

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

1. Lista de verificación de auditoría interna para ISO 27001

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

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

[https://www.iso.org/standard/72431.html](#)
[https://www.iso.org/standard/72432.html](#)
[https://www.iso.org/standard/72433.html](#)
[https://www.iso.org/standard/72434.html](#)
[https://www.iso.org/standard/72435.html](#)
[https://www.iso.org/standard/72436.html](#)
[https://www.iso.org/standard/72437.html](#)
[https://www.iso.org/standard/72438.html](#)
[https://www.iso.org/standard/72439.html](#)
[https://www.iso.org/standard/72440.html](#)
[https://www.iso.org/standard/72441.html](#)
[https://www.iso.org/standard/72442.html](#)
[https://www.iso.org/standard/72443.html](#)
[https://www.iso.org/standard/72444.html](#)
[https://www.iso.org/standard/72445.html](#)
[https://www.iso.org/standard/72446.html](#)
[https://www.iso.org/standard/72447.html](#)
[https://www.iso.org/standard/72448.html](#)
[https://www.iso.org/standard/72449.html](#)
[https://www.iso.org/standard/72450.html](#)
[https://www.iso.org/standard/72451.html](#)
[https://www.iso.org/standard/72452.html](#)
[https://www.iso.org/standard/72453.html](#)
[https://www.iso.org/standard/72454.html](#)
[https://www.iso.org/standard/72455.html](#)
[https://www.iso.org/standard/72456.html](#)
[https://www.iso.org/standard/72457.html](#)
[https://www.iso.org/standard/72458.html](#)
[https://www.iso.org/standard/72459.html](#)
[https://www.iso.org/standard/72460.html](#)
[https://www.iso.org/standard/72461.html](#)
[https://www.iso.org/standard/72462.html](#)
[https://www.iso.org/standard/72463.html](#)
[https://www.iso.org/standard/72464.html](#)
[https://www.iso.org/standard/72465.html](#)
[https://www.iso.org/standard/72466.html](#)
[https://www.iso.org/standard/72467.html](#)
[https://www.iso.org/standard/72468.html](#)
[https://www.iso.org/standard/72469.html](#)
[https://www.iso.org/standard/72470.html](#)
[https://www.iso.org/standard/72471.html](#)
[https://www.iso.org/standard/72472.html](#)
[https://www.iso.org/standard/72473.html](#)
[https://www.iso.org/standard/72474.html](#)
[https://www.iso.org/standard/72475.html](#)
[https://www.iso.org/standard/72476.html](#)
[https://www.iso.org/standard/72477.html](#)
[https://www.iso.org/standard/72478.html](#)
[https://www.iso.org/standard/72479.html](#)
[https://www.iso.org/standard/72480.html](#)
[https://www.iso.org/standard/72481.html](#)
[https://www.iso.org/standard/72482.html](#)
[https://www.iso.org/standard/72483.html](#)
[https://www.iso.org/standard/72484.html](#)
[https://www.iso.org/standard/72485.html](#)
[https://www.iso.org/standard/72486.html](#)
[https://www.iso.org/standard/72487.html](#)
[https://www.iso.org/standard/72488.html](#)
[https://www.iso.org/standard/72489.html](#)
[https://www.iso.org/standard/72490.html](#)
[https://www.iso.org/standard/72491.html](#)
[https://www.iso.org/standard/72492.html](#)
[https://www.iso.org/standard/72493.html](#)
[https://www.iso.org/standard/72494.html](#)
[https://www.iso.org/standard/72495.html](#)
[https://www.iso.org/standard/72496.html](#)
[https://www.iso.org/standard/72497.html](#)
[https://www.iso.org/standard/72498.html](#)
[https://www.iso.org/standard/72499.html](#)

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

Commented [AES5]: Para completar durante la auditoría:

Commented [AES4]: Para completar durante la auditoría:

Requisito	Requisitos de la norma	Comentarios	Observaciones
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?		
5.1	¿Los objetivos generales de la organización son compatibles con la declaración estratégica?		
5.1	¿La declaración estratégica es el resultado de un proceso definido?		
5.2	¿Cómo se publica la información de la información con límites e interfaces claramente definidos?		
5.2	¿Se controla la publicación de la información dentro de la organización?		
5.2	¿Se define y responsabilidades para seguridad de la información están asignadas e implementadas?		
5.2.2	¿Cómo documentado el proceso de evaluación de riesgos, incluye los criterios de aceptabilidad de riesgo y de evaluación de riesgo?		
5.2.2.1	¿Cómo documentado los riesgos, los impactos, oportunidades, consecuencias o nivel de riesgo? ¿Cómo evaluados estos documentados?		
5.2.2	¿Cómo documentado el proceso de evaluación de riesgo, incluye los criterios para tratamiento de los riesgos?		
5.2.2.1	¿Cómo los riesgos se controlados con medidas definiendo los controles y controles del riesgo? ¿Cómo evaluados estos documentados?		
5.2.2	¿Los tratamientos de oportunidades son definidos con planificación y control para cada control?		
5.2.2.1	¿Cómo el Plan de tratamiento de riesgos controlados por la estructura de los riesgos?		

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?		
8.1	¿El personal es consciente de la Política de seguridad de la información, de su rol y de las consecuencias por el no cumplimiento de la misma?		
8.2	¿Existen el proceso para la actualización periódicamente con seguridad de la información, incluya las responsabilidades y qué hay que considerar?		
8.3	¿Existen el proceso para gestión de documentos y registros, incluya gestión control y revisión documentos, almacenamiento de archivos, archivo y proteger?		
8.4	¿Se controlan los documentos de origen externo?		
8.5	¿Se identifica y controla los procesos automatizados?		
8.6	¿Se define con qué se realiza, con qué método, quién es responsable, quién realiza y cuándo se realiza?		
8.7	¿Se documentan los resultados de la auditoría y son reportados a las personas responsables?		
8.8	¿Existen el programa de auditoría que define los tiempos, responsabilidades, informes, acciones y plazos de la auditoría?		
8.9	¿Las auditorías internas se realizan de acuerdo al programa de auditoría, los resultados se informan a nivel del informe de auditoría interna y se abren las acciones correctivas correspondientes?		
8.10	¿Se realiza periódicamente la revisión por parte de la Dirección y sus resultados son documentados en actas de la reunión?		

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?		
9.3.1	¿Se registran todos los no-conformidades, según con las acciones correctivas?		
9.3.2	¿Tiene las políticas de seguridad de la información relacionadas con seguridad por la dirección o bajo autoridad?		
9.3.3	¿Tiene las políticas de seguridad de la información con recursos y actividades?		
9.3.4	¿Tiene los recursos definidos sobre las responsabilidades, competencias y la seguridad de la información a través de una o varias direcciones?		
9.3.5	¿Tiene definidas las políticas y responsabilidades de formación que se refieren al conflicto de intereses, particularmente con la información y los sistemas que involucran alta seguridad?		
9.3.6	¿Se describe cada activamente que todas las actividades y actividades cumplen con la política de seguridad de la información?		
9.3.7	¿Tiene los recursos definidos sobre cómo interactuar en contacto con sus actividades?		
9.3.8	¿Tiene los recursos definidos sobre cómo interactuar en contacto con sus grupos de interés, asociados o asociaciones profesionales?		
9.3.9	¿Se respaldar y auditar las actividades de la seguridad de la información para general inteligencia sobre amenazas?		
9.3.10	¿Tiene incluido las normas de seguridad de la información en cada proyecto?		
9.3.11	¿Tiene definidas las respuestas de seguridad para los recursos internos de información y para cualquier conflicto en los recursos?		
9.3.12	¿Se incluye un mecanismo de acción?		

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.5.10	¿Existen los registros y controles de clasificación sobre los activos de la organización cuando se crean o se modifican?		
A.5.10	¿Se aplica la información de acuerdo con ciertos requisitos?		
A.5.10	¿La información clasificada está protegida de acuerdo con los procedimientos definidos?		
A.5.10	¿Los productos de la transformación de información están protegidos en función de procedimientos formales?		
A.5.10	¿Existen acuerdos con terceros que regulen la seguridad de la transformación de información?		
A.5.10	¿Existen procedimientos que protejan los derechos de los proveedores y clientes de los datos?		
A.5.10	¿Existen los controles de acceso de acuerdo con el nivel de requisitos comerciales y de seguridad para el control de acceso?		
A.5.10	¿Los usuarios tienen acceso únicamente a aquellos datos y servicios para los que están autorizados a acceder?		
A.5.10	¿Se otorgan los derechos de acceso cuando se da un proceso de registro formal?		
A.5.10	¿Se supervisan los datos sensibles y otra información de administración cuando se transfieren?		
A.5.10	¿Existen reglas de acceso para los usuarios sobre cómo proteger los datos y otra información de administración?		
A.5.10	¿Los sistemas que gestionan los datos son identificados y permiten la creación de datos legales?		
A.5.10	¿Existen los sistemas formales de control de acceso al nivel adecuado 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?		
A.5.20	¿Se revisan los requisitos de seguridad relacionados incluidos en los acuerdos con los proveedores y socios?		
A.5.20	¿Se revisan con los proveedores de la nube y otros proveedores cualquier requisito de seguridad para garantizar la entrega segura de servicios?		
A.5.20	¿Se proveen los procedimientos regularmente para verificar el cumplimiento de los requisitos de seguridad con los proveedores y socios?		
A.5.20	¿Se revisan los riesgos en los acuerdos y contratos con proveedores y socios, así como en cuanto los riesgos y los procesos asociados?		
A.5.20	¿Se revisan los procesos de adquisición, del servicio o salida de los servicios en la nube con los requisitos de seguridad identificados?		
A.5.20	¿Se documentan detallada los procedimientos y responsabilidades para la gestión de incidentes?		
A.5.20	¿Se revisan y validan todos los niveles de seguridad?		
A.5.20	¿Se documentan los procedimientos sobre cómo responder a los incidentes?		
A.5.21	¿Se revisan los incidentes de seguridad para obtener datos asociados?		
A.5.20	¿Existen procedimientos que definen cómo recopilar evidencia de incidentes que sean accionables durante el proceso legal?		
A.5.20	¿Se definen los requisitos para la continuidad de la seguridad de la información?		
A.5.20	¿Existen procedimientos que garantizan la continuidad de la seguridad de la información durante una crisis o un desastre?		

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	¿Existen procedimientos con garantías de cumplimiento de los derechos de propiedad intelectual, incluido el uso de software con licencia?		
A.5.33	¿Existen todos los registros apropiados de acuerdo con los requisitos reglamentarios, contractuales y de otro tipo identificados?		
A.5.34	¿Las informaciones de identificación personal están protegidas según lo exigen la ley y los reglamentos?		
A.5.35	¿Las reglas de la información se cumplen rigurosamente por un auditor independiente?		
A.5.36	¿Se garantiza, entre otros procedimientos, la independencia y procedimientos de seguridad en todos los procedimientos en las áreas de responsabilidad?		
A.5.37	¿Se realiza periódicamente la revisión de información para verificar su cumplimiento con las políticas y estándares de seguridad de la información?		
A.5.38	¿Se han documentado los procedimientos apropiados para los procesos de IT?		
A.5.39	¿Se realizan verificaciones de conformidad de los estándares para el cumplimiento de los contratos?		
A.5.40	¿Los acuerdos con empleados o contratistas especifican las responsabilidades de seguridad de la información?		
A.5.41	¿Todos los empleados o contratistas identificados están siendo formados para desarrollar sus funciones de seguridad y recibir programas de capacitación?		

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	¿Existen reglas que obligan a los empleados a proteger la información de la organización cuando se trabaja de forma remota?		
A.6.8	¿Las actividades y actividades relacionadas con la actividad y los recursos de seguridad?		
A.6.9	¿Existen reglas que obligan a los empleados a proteger la información sensible?		
A.6.10	¿Las actividades y las áreas logísticas están protegidas con controles que permiten el acceso solo a las personas autorizadas?		
A.6.11	¿Las áreas de trabajo o logísticas controladas de tal manera que las personas no autorizadas no pueden ingresar a las instalaciones de la organización?		
A.6.12	¿Existen reglas logísticas diseñadas de tal manera que no sean viables para los visitantes y no sean fácilmente accesibles desde el exterior?		
A.6.13	¿Se controlan las instalaciones para detectar intrusiones no autorizadas?		
A.6.14	¿Existen medidas de detección, prevención contra incendios y otros riesgos?		
A.6.15	¿Existen definidas con claridad las procedimientos de trabajo para las áreas logísticas?		
A.6.16	¿Existen reglas que obligan a los visitantes a utilizar pasillos y puertas cuando se están presentes y mantenerlos cerrados?		
A.6.17	¿Existen reglas diseñadas de tal manera que estén protegidos del acceso no autorizado a los recursos autorizados?		

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?		
A.7.10	¿Existen procedimientos formales de clasificación de datos?		
A.7.10	¿Los datos de correo electrónico almacenados están adecuadamente protegidos?		
A.7.10	¿Existen reglas de clasificación de datos de acuerdo con las especificaciones o normas aplicables de los fabricantes?		
A.7.10	¿Se eliminan todos los datos confidenciales y el software con licencia de los medios o equipos cuando se desechan?		
A.7.10	¿Existen reglas para el manejo seguro de dispositivos móviles?		
A.7.10	¿Existen los recursos protegidos o medios cuando se están en posesión física del usuario?		
A.7.10	¿Los dispositivos de acceso protegidos se manejan con especial cuidado?		
A.7.10	¿El acceso a los dispositivos, software y sistemas está restringido de acuerdo con la política de control de acceso?		
A.7.10	¿El acceso al código fuente está restringido o apropiado controlado?		
A.7.10	¿El software se copia de todos los tipos de los sistemas de acuerdo con la política de control de acceso?		
A.7.10	¿Algunos miembros del personal de los usuarios o proveedores de servicios operan?		
A.7.10	¿Existen medidas de seguridad de software aplicables y otros software para la protección contra malware?		
A.7.10	¿Existen reglas o reglas de manejo de información sobre la confidencialidad y sus responsabilidades en cualquier momento?		

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?		
A.8.11	¿Se definen roles y responsabilidades de acuerdo con las políticas aplicables a los recursos tecnológicos y legales?		
A.8.12	¿Se aplican controles de acceso de acceso de Terceros de datos a los activos que procesan, almacenan o transmiten información confidencial?		
A.8.13	¿Se documentan la política de copia de seguridad, ¿se realiza la copia de seguridad de acuerdo con esta política?		
A.8.14	¿Se implementan los estándares de TI con referencias para cumplir con las regulaciones de datos de terceros?		
A.8.15	¿Se registran todos los accesos de los usuarios, roles y otros miembros de los sistemas de TI durante los cambios?		
A.8.16	¿Se registran cambios de registros de información sobre accesos privilegiados de los usuarios con los sistemas de administración de usuarios confidenciales?		
A.8.17	¿Se implementan los roles, los sistemas y los procedimientos, y se usan los medios apropiados para reducir posibles incidentes de seguridad de la información?		
A.8.18	¿Se protege de todos los sistemas de TI datos almacenados con una única fuente de datos confidenciales?		
A.8.19	¿El uso de los servicios de servicios públicos que pueden afectar los controles de seguridad de los dispositivos y los sistemas está adecuadamente controlado y limitado a un nivel de riesgo de aceptable?		

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?		
A.8.22	¿Se aplican los controles de acceso a datos en sistemas para asegurar la integridad de los datos?		
A.8.23	¿Se aplican los controles de acceso a datos en sistemas para asegurar la confidencialidad de los datos?		
A.8.24	¿Se aplican los controles de acceso a datos en sistemas para asegurar la disponibilidad de los datos?		
A.8.25	¿Se aplican los controles de acceso a datos en sistemas para asegurar la integridad de los datos?		
A.8.26	¿Se aplican los controles de acceso a datos en sistemas para asegurar la confidencialidad de los datos?		
A.8.27	¿Se aplican los controles de acceso a datos en sistemas para asegurar la disponibilidad de los datos?		
A.8.28	¿Se aplican los controles de acceso a datos en sistemas para asegurar la integridad de los datos?		
A.8.29	¿Se aplican los controles de acceso a datos en sistemas para asegurar la confidencialidad de los datos?		
A.8.30	¿Se aplican los controles de acceso a datos en sistemas para asegurar la disponibilidad de los datos?		
A.8.31	¿Se aplican los controles de acceso a datos en sistemas para asegurar la integridad de los datos?		
A.8.32	¿Se aplican los controles de acceso a datos en sistemas para asegurar la confidencialidad de los datos?		
A.8.33	¿Se aplican los controles de acceso a datos en sistemas para asegurar la disponibilidad de los datos?		
A.8.34	¿Se aplican los controles de acceso a datos en sistemas para asegurar la integridad de los datos?		
A.8.35	¿Se aplican los controles de acceso a datos en sistemas para asegurar la confidencialidad de los datos?		
A.8.36	¿Se aplican los controles de acceso a datos en sistemas para asegurar la disponibilidad de los datos?		
A.8.37	¿Se aplican los controles de acceso a datos en sistemas para asegurar la integridad de los datos?		
A.8.38	¿Se aplican los controles de acceso a datos en sistemas para asegurar la confidencialidad de los datos?		
A.8.39	¿Se aplican los controles de acceso a datos en sistemas para asegurar la disponibilidad de los datos?		
A.8.40	¿Se aplican los controles de acceso a datos en sistemas para asegurar la integridad de los datos?		

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

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?		
8.1	¿Existen los procedimientos que definen qué acciones se deben tomar en caso de una interrupción de negocio, cuáles son los roles y responsabilidades?		
8.2	¿Existen el proceso para gestión de documentos y registros, incluidos aquellos relativos a grandes documentos, datos y otros de carácter crítico y sensible?		
8.3	¿Se controlan los documentos de origen externo?		
8.4	¿Se identifican y controlan los procesos automatizados?		
8.5.1	¿Existen definidos los procesos para evaluación de riesgo y análisis de impacto en el negocio?		
8.5.2	¿Se realiza el análisis de impacto en el negocio, incluido todas las actividades, y se evalúan los impactos de su realización sobre actividades críticas o de alto impacto?		
8.5.3	¿Se realiza un análisis de riesgo sobre todas las actividades para cada actividad? ¿Se identifican las dependencias entre actividades y sobre actividades?		
8.5.4	¿Se realiza la evaluación de riesgo para todas las actividades, procesos y activos, y se identifican las interrupciones que ocasionan riesgos?		
8.5.5	¿Se identifican las estrategias y acciones de continuidad del negocio?		
8.5.6	¿Se seleccionan estrategias y acciones viables en los objetivos de tiempo de recuperación establecidos para cada actividad?		
8.5.7	¿Se identifican los recursos necesarios para la recuperación personal, información, equipos y servicios, suministros, sistemas de TI y comunicaciones, transporte, alojamiento, servicios y proveedores?		

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?		
8.4.4	¿Existen planes de continuidad de negocio que indiquen roles y responsabilidades sobre definidos para la recuperación de actividades?		
8.4.5	¿Existen procedimientos de procedimientos que definen la recuperación de actividades?		
8.4.6	¿Se realizan pruebas y verificaciones periódicas de bases de datos? ¿Se genera informes luego de las pruebas?		
8.4.7	¿Se realizan pruebas periódicas de la documentación y los medios de cumplimiento de todos los requisitos?		
8.4.8	¿Se realizan pruebas, pruebas y verificaciones periódicas de incidentes después de activarse los procedimientos de continuidad de negocio?		
8.4.9	¿Se realizan las actividades de continuidad operacional de procedimientos y roles?		
8.4.10	¿Existen definidos que roles se realicen, con qué recursos, quién es responsable, quién realizará, cuándo se realizará?		
8.4.11	¿Existen documentados los resultados de la revisión y monitoreo, y con responsable y las acciones requeridas?		
8.4.12	¿Existen un programa de auditoría que defina los tiempos, responsabilidades, acciones, roles y roles de la auditoría?		

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?		
9.4	¿Los procedimientos de auditoría interna son actualizados periódicamente para el ciclo de vida de la organización?		
9.5	¿La organización establece objetivos de auditoría interna y los resultados, cuando correspondan, son acciones correctivas?		
9.6	¿La organización realiza la auditoría interna, para los sistemas críticos?		