# Apéndice 3 – Lista de verificación de auditoría interna para ISO 27001 e ISO 22301

## 1. Lista de verificación de auditoría interna para ISO 27001

| Capítulo | Requerimiento de la norma | Cumplimiento (s/No) | Evidencia |
|---|---|---|---|
| 4.2 | ¿La organización determinó las partes interesadas? | | |
| 4.2 | ¿Existe la lista de todos los requerimientos para las partes interesadas? | | |
| 4.3 | ¿Está documentado el alcance con límites e interfaces claramente definidos? | | |
| 5.2 | ¿Los objetivos generales del SGSI son compatibles con la dirección estratégica? | | |
| 5.1 | ¿La dirección asegura que el SGSI cumple sus objetivos? | | |
| 5.2 | ¿Existe la Política de seguridad de la información con objetivos o marco para establecer los objetivos? | | |
| 5.2 | ¿Se comunica la Política de seguridad de la información dentro de la organización? | | |
| 5.3 | ¿Los roles y responsabilidades para seguridad de la información están asignados y comunicados? | | |
| 6.1.2 | ¿Está documentado el proceso de evaluación de riesgos, incluidos los criterios de aceptabilidad de riesgos y de evaluación de riesgos? | | |
| 6.1.2, 8.2 | ¿Están definidos los riesgos, sus propietarios, probabilidad, consecuencias y nivel de riesgo? ¿Estos resultados están documentados? | | |
| 6.1.3 | ¿Está documentado el proceso de tratamiento del riesgo, incluidas las opciones para tratamiento de los riesgos? | | |
| 6.1.3, 8.3 | ¿Todos los riesgos no aceptables son tratados utilizando las opciones y controles del Anexo A? ¿Estos resultados están documentados? | | |
| 6.1.3 | ¿La Declaración de aplicabilidad está confeccionada con justificaciones y estados para cada control? | | |
| 6.1.3, 8.3 | ¿Existe el Plan de tratamiento de riesgos aprobado por los propietarios de los riesgos? | | |

Commented [AES1]: Si necesita ayuda para realizar la auditoría

Commented [AES2]: Para conocer más sobre este tema:

Commented [AES3]: Estos son los requerimientos de la norma

Commented [AES5]: Para completar durante la auditoria:

Commented [AES4]: Para completar durante la auditoria:

| | | | |
|---|---|---|---|
| 6.2 | ¿El Plan de tratamiento de riesgos define quién es responsable de la implementación de qué control, con qué recursos, con qué plazos y cuál es el método de evaluación? | | |
| 7.1 | ¿Se proporcionan los recursos adecuados para todos los elementos del SGSI? | | |
| 7.2 | ¿Están definidas las competencias requeridas, las capacitaciones realizadas y se llevan registros de competencias? | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |

| | | | |
|---|---|---|---|
| 9.3 | ¿La dirección tuvo decisión sobre todos los temas críticos importantes para el éxito del SGSI? | | |
| 10.1 | ¿La organización reacciona ante cada no-conformidad? | | |
| 10.1 | ¿La organización considera eliminar las causas de la no-conformidad y, cuando corresponde, toma acciones correctivas? | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |

| | | | |
|---|---|---|---|
| A.5.9 | ¿Todos los bienes del Inventario de activos tienen un propietario designado? | | |
| A.5.10 | ¿Están documentadas las reglas para el manejo adecuado de la información y los activos? | | |
| A.5.10 | ¿Existen procedimientos que definan cómo manejar la información clasificada? | | |
| A.5.11 | ¿Todos los empleados y contratistas devuelven todos los activos de la organización cuando terminan con su empleo? | | |
| A.5.12 | ¿Se clasifica la información de acuerdo con criterios específicos? | | |
| A.5.13 | ¿La información clasificada está etiquetada de acuerdo con los procedimientos definidos? | | |
| A.5.14 | ¿La protección de la transferencia de información está regulada en políticas y procedimientos formales? | | |
| A.5.14 | ¿Existen acuerdos con terceros que regulen la seguridad de la transferencia de información? | | |
| A.5.14 | ¿Están debidamente protegidos los mensajes que se intercambian a través de las redes? | | |
| A.5.15 | ¿Existe una Política de control de acceso que defina los requisitos comerciales y de seguridad para el control de acceso? | | |
| A.5.15 | ¿Los usuarios tienen acceso únicamente a aquellas redes y servicios para los que están específicamente autorizados? | | |
| A.5.16 | ¿Se otorgan los derechos de acceso a través de un proceso de registro formal? | | |
| A.5.17 | ¿Se proporcionan las claves iniciales y otra información de autenticación secreta de forma segura? | | |
| A.5.17 | ¿Existen reglas claras para los usuarios sobre cómo protegen las claves y otra información de autenticación? | | |
| A.5.17 | ¿Los sistemas que gestionan las claves son interactivos y permiten la creación de claves seguras? | | |
| A.5.18 | ¿Existe un sistema formal de control de acceso al iniciar sesión en los sistemas de información? | | |

| | | | |
|---|---|---|---|
| A.5.18 | ¿Los propietarios de activos verifican periódicamente todos los derechos de acceso privilegiado? | | |
| A.5.18 | ¿Se han eliminado los derechos de acceso de todos los empleados y contratistas al término de sus contratos? | | |
| A.5.19 | ¿Está documentada la política sobre cómo tratar los riesgos relacionados con proveedores y socios? | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |

| | | | |
|---|---|---|---|
| A.5.29 | ¿Se realizan ejercicios y pruebas para garantizar una respuesta eficaz? | | |
| A.5.30 | ¿Se planifica, implementa, mantiene y prueba la preparación de las TIC en función de los requisitos de continuidad del negocio y de las TIC? | | |
| A.5.31 | ¿Están enumerados y documentados todos los requisitos de seguridad legislativos, reglamentarios, contractuales y de otro tipo? | | |
| A.5.32 | [redacted] | | |
| A.5.33 | [redacted] | | |
| A.5.34 | [redacted] | | |
| A.5.35 | [redacted] | | |
| A.5.36 | [redacted] | | |
| A.5.36 | [redacted] | | |
| A.5.37 | [redacted] | | |
| A.6.1 | [redacted] | | |
| A.6.2 | [redacted] | | |
| A.6.3 | [redacted] | | |

| | | | |
|---|---|---|---|
| A.6.4 | ¿Todos los empleados que han cometido una brecha de seguridad han sido objeto de un proceso disciplinario formal? | | |
| A.6.5 | ¿Están definidas en el acuerdo las responsabilidades de seguridad de la información que siguen siendo válidas después de la terminación del empleo? | | |
| A.6.6 | ¿La organización enumeró todas las cláusulas de confidencialidad que deben incluirse en los acuerdos con terceros? | | |
| A.6.7 | [illegible] | | |
| A.6.8 | [illegible] | | |
| A.7.1 | [illegible] | | |
| A.7.2 | [illegible] | | |
| A.7.3 | [illegible] | | |
| A.7.4 | [illegible] | | |
| A.7.5 | [illegible] | | |
| A.7.6 | [illegible] | | |
| A.7.7 | [illegible] | | |
| A.7.8 | [illegible] | | |
| A.7.9 | [illegible] | | |

| | | | |
|---|---|---|---|
| A.7.9 | ¿Los activos de la organización están adecuadamente protegidos cuando no se encuentran en las instalaciones de la organización? | | |
| A.7.10 | ¿Los procedimientos que definen cómo manejar los medios extraíbles están en línea con las reglas de clasificación? | | |
| A.7.10 | ¿Existen procedimientos formales para desechar los medios? | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |

| | | | |
|---|---|---|---|
| A.8.8 | ¿Se revisan periódicamente los sistemas de información para verificar su cumplimiento con las políticas y estándares de seguridad de la información? | | |
| A.8.9 | ¿Se establecen, documentan, implementan, supervisan y revisan las configuraciones de hardware, software, servicios y redes? | | |
| A.8.10 | ¿Se elimina la información almacenada en sistemas, dispositivos y medios cuando ya no se necesita? | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |

| | | | |
|---|---|---|---|
| A.8.19 | ¿Se controla estrictamente la instalación de software? ¿Existen procedimientos para tal fin? | | |
| A.8.20 | ¿Las redes están controladas de tal manera que protegen la información en los sistemas y aplicaciones? | | |
| A.8.21 | ¿Los requisitos de seguridad para los servicios de red internos y externos están definidos e incluidos en los acuerdos? | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |

| | | | |
|---|---|---|---|
| A.8.34 | ¿Se planifican y ejecutan las auditorías de los sistemas de producción de tal manera que minimicen el riesgo de interrupción? | | |

## 2. Lista de verificación de auditoría interna para ISO 22301

| Capítulo | Requerimiento de la norma | Completamente (s/No) | Evidencia |
|---|---|---|---|
| 4.2.1 | ¿La organización determinó las partes interesadas? | | |
| 4.2.2 | ¿Existe la lista de todos los requerimientos para las partes interesadas? | | |
| 4.2.2 | ¿La organización determinó un proceso para gestionar los requisitos legales y aplicables? | | |
| 4.3 | ¿Está documentado el alcance, que define qué productos y servicios están incluidos, y se explican las exclusiones? | | |
| 5.1 | ¿La alta dirección apoya activamente las actividades de continuidad de negocio? | | |
| 5.2 | ¿El SGCN es compatible con el propósito de la organización? | | |
| 5.2 | ¿La alta dirección muestra compromiso suministrando todos los recursos y comunica la importancia de la continuidad de negocio? | | |
| 5.2 | ¿Existe una Política de continuidad del negocio y define el marco para establecer objetivos? | | |
| 5.2 | ¿La Política de continuidad del negocio se comunica dentro de la organización? | | |
| 5.3 | ¿Se nombra a la persona responsable del SGCN y esta persona tiene suficiente autoridad? | | |
| 5.3 | ¿Los roles y responsabilidades para continuidad de negocio están asignados y comunicados? | | |
| 6.1 | ¿La organización determinó todos los riesgos y oportunidades? | | |
| 6.2 | ¿La organización planificó las acciones para atender los riesgos y oportunidades identificados? | | |
| 6.2.1 | ¿Se determinaron objetivos para continuidad de negocio, y fueron comunicados a los empleados correspondientes? | | |
| 6.2.1 | ¿Son cuantificables los objetivos de continuidad de negocio, se controlan y actualizan? | | |
| 6.2.2 | ¿Está definido lo siguiente: pasos necesarios para lograr objetivos, quién es responsable, cuáles son los plazos y qué recursos son necesarios? | | |
| 6.3 | ¿Se realizan los cambios necesarios para el SGCN de manera planificada? | | |

**Commented [AES6]:** Estos son los requerimientos de la norma

**Commented [AES8]:** Para completar durante la auditoria:

**Commented [AES7]:** Para completar durante la auditoria:

| | | | |
|---|---|---|---|
| 7.1 | ¿Se proporcionan los recursos adecuados para todos los elementos del SGCN? | | |
| 7.2 | ¿Están definidas las competencias requeridas, las capacitaciones realizadas y se llevan registros de competencias? | | |
| 7.3 | ¿El personal es consciente de la Política de continuidad de negocio, de su rol y de las consecuencias por el no cumplimiento de las normas? | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |

| | | | |
|---|---|---|---|
| 8.4.1 | ¿Los procedimientos o planes de continuidad de negocio tienen estos elementos: definir protocolos de comunicación, tener pasos específicos, ser flexibles para todo tipo de condiciones de interrupción de amenazas, se centran en minimizar las consecuencias, asignar roles y responsabilidades? | | |
| 8.4.2 | ¿Existen los procedimientos de respuesta ante incidentes con umbrales de inicio y procedimientos de respuesta? | | |
| 8.4.3 | ¿Existe el procedimiento para comunicar a las personas interesadas? ¿Este procedimiento define cuáles son los medios de comunicación que estarán disponibles? | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |

| | | | |
|---|---|---|---|
| 9.2 | ¿Las auditorías internas se realizan de acuerdo al programa de auditoría, los resultados son informados a través del informe de auditoría interna y se elevan las acciones correctivas correspondientes? | | |
| 9.3 | ¿Se realiza periódicamente la revisión por parte de la dirección y sus resultados son documentados en actas de la reunión? | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |
| [illegible] | [illegible] | | |