Área Tecnologías de Información y Ciberseguridad

nacap

SGSI Sistema de Gestión de Seguridad de la Información /ISO 27001

nacap

SGSI, Sistema de Gestión de la Seguridad de la Información

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de políticas, procedimientos, directrices, prácticas y recursos organizacionales que tienen como objetivo proteger la confidencialidad, integridad y disponibilidad de la información dentro de una organización.

Un SGSI se centra en gestionar de manera efectiva los riesgos asociados con la seguridad de la información, garantizando que los activos de información sean protegidos de amenazas y vulnerabilidades de forma constante.



nacap

Características

Características	
Enfoque basado en riesgos	El SGSI se orienta a identificar, evaluar y gestionar los riesgos que podrían afectar a la seguridad de la información en la organización.
Ciclo mejora continua	Un SGSI sigue el ciclo de Planificar-Hacer-Verificar-Actuar (PDCA), lo que permite que la organización mejore constantemente sus procesos de seguridad.
Cumplimiento normativo	El SGSI ayuda a garantizar el cumplimiento de normativas y estándares internacionales de seguridad, como la norma ISO/IEC 27001, que proporciona un marco para implementar, mantener y mejorar el sistema de gestión de seguridad de la información.
Protección Activos de Información	Establece controles para proteger los activos críticos de la organización, como datos, sistemas, procesos y personas.
Alineación objetivos organizacionales	El SGSI debe estar alineado con los objetivos estratégicos de la organización y debe adaptarse a sus necesidades y contexto.

Componentes Claves

Características	
Políticas de seguridad de la información	Conjunto de reglas y directrices establecidas para asegurar que la información se maneje de forma segura. Estas políticas cubren áreas como el control de accesos, el uso de dispositivos, y la protección de datos.
Evaluación de riesgos	dentificación de amenazas y vulnerabilidades que podrían afectar la seguridad de la información, seguido de una evaluación del impacto y la probabilidad de que ocurra un incidente de seguridad.
Controles de seguridad	Procedimientos, herramientas y tecnologías implementadas para mitigar los riesgos identificados. Estos controles incluyen medidas técnicas (firewalls, cifrado) y organizativas (entrenamiento, monitoreo).
Gestión de incidentes	Procedimientos establecidos para identificar, responder y recuperar ante incidentes de seguridad de la información, como ataques cibernéticos o brechas de datos.
Auditoría y monitoreo	Supervisión constante de las actividades relacionadas con la seguridad de la información, incluyendo registros de auditoría, monitoreo de redes y sistemas, y evaluación de cumplimiento.
Revisión y mejora continua	El SGSI debe ser revisado regularmente para garantizar su efectividad y adaptabilidad frente a cambios en las amenazas, la tecnología y el contexto organizacional. Esto incluye auditorías internas y externas y revisiones de gestión.

Beneficios SGSI

Beneficios	
Protección contra amenazas	Ayuda a proteger la información confidencial de accesos no autorizados, pérdida o corrupción.
Cumplimiento legal	Facilita el cumplimiento de regulaciones y normativas sobre privacidad y seguridad de la información, como GDPR, HIPAA, etc.
Confianza y reputación	Un SGSI bien implementado aumenta la confianza de clientes, socios y partes interesadas al demostrar que la organización toma en serio la seguridad de la información.
Reducción de riesgos	Mejora la identificación y mitigación de riesgos, minimizando el impacto de incidentes de seguridad.
Mejora continua	El enfoque de mejora continua asegura que el SGSI evolucione y se mantenga efectivo frente a nuevos riesgos y desafíos.

nacap

Relación con ISO 27001

La ISO/IEC 27001 es el estándar internacional más reconocido para la implementación de un SGSI.

Proporciona los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información.

Las organizaciones que cumplen con este estándar pueden obtener una certificación que demuestra su compromiso con la seguridad de la información.

nacap

Confidencialidad, Disponibilidad, Integridad



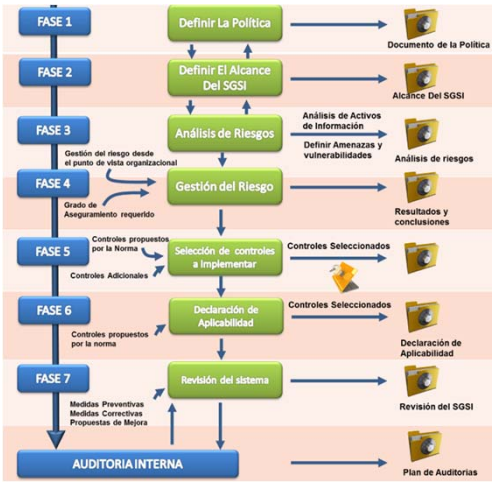
nacap

Activos



nacap

Fases de implementación SGSI



ISO 27001

Esta norma define los requerimientos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, dentro del contexto de la organización.

ISO 27001

Esta norma incluye además los requisitos para la evaluación y tratamiento de los riesgos de la seguridad de la información que se adapta a las necesidades de la organización.

ISO 27001

Los requisitos definidos en esta norma son genéricos y tienen por objetivo ser aplicables a todas las organizaciones, sin importar el tipo, tamaño o naturaleza.

Normas

Comparación

ISO/IEC 27032	ISO/IEC 27001
1. No es certificable. 2. Define conceptos. 3. Incluye elementos de análisis de riesgos: i. Amenazas. ii. Vulnerabilidades. iii. Tipificación.	1. Certificable. 2. Define un sistema de gestión 3. Exige análisis de riesgos: i. Metodología. ii. Objetividad. iii. Independencia.

nacap

ISO/EIC 27103



1. Publicada en febrero de 2018.
2. Basada en el Marco de Trabajo de Ciberseguridad NIST.
3. Ofrece una vision sobre cómo aprovechar los estándares existentes para ciberseguridad.

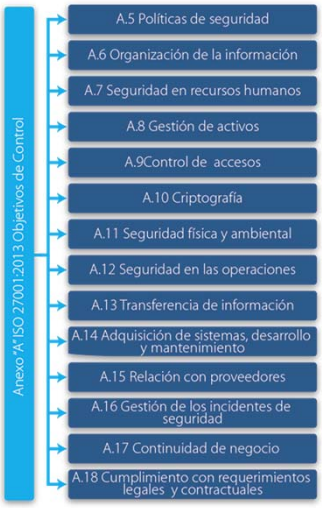
NIST = Instituto Nacional de Estándares y Tecnología (USA)

nacap

Dominios, objetivos de control y controles

- En la norma ISO 27001:2013 existen 14 dominios, 35 objetivos de control y 114 controles.
- Una de su grandes características es la importancia que le entrega a la evaluación y aprendizaje de los eventos de seguridad de TI que se centra en el programa de respuesta a incidentes.

Dominios NCH/ISO 27001



Evaluación y tratamiento de riesgos

Una de las principales atracciones ISO 27001 es el proceso de gestión del riesgo, al que se le ha querido ofrecer una gran flexibilidad.

Este proceso consiste en identificar todos los riesgos que existen y sus propietarios, analizarlos y gestionar un plan de tratamiento de los mismos que tenga en **cuenta la integridad, la disponibilidad y la confidencialidad**, es necesario intentar así adaptar este proceso a la norma ISO 31000.

Esto consigue que el proceso de evaluación de riesgos sea mucho más claro, completo y objetivo siendo un requisito de una buena gestión en cuanto a la seguridad de TI.

nacap

Mejora y Orden

La ISO reconoce que lo verdaderamente importante es la mejora continua por lo que existen muchas metodologías, aparte del ciclo PHVA, igualmente válidas para cumplir con esto.

nacap

Los Dominios Tecnológicos de Seguridad incorporan los activos de la información que van a proteger y cumplir.

A.5Dominio de la política de seguridad

Su objetivo es garantizar a la **empresa el soporte y gestión necesarios para la seguridad de la información** según todos los requisitos institucionales y normativos.

Se debe establecer la política según los objetivos establecidos por la empresa. Es necesario contar con el compromiso en cuanto a la **seguridad de la información**.

A.5 Dominio de la política de seguridad

A.5.1.1 Políticas de Seguridad de Información

Un conjunto de políticas de seguridad de información debe estar definido, aprobado por la administración, publicado y comunicado a todos los empleados y partes externas relevantes.

a. Control de acceso.
b. Clasificación de la información.
c. Seguridad física y ambiental.
d. Usuario final:
   i. Uso aceptable de activos.
   ii. Escritorio y pantalla limpios.
   iii. Transferencia de información.
   iv. Dispositivos móviles y teletrabajo.
   v. Restricciones sobre instalación y uso de software.

A.5 Dominio de la política de seguridad

A.5.1.1 Políticas de Seguridad de Información

[…] Continuación

e. Respaldos.
f. Transferencia de información.
g. Protección contra malware.
h. Gestión de vulnerabilidades técnicas.
i. Uso de controles criptográficos.
j. Seguridad en las comunicaciones.
k. Privacidad y protección de información personal.
l. Relaciones con proveedores.

RECOMENDACIÓN
Instituciones pequeñas -> Pocos documentos
Instituciones grandes -> Documentos específicos

En general, es preferible reducir la documentación

A.6 Dominio de la organización en cuanto a la seguridad de la información

Su finalidad es instaurar un marco de referencia para definir el camino para la implantación y control de la seguridad de la información dentro de la empresa.

La dirección de la empresa es la responsable de establecer la política de seguridad, además debe establecer los roles de los comités y nombrar al encargado mediante una resolución. El Encargado debe coordinar y revisar el proceso.

A.6 Dominio de la organización en cuanto a la seguridad de la información

A.06.01.01 Roles y responsabilidades en seguridad de la información

Todas las responsabilidades de seguridad de información deben estar claramente definidas:

- Custodio de los datos.
- Comité de seguridad.
- Encargado de seguridad.
- Administrador de seguridad.
- Custodio físico.
- Personal y usuarios de los recursos en general.



A.7 Dominio de seguridad de los recursos humanos

Su objetivo es fijar las medidas necesarias para **controlar la seguridad de la información**, que ha sido manejada por los recursos humanos de la empresa.

nacap

A.7 Dominio de seguridad de los recursos humanos

A.07.02.02 Capacitación, educación y entrenamiento en seguridad de información

Todos los funcionarios y, eventualmente, los contratistas, deben recibir capacitación, entrenamiento y actualizaciones regulares en las políticas y procedimientos de la organización que sean relevantes para su función laboral.



nacap

A.8 Dominio de gestión de activos

Este dominio tiene el objetivo de llevar a cabo una protección adecuada en cuanto a los activos de la empresa.

En todo momento los activos se encuentran inventariados y controlados por un responsable que también se encarga de manipularlos de forma correcta.

nacap

A.8 Dominio de gestión de activos

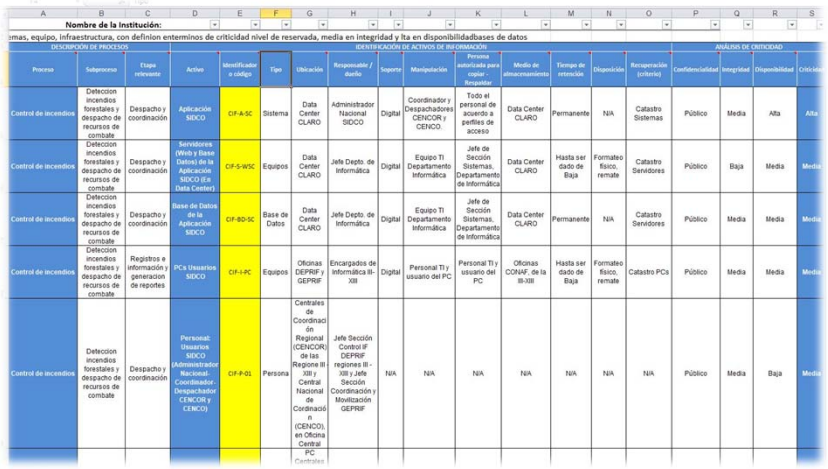
A.08.01.01 Inventario de Activos

Todos los activos asociados con la información y las instalaciones para su procesamiento deben estar claramente identificados, y debe existir un inventario de los mismos; revisado y sujeto a mantenimiento.



nacap

A.8 Dominio de gestión de activos



Nombre de la Institución:

...mas, equipo, Infraestructura, con definion enterminos de criticidad nivel de reservada, media en Integridad y Ita en disponibilidadbases de datos

DESCRIPCION DE PROCESOS			IDENTIFICACIÓN DE ACTIVOS DE INFORMACION												ANÁLISIS DE CRITICIDAD			
Proceso	Subproceso	Etapa relevante	Activo	Identificador o código	Tipo	Ubicación	Responsable / dueño	Soporte	Manipulación	Persona autorizada para copiar - Respaldar	Medio de almacenamiento	Tiempo de retención	Disposición	Recuperación (criterio)	Confidencialidad	Integridad	Disponibilidad	Criticidad
Control de incendios	Deteccion incendios forestales y despacho de recursos de combate	Despacho y coordinación	Aplicación SIDCO	CIF-A-SC	Sistema	Data Center CLARO	Administrador Nacional SIDCO	Digital	Coordinador y Despachadores CENCOR y CENCO.	Todo el personal de acuerdo a perfiles de acceso	Data Center CLARO	Permanente	N/A	Catastro Sistemas	Público	Media	Alta	Alta
Control de incendios	Deteccion incendios forestales y despacho de recursos de combate	Despacho y coordinación	Servidores (Web y Base Datos) de la Aplicación SIDCO (En Data Center)	CIF-S-WSC	Equipos	Data Center CLARO	Jefe Depto. de Informática	Digital	Equipo TI Departamento Informática	Jefe de Sección Sistemas, Departamento de Informática	Data Center CLARO	Hasta ser dado de Baja	Formateo físico, remate	Catastro Servidores	Público	Baja	Media	Media
Control de incendios	Deteccion incendios forestales y despacho de recursos de combate	Despacho y coordinación	Base de Datos de la Aplicación SIDCO	CIF-BD-SC	Base de Datos	Data Center CLARO	Jefe Depto. de Informática	Digital	Equipo TI Departamento Informática	Jefe de Sección Sistemas, Departamento de Informática	Data Center CLARO	Permanente	N/A	Catastro Servidores	Público	Media	Media	Media
Control de incendios	Deteccion incendios forestales y despacho de recursos de combate	Registros e información y generacion de reportes	PCs Usuarios SIDCO	CIF-I-PC	Equipos	Oficinas DEPRIF y GEPRIF	Encargados de Informática III-XIII	Digital	Personal TI y usuario del PC	Personal TI y usuario del PC	Oficinas CONAF, de la III-XIII	Hasta ser dado de Baja	Formateo físico, remate	Catastro PCs	Público	Media	Media	Media
Control de incendios	Deteccion incendios forestales y despacho de recursos de combate	Despacho y coordinación	Personal: Usuarios SIDCO (Administrador Nacional- Coordinador- Despachador CENCOR y CENCO)	CIF-P-01	Persona	Centrales de Coordinación Regional (CENCOR) de las Regione III - XIII y Central Nacional de Coordinación (CENCO), en Oficina Central PC Centrales	Jefe Sección Control IF DEPRIF regiones III - XIII y Jefe Sección Coordinación y Movilización GEPRIF	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Público	Media	Baja	Media

A.9 Dominio control de acceso

Se asegura el acceso autorizado a todos los sistemas de información de la empresa. Es necesario realizar diversas acciones como controles para evitar el acceso de usuarios no autorizados, controles de entrada, etc.

A.9 Dominio control de acceso

A.09.01.01 Política de Control de Acceso

Debe ser establecida, documentada y revisada una Política de Control de Acceso, basándose en los requerimientos de negocios y seguridad.



nacap

A.9 Dominio control de acceso

A.09.01.02 Acceso a redes y servicios de red

Los usuarios sólo deben ser provistos de acceso a las redes y servicios de red que ellos estén específicamente autorizados para usar:

- Roles y activos se cruzan en una matriz de accesos y privilegios.
- Control de Acceso basado en roles.

Activo / Rol	Activo 1	Activo 2	Activo 3
Funcionario A	Lectura Escritura Borrado	Lectura	Sin acceso
Funcionario B	Sin acceso	Sin acceso	Lectura Escritura Borrado
Funcionario C	Lectura	Lectura Escritura Borrado	Lectura

nacap

A.9 Dominio control de acceso

A.09.04.03 Sistemas de administración de contraseñas

Los sistemas para el manejo de contraseñas serán interactivos y asegurarán el uso de contraseñas de calidad.

- Directorio Activo.
- Equivalente bajo costo.
- LDAP.



nacap

A.11 Dominio en cuanto la seguridad física y del medio ambiente

Con este dominio se consigue proteger todas las instalaciones de la empresa y toda la información que maneja.

Por esto, se establecen diferentes barreras de seguridad y controles de acceso.

nacap

A.11 Dominio en cuanto la seguridad física y del medio ambiente

A.11.01.01 Perímetro de Seguridad Física

Un perímetro de seguridad debe estar definido y en uso para proteger áreas que contengan información o instalaciones de procesamiento, sean críticas o sensibles:

- Clasificar zonas.
- Protocolos de trabajo y circulación.
- Acceso basado en roles.



nacap

A.12 Dominio gestión de las comunicaciones y operaciones

El objetivo se encuentra en determinar los procesos y responsabilidades de las operaciones que lleva a cabo la organización. Se debe asegurar que todos los procesos se encuentren relacionados con la información ejecutada de forma adecuada.

nacap

A.12 Dominio gestión de las comunicaciones y operaciones

A.12.01.04 Separación de instalaciones de desarrollo, pruebas y operación

Las ambientes de desarrollo, prueba y operación deben estar separados para reducir el riesgo de acceso no autorizado o cambios en el ambiente operacional.



nacap

A.12 Dominio gestión de las comunicaciones y operaciones

A.12.02.01 Controles contra código malicioso

Controles de detección, prevención y recuperación deben estar implantados para protegerse contra el código malicioso. Además, debe implementarse un procedimiento de concientización de usuarios.



nacap

A.12 Dominio gestión de las comunicaciones y operaciones

A.12.05.01 Instalación de software en sistemas operacionales

Para controlar la instalación de software en sistemas operacionales, deben existir procedimientos implementados.



nacap

A.12 Dominio gestión de las comunicaciones y operaciones

A.12.04.01 Registros de eventos

Registros de las actividades de los usuarios, excepciones, fallas y eventos de seguridad de información deben producirse, resguardarse y probarse periódicamente.



nacap

A.12 Dominio gestión de las comunicaciones y operaciones

A.12.04.03 Registros de administrador y operador

Las actividades de administradores y operadores deben ser registradas. Estos registros deben ser protegidos y revisados periódicamente.



nacap

A.12 Dominio gestión de las comunicaciones y operaciones

A.12.03.01 Respaldos de información

Copias de respaldo de información y software deben realizarse y probarse periódicamente, en conformidad con la política de respaldo acordada.



nacap

A.12 Dominio gestión de las comunicaciones y operaciones

A.12.06.02 Restricción de instalación de software

Deben establecerse e implementarse reglas para controlar la instalación de software por parte de los usuarios.



nacap

A.12 Dominio gestión de las comunicaciones y operaciones

A.12.04.04 Sincronización de Reloj

Los relojes de todos los sistemas que procesan información relevante en una organización o dominio de seguridad deben estar sincronizados con una fuente de señal horaria confiable y previamente acordada.



nacap

A.12 Dominio gestión de las comunicaciones y operaciones

A.12.06.01 Gestión de vulnerabilidades técnicas

Debe obtenerse oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información en uso, evaluar el nivel de exposición de la organización, y tomar las medidas apropiadas en relación al riesgo asociado.



nacap

A.12 Dominio gestión de las comunicaciones y operaciones

A.12.01.04 Separación de instalaciones de desarrollo, pruebas y operación

Las ambientes de desarrollo, prueba y operación deben estar separados para reducir el riesgo de acceso no autorizado o cambios en el ambiente operacional.



nacap

A.13 Transferencia de Información

A.13.01.01 Controles de Red

Las redes deben ser administradas y controladas adecuadamente para proteger la información en sistemas de información y aplicaciones.



nacap

A.13 Transferencia de Información

A.13.01.02 Seguridad de los servicios de red

Los mecanismos de seguridad, niveles y requerimientos de todos los servicios de red deben estar identificados e incluidos en un acuerdo de nivel de servicios de red, indistintamente de si son prestados *in_house* o son externalizados.



nacap

A.14 Dominio de adquisición, desarrollo y mantenimiento de los sistemas de información

Este dominio se encuentra dirigido a aquellas empresas que desarrollen software internamente o que tenga un contrato con otra empresa que se encarga de desarrollarlo. Se tiene que establecer los requisitos en la etapa de implantación y desarrollo de software para que sea seguro.

A.14 Dominio de adquisición, desarrollo y mantenimiento de los sistemas de información

A.14.01.02 Seguridad de aplicaciones de servicio en redes publicas

La información involucrada con servicios de aplicación que pasan a través de redes públicas debe estar protegida de actividades fraudulentas, disputas contractuales,
o modificaciones y divulgación no autorizadas.



A.14 Dominio de adquisición, desarrollo y mantenimiento de los sistemas de información

A.14.02.01 Política de desarrollo seguro

Deben establecerse y aplicarse, para los desarrollos al interior de la organización, reglas para el desarrollo de software y sistemas



nacap

A.14 Dominio de adquisición, desarrollo y mantenimiento de los sistemas de información

A.14.02.02 Procedimientos de Control de Cambios en sistemas

Los cambios a los sistemas dentro del ciclo de vida de desarrollo deben ser controlados a través del uso de un procedimiento formal de control de cambios.



nacap

A.14 Dominio de adquisición, desarrollo y mantenimiento de los sistemas de información

A.14.02.05 Principios de ingeniería de software segura

Deben estar establecidos, documentados, mantenidos y aplicados, principios de ingeniería de software segura a los esfuerzos de implementación de cualquier sistema de información.



nacap

A.14 Dominio de adquisición, desarrollo y mantenimiento de los sistemas de información

A.14.02.06 Ambiente de desarrollo seguro

Las organizaciones deben establecer y proteger apropiadamente un ambiente de desarrollo seguro para sistemas de información, junto con esfuerzos de integración que cubran la totalidad del ciclo de vida de desarrollo de sistemas.



nacap

A.14 Dominio de adquisición, desarrollo y mantenimiento de los sistemas de información

A.14.02.08 Pruebas de seguridad de sistemas

Pruebas a las funcionalidades de seguridad deben llevarse a cabo durante el desarrollo.



nacap

A.14 Dominio de adquisición, desarrollo y mantenimiento de los sistemas de información

A.14.02.09 Pruebas de aceptación de sistemas

Programas de prueba de aceptación de sistemas y criterios relativos deben estar establecidos para los nuevos sistemas de información, actualizaciones o nuevas versiones.



nacap

A.15 Relaciones con proveedores

A.15.02.01 Monitoreo y revisión de los proveedores de servicios

La organización debe monitorear, revisar y auditar periódicamente la prestación del servicio del proveedor.



nacap

A.16 Dominio de gestión de incidentes en la seguridad de la información

Con este dominio se aplica un proceso de mejora continua en la gestión de percances de seguridad de la información.

nacap

A.16 Dominio de gestión de incidentes en la seguridad de la información

A.16.01.02 Reportar eventos de seguridad de información

Los eventos de seguridad de información deben ser reportados a través del canal administrativo más rápido posible.



nacap

A.16 Dominio de gestión de incidentes en la seguridad de la información

A.16.01.05 Respuesta a incidentes de seguridad de información

Los incidentes de seguridad de información deben ser respondidos en concordancia con procedimientos documentados.



nacap

A.17 Dominio de gestión de continuidad de negocio

El objetivo es asegurar la continuidad operativa de la empresa.

Se requiere aplicar controles que eviten o reduzcan todos los incidentes de las actividades desarrolladas por la empresa que puedan generar un impacto.

nacap

A.17 Continuidad de negocio

A.17.01.01 Planificación de continuidad de seguridad de información

La organización debe determinar sus requerimientos para seguridad de información y la continuidad de la gestión de seguridad de información en condiciones adversas. Por ejemplo, durante una crisis o desastre.



nacap

A.18 Dominio de cumplimiento

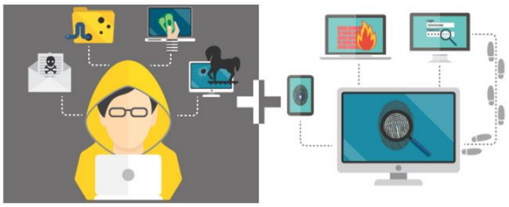
Su finalidad es asegurar que los requisitos legales de seguridad que han sido referidos al diseño y gestión de los sistemas de información.

nacap

A.18 Dominio de cumplimiento

A.18.02.01 Revisiones independientes de seguridad de información

El enfoque de la organización a la gestión de seguridad de información y su implementación; es decir, objetivos de control, controles, políticas, procesos y procedimientos, deben ser revisados por alguna entidad independiente, en intervalos periódicos planificados o cuando ocurra algún cambio importante.



nacap

A.18 Dominio de cumplimiento

A.18.02.02 Cumplimiento de políticas y estándares de seguridad

Los administradores deben revisar regularmente que el procesamiento de información y los procedimientos, dentro de su área de responsabilidad, cumplen con las políticas, estándares y/o cualquier otro requerimiento de seguridad.



nacap

A.18 Dominio de cumplimiento

A.18.02.02 Cumplimiento de políticas y estándares de seguridad

Los administradores deben revisar regularmente que el procesamiento de información y los procedimientos, dentro de su área de responsabilidad, cumplen con las políticas, estándares y/o cualquier otro requerimiento de seguridad.



nacap

A.18 Dominio de cumplimiento

A.18.02.03 Revisión de cumplimiento técnico

Los sistemas de información deben ser revisados regularmente para asegurar el cumplimiento de las políticas y estándares de seguridad de la organización.



nacap