.3 | Notificación de puntos débiles de la seguridad | SI | 0.Incompleto | Todos los usuarios deben notificar cualquier punto que afecte a la seguridad de la información |
| 16.1.4 | Evaluación y decisión sobre los eventos de seguridad de la información | SI | 0.Incompleto | Los eventos de seguridad de la información deben ser evaluados y clasificados apropiadamente. |
| 16.1.5 | Respuesta a incidentes de seguridad de la información | SI | 0.Incompleto | La respuesta a incidentes deberá ser de acuerdo a procedimientos documentados. |
| 16.1.6 | Aprendizaje de los incidentes de seguridad de la información | SI | 0.Incompleto | El conocimiento obtenido de los incidentes de seguridad deberá ser utilizado para reducir la probabilidad de ocurrencia a futuro |
| 16.1.7 | Recopilación de evidencias | SI | 0.Incompleto | Se deben definir y aplicar procedimientos para la aplicación, recogida, adquisición y preservación de información que pueda servir de evidencia. |

| 17. Aspectos de seguridad de la información par la gestión de la continuidad del negocio | | | | |
|---|---|---|---|---|
| **Punto** | **Control ISO/IEC 27002:2013** | **Aplica** | **Estado Actual** | **Descripción** |
| 17.1. Planificación de la continuidad de la seguridad de la información | | | | |
| 17.1.1 | Planificación de la continuidad de la seguridad de la información | SI | 0.Incompleto | Se debe determinar las necesidades de continuidad de negocio para la gestión de la seguridad de la información en situaciones adversas |
| 17.1.2 | Implementar la continuidad de la seguridad de la información | SI | 0.Incompleto | Se debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información en situaciones adversas |
| 17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | SI | 0.Incompleto | Se deben controlar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces |
| 17.2. Redundancias | | | | |
| 17.2.1 | Disponibilidad de los recursos de tratamiento de la información | SI | 0.Incompleto | Los recursos que tratan la seguridad de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de seguridad |
| | | | | |

| 18. Cumplimiento | | | | |
|---|---|---|---|---|
| **Punto** | **Control ISO/IEC 27002:2013** | **Aplica** | **Estado Actual** | **Descripción** |
| 18.1. Cumplimiento de los requisitos legales y contractuales | | | | |
| 18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales | SI | 1.Ejecutado | Todos los requisitos pertinentes y el enfoque de la empresa para cumplirlos se deben definir de forma explícita documentarse y mantenerse actualizados |
| 18.1.2 | Derechos de propiedad intelectual | SI | 1.Ejecutado | Se deben implementar procedimientos adecuados para garantizar el cumplimiento de los requisitos legales respecto a los derechos de propiedad intelectual. |
| 18.1.3 | Protección de los registros de la organización | SI | 0.Incompleto | Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizado. |
| 18.1.4 | Protección y privacidad de la información de carácter personal | SI | 0.Incompleto | Se debe garantizar la protección y la privacidad de los datos según la regulación vigente |
| 18.1.5 | Regulación de los controles criptográficos | SI | 0.Incompleto | Se deben utilizar los controles criptográficos según las leyes y regulaciones de aplicación |
| | | | | |
| 18.2.1 | Revisión independiente de la seguridad de la información | SI | 0.Incompleto | La seguridad de la información de la empresa debe someterse a una revisión independiente a intervalos regulares o siempre que se realicen cambios significativos |
| 18.2.2 | Cumplimiento de las políticas y normas de seguridad | SI | 0.Incompleto | La dirección de la empresa debe asegurarse que todos los procedimientos relativos a la seguridad se realizan correctamente con el fin de cumplir el cumplimiento legal y normativo. |
| 18.2.3 | Comprobación del cumplimiento técnico | SI | 0.Incompleto | Se debe comprobar periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización. |