Cláusula	ANEXO A ISO 27001
A5	**Políticas de Seguridad de la Información**
A5.1	**Dirección de gestión para la seguridad de la información**
1.-	¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?
2.-	¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?
A6	**Organización de la Seguridad de la Información**
A6.1	
1.-	¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?
2.-	¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?
3.-	¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?
4.-	¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?
5.-	¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?
A6.2	**Dispositivos Móviles y Teletrabajo**
1.-	¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?
2.-	¿Se aplican los criterios de Seguridad para los accesos de teletrabajo?
A7	**Seguridad en los Recursos Humanos**
A7.1	**Antes de contratar a un empleado**
1.-	¿Se investigan los antecedentes de los candidatos? -Formación -Experiencia -Verificar Titulación -Referencias
2.-	¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?
A7.2	**Durante el contrato**

1.-	¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?
2.-	¿Existen procesos de información, formación y sensibilización sobre las responsabilidades sobre la Seguridad de la Información?
3.-	¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?
A7.3	**Terminación del contrato**
1.-	¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?
2.-	¿Se definen responsabilidades sobre la Seguridad de la información que se extiendan más allá de la finalización de un contrato como por ejemplo cuestiones relativas a la confidencialidad de la Información?
A8	**Gestión de Activos**
A8.1	**Responsabilidad sobre los Activos**
1.-	¿Se ha realizado un inventarios de activos que dan soporte al negocio y de Información?
2.-	¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?
3.-	¿Se han establecido normas para el uso de activos en relación a su seguridad?
4.-	¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?
A8.2	**Clasificación de la Información**
1.-	¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad especificas?
2.-	¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación?
3.-	¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?
A8.3	**Manipulación de Soportes**
1.-	¿Existen controles establecidos para aplicar a soportes extraíbles? -Uso -Cifrado -Borrado -Etc.
2.-	¿Existen procedimientos establecidos para la eliminación de soportes?
3.-	¿Existen procedimientos para el traslado de soportes de información para proteger su seguridad? -Control de salidas -Cifrado etc.
A9	**Control de Acceso**
A9.1	**Requisitos generales para el control de acceso**

1.-	¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?
2.-	¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?
A9.2	**Accesos de Usuario**
1.-	¿Existen procesos formales de registros de usuarios?
2.-	¿Existen procesos formales para asignación de perfiles de acceso?
3.-	¿Se define un proceso específico para la asignación y autorización de permisos especiales de administración de accesos?
4.-	¿Se ha establecido una política específica para el manejo de información clasificada cono secreta ? en cuanto a: -Autenticación -Compromisos
5.-	¿Se establecen periodos concretos para renovación de permisos de acceso?
6.-	¿Existen un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos?
A9.3	**Responsabilidades de los usuarios**
1.-	¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso?
A9.4	**Control de acceso a sistemas y aplicaciones**
1.-	¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar?
2.-	¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla etc.?
3.-	¿Se establecen medidas para controlar el establecimiento de contraseñas seguras?
4.-	¿Se controla la capacitación y perfil de las personas que tienen permisos de administración con perfiles bajos de Seguridad?
5.-	¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?
A10	**Criptografía**
A10.1	**Control criptográfico**
1.-	¿Existe una política para el establecimiento u yo de controles criptográficos?
2.-	¿Existe un control del ciclo de vida de las claves criptográficas?

A11	Seguridad Física y del entorno
A11.1	**Áreas de Seguridad**
1.-	¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?
2.-	¿Existen controles de acceso a personas autorizadas en áreas restringidas?
3.-	¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas etc. en áreas de accesibles a personal externo?
4.-	¿Se controla o supervisa la actividad de personal que accede a áreas seguras?
5.-	¿Se controlan las áreas de Carga y descarga con procedimientos de control de mercancías entregadas etc.?
A11.2	**Seguridad de los equipos**
1.-	¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados?
2.-	¿Se protegen los equipos contra fallos de suministro de energía?
3.-	¿Existen protecciones para los cableados de energía y de datos?
4.-	¿Se planifican y realizan tareas de mantenimiento sobre los equipos?
5.-	¿Se controlan y autorizan la salida de equipos, aplicaciones etc. Que puedan contener información?
6.-	¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia empresa?
7.-	¿Se establecen protocolos para proteger o eliminar información de equipos que causan baja o van a ser reutilizados?
8.-	¿Se establecen normas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo?
9.-	¿Se establecen reglas de comportamiento para abandonos momentáneos o temporales del puesto de trabajo?
A12	**Seguridad en las Operaciones**
A12.1	**Procedimientos y responsabilidades**
1.-	¿Se documentan los procedimientos y se establecen responsabilidades?
2.-	¿Se controla que la información sobre procedimientos se mantenga actualizada?

3.-	¿Se dispone de un procedimiento para evaluar el impacto en la seguridad de la información ante cambios en los procedimientos?
4.-	¿Se controla el uso de los recursos en cuanto al rendimiento y capacidad de los sistemas?
5.-	¿Los entornos de desarrollo y pruebas están convenientemente separados de los entornos de producción?
A12.2	**Protección contra software malicioso**
	¿Existen sistemas de detección para Software malicioso o malware?
A12.3	**Copias de Seguridad**
1.-	¿Se ha establecido un sistema de copias de seguridad acordes con las necesidades de la información y de los sistemas?
A12.4	**Registros y supervisión**
1.-	¿Se realiza un registro de eventos? -Intentos de acceso fallidos/exitosos -Desconexiones del sistema -Alertas de fallos Etc.
2.-	¿Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad?
3.-	¿Se protege convenientemente y de forma específica los accesos o los de los administradores?
4.-	¿Existe un control de sincronización de los distintos sistemas?
A12.5	**Control del Software**
1.-	¿Las instalaciones de nuevas aplicaciones SW o modificaciones son verificadas en entornos de prueba y existen protocolos de seguridad para su instalación?
A12.6	**Vulnerabilidad Técnica**
1.-	¿Se establecen métodos de control para vulnerabilidades técnicas "hacking ético" etc.?
2.-	¿Se establecen medidas restrictivas para la instalación de Software en cuanto a personal autorizado evitando las instalaciones por parte de usuarios finales?
A12.6	**Auditorias de Sistemas de Información**
1.-	¿Existen mecanismos de auditorías de medidas de seguridad de los sistemas?
2.-	¿Se establecen protocolos específicos para desarrollo de auditorías Software considerando su impacto en los sistemas?

A13	Seguridad en las Comunicaciones
A13.1	**Seguridad de Redes**
1.-	¿En el entorno de red se gestiona la protección de los sistemas mediante controles de red y de elementos conectados?
2.-	¿Se establecen condiciones de seguridad en los servicios de red tanto propios como subcontratados?
3.-	¿Existe separación o segregación de redes tomando en cuenta condiciones de seguridad y clasificación de activos?
A13.2	**Intercambio de Información**
1.-	¿Se establecen políticas y procedimientos para proteger la información en los intercambios?
2.-	¿Se delimitan y establecen acuerdos de responsabilidad en intercambios de información con otras entidades?
3.-	¿Se establecen normas o criterios de seguridad en mensajería electrónica?
4.-	¿Se establecen acuerdos de confidencialidad antes de realizar intercambios de información con otras entidades
A14	**Adquisición, desarrollo y mantenimiento de sistemas de información**
A14.1	**Intercambio de Información**
1.-	¿Se definen y documentan los requisitos de Seguridad de la Información para los nuevos sistemas de Información?
2.-	¿Se especifican los requisitos de Seguridad de la información en el diseño de nuevos sistemas?
3.-	¿Se consideran requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información?
4.-	¿Se establecen medidas de protección para transacciones Online?
A14.2	**Seguridad en los procesos de Soporte**
1.-	¿Se establecen procedimientos que garanticen el desarrollo seguro del Software?
2.-	¿Se gestiona el control de cambios en relación al impacto que puedan tener en los sistemas?

3.-	¿Se establecen procedimientos de revisión después de efectuar cambios o actualizaciones?
4.-	¿Se establecen procesos formales para cambios en versiones o nuevas funcionalidades para Software de terceros?
5.-	¿Se definen políticas de Seguridad de la Información en procesos de ingeniería de Sistemas?
6.-	¿Se realiza una evaluación de riesgos para herramientas de desarrollo de Software?
7.-	¿Se acuerdan los requisitos de seguridad de la Información para Software desarrollado por terceros?
8.-	¿Se realizan pruebas funcionales de seguridad de los sistemas antes de su fase de producción?
9.-	¿Se establecen protocolos y pruebas de aceptación de sistemas para nuevos sistemas y actualizaciones?
A14.3	**Datos de prueba**
1.-	¿Se utilizan datos de prueba en los ensayos o pruebas de los sistemas?
A15	**Relación con Proveedores**
A15.1	**Seguridad en la Relación con Proveedores**
1.-	¿Existe una política de Seguridad de la información para proveedores que acceden a activos de la información de la empresa?
2.-	¿Se han establecido requisitos de seguridad de la información en contratos con terceros¿
3.-	¿Se fijan requisitos para extender la seguridad de la información a toda la cadena de suministro?
A15.1	**Gestión de servicios externos**
1.-	¿Se controla el cumplimiento de los requisitos establecidos con proveedores externos?
2.-	¿Se controlan los posibles impactos en la seguridad ante cambios de servicios de proveedores externos?
A16	**Gestión de incidentes de seguridad de la información**
A16.1	**Gestión de incidentes de seguridad de la información y mejoras.**

1.-	¿Se definen responsabilidades y procedimientos para responder a los incidentes de la Seguridad de la Información?
2.-	¿Se han implementado canales adecuados para la comunicación de incidentes en la seguridad de la Información?
3.-	¿Se promueve y se hayan establecidos canales para comunicar o identificar puntos débiles en la Seguridad de la Información?
4.-	¿Se ha establecido un proceso para gestionar los incidentes en la Seguridad de la Información?
5.-	¿Existen mecanismos para dar respuesta a los eventos de la Seguridad de la Información?
6.-	¿La información que proporcionada por los eventos en la Seguridad de la información son tratados para tomar medidas preventivas?
7.-	¿Existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de la Información?
A17	**Gestión de la Continuidad del Negocio**
A17.1	**Continuidad de la seguridad de la información.**
1.-	¿Se ha elaborado un plan de continuidad del negocio ante incidentes de Seguridad de la Información?
2.-	¿Se ha implementado las medidas de recuperación previstas en el plan de Continuidad del Negocio?
3.-	¿Se han verificado o probado las acciones previstas en el plan de Continuidad del Negocio?
A17.2	**Redundancias**
1.-	¿Se ha evaluado la necesidad de redundar los activos críticos de la Información?
A18	**Cumplimiento**
A18.1	**Cumplimiento de los requisitos legales y contractuales.**

1.-	¿Se han identificado las legislaciones aplicables sobre protección de datos personales y su cumplimiento? -LOPD -Leyes para comercio Electrónico -Transacciones Bancarias -Información Protegida -Otras propias del negocio o actividad -Ley general de Telecomunicaciones
2.-	¿Existen procedimientos implementados sobre la propiedad intelectual?
3.-	¿Se establecen criterios para clasificación de registros y medidas de protección según niveles?
4.-	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?
5.-	¿Si se utiliza el cifrado, se establecen controles criptográficos de acuerdo a la legislación?
A18.2	**Revisiones de la Seguridad de la Información**
1.-	¿Se revisan los controles de la Seguridad de la Información por personal independiente a los responsables de implementar los controles?
2.-	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la Seguridad de la información?
3.-	¿Se realizan evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protección para la seguridad de la información?