Optimizando los procesos de adecuación de frameworks (ISO 27001, NIST, ENS) y hardening con herramientas de automatización.

opencloud factory

opennac enterprise

Índice

Claves del documento:

¿A quién va dirigido este documento?

Este documento va dirigido a aquellas empresas y personal involucrado en procesos de adecuación de marcos de buenas prácticas, interesados en conocer cómo a partir de una solución tecnológica se pueden automatizar y centralizar procesos mecánicos iterativos propios de las auditorías.

¿Qué ofrece el contenido de este whitepaper?

El documento presenta un contexto de certificación de los frameworks ISO 27001, NIST y ENS, haciendo zoom en cada uno de ellos para presentar cómo sus iniciativas para la gestión del riesgo son coincidentes entre sí, y cómo pueden automatizarse varias tareas de manera que se agilicen los procesos de certificación. Se hace especial hincapié sobre las iniciativas relacionadas con **la necesidad de gestionar y realizar bastionado (hardening) de las configuraciones de los dispositivos de red y el respectivo back-up de las configuraciones.**

Principales desafíos a los que se enfrentan las compañías en este contexto

En el documento se ilustran algunos de los desafíos más comunes que tienen que ver con estas iniciativas de gestión de riesgo y cómo se podrían superar articulando las tareas repetitivas más operativas sobre una herramienta de automatización, liberando al empleado de la carga laboral que el proceso de adecuación de un estándar de buenas prácticas supone.

Soluciones que se aportan en este documento

Finalmente, en este documento se recomienda el módulo Network Device Compliance de OpenNAC Enterprise, una solución capaz de centralizar y automatizar parte del proceso de auditoría y hardening de las configuraciones de la electrónica de red, comparando configuraciones actuales con líneas base y best practices de configuración.

La adecuación de un marco de buenas prácticas como NIST, ISO 27001 o ENS, entre otros, demanda optimización. La optimización de los procesos y procedimientos de seguridad en un departamento de IT en una empresa tras la adecuación de un framework de buenas prácticas, depende de las dinámicas entre el personal técnico operativo y las plataformas tecnológicas, siendo la automatización de tareas repetitivas el factor clave para lograr este objetivo.

La motivación para que las empresas consideren la adopción de un framework de buenas prácticas puede ser diferente para cada caso. La cantidad de trabajo que demanda la adecuación de un estándar no es trivial: la inversión es significativa y generalmente la iniciativa está vinculada con una necesidad o un requerimiento que podemos distinguir entre los 3 siguientes:

1. **Un requerimiento legal:** Principalmente en empresas de un determinado nicho que se encuentran sujetas a regulaciones de gobierno o su mercado demanda cierto sello de certificación.

2. **La necesidad de mercado:** Algunos mercados requieren sellos de calidad porque el cliente encuentra este hecho diferenciador con la competencia. Generalmente ocurre en mercados donde se maneja información sensible como datos personales, información financiera, etc.

3. **Necesidad corporativa:** Las empresas que gestionan un número importante de servicios e información requieren implementar modelos de gestión para estandarizar procesos. A menudo, esta estandarización se logra con la adecuación de un framework de buenas prácticas.

El proceso de adopción de un estándar de buenas prácticas para la gestión de la seguridad de la información está, por lo general, vinculado al cumplimiento de una regulación vigente o una iniciativa organizacional para establecer un sello de calidad que permita generar un factor diferenciador entre competidores del mismo nicho. A su vez, la adecuación de un marco de buenas prácticas requiere un proceso de evaluación continua de implantación de las iniciativas sugeridas en este. Por lo general, esta evaluación se ejecuta mediante un proceso de auditoría dentro de las compañías.

ISO 27001 Certified

NIST National Institute of Standards and Technology U.S. Department of Commerce

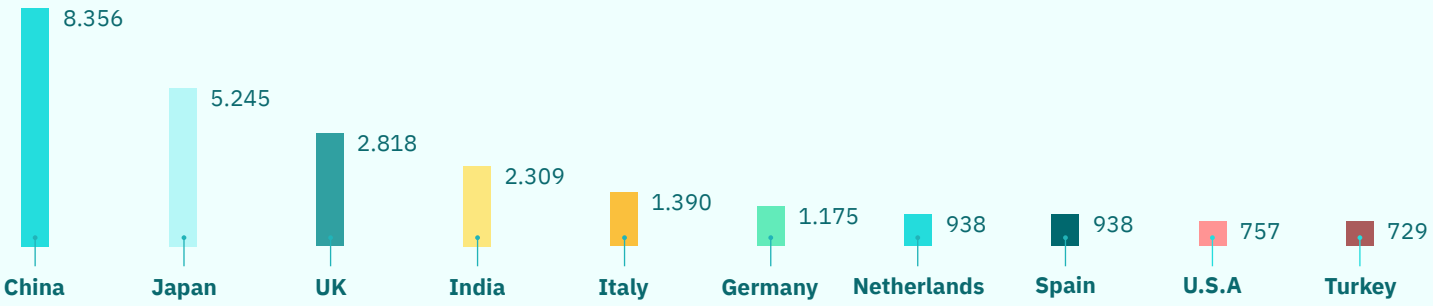
ens Esquema Nacional de Seguridad

ISO 27001

La norma **ISO 27001** es uno de los marcos de buenas prácticas más populares y reconocidos que existen actualmente gracias a sus altos estándares de construcción y aplicación. De acuerdo con una encuesta realizada por Deloitte en el año 2019, el 80% de las compañías que realizan sus operaciones de seguridad en España se adecúan a la **ISO 27001**. Por este motivo, lo hemos tomado como referente y revisaremos algunos aspectos relevantes de este modelo y su masiva relevancia en el mundo de la seguridad IT.

Según la propia **Organización Internacional de Estandarización** (ISO, International Standarization Organization en inglés), el año pasado se certificaron 36.362 compañías en el mundo en este estándar de seguridad, siendo España el octavo país del mundo con más empresas certificadas en **ISO 27001.** Dicha organización ha creado la norma **ISO 27001** con el objeto de ofrecer una norma viable y óptima para promover la correcta gestión de servicios de las tecnologías de la información (ITSM).

Top 10 países con mayor número de empresas certificadas en ISO 27001 en 2019

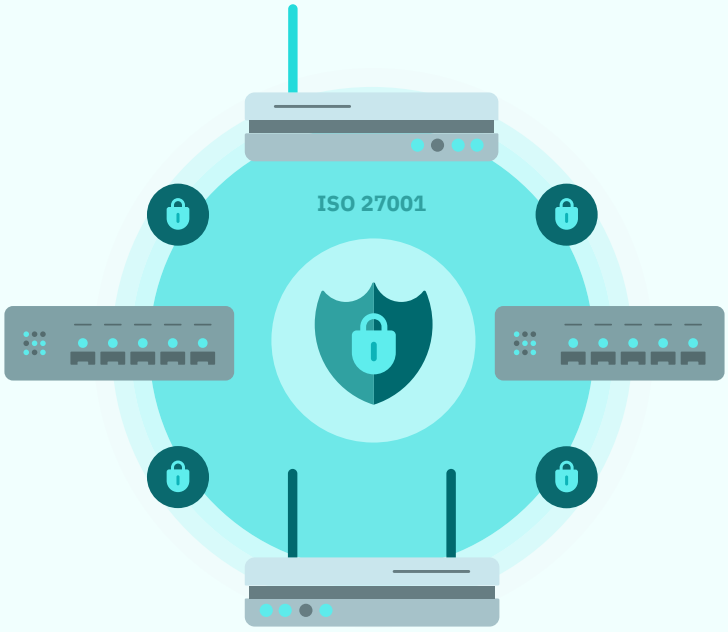


Adicionalmente, los sectores con un mayor número de empresas certificadas en 2019 fueron los siguientes:

1.	**Tecnología de la información**	8562	6.	**Construcción**	410
2.	**Otros servicios**	1435	7.	**Salud y trabajo social**	408
3.	**Logística, almacenaje y comunicaciones**	989	8.	**Servicios de ingeniería**	369
4.	**Intermediación financiera, inmobiliaria, renting**	560	9.	**Equipamiento eléctrico y óptico**	36
5.	**Textil y productos textiles**	499	10.	**Venta al por mayor y retail, reparación de vehículos a motor, bienes personales e inmuebles**	366

Esta norma internacional especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. Este estándar internacional también incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en este framework son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente del tipo, tamaño o naturaleza.

El sistema de gestión de seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas en que los riesgos se gestionan adecuadamente. En consecuencia, el marco **ISO 27001** toma la evaluación de riesgos como eje central para así ofrecer una metodología estandarizada que permita a la organización valorar su nivel de seguridad informática.



El número total de controles en la **ISO 27001** son 114, distribuidos en 35 objetivos de control y 14 dominios. Los 114 controles abarcan todas las buenas prácticas para el establecimiento de un sistema de gestión de seguridad de la información. En estos 114 controles se incluyen controles específicos de buenas prácticas para gestionar la configuración de los dispositivos de red, las vulnerabilidades asociadas y sus copias de seguridad.

En la siguiente tabla se han consolidado los controles específicos para la gestión de las vulnerabilidades, las copias de respaldo (back-ups), y algunos otros que hacen referencia al cumplimiento y tareas propias del proceso de auditoría. Estos controles, a su vez, aterrizan en acciones técnicas que generalmente se apoyan en infraestructura tecnológica y recursos humanos. Este hecho, sumado a la naturaleza de los procesos de adecuación de un framework, generan tareas operativas repetitivas que sobrecargan al equipo técnico de actividades susceptibles de automatizar por medio de herramientas tecnológicas.

ISO 27001			
Dominio	**Objetivo**	**Control**	**Descripción**
12. Seguridad en la operativa.	**12.3** Copias de Respaldo	**12.3.1** Copias de Respaldo de información	Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
	12.6 Gestión de la vulnerabilidad técnica.	**12.6.1** Gestión de las vulnerabilidades técnicas.	Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
	12.7 Consideraciones de las auditorías de los sistemas de información.	**12.7.1** Controles de auditoría de los sistemas de información.	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
18. Cumplimiento	**18.2** Revisiones de la seguridad de la información.	**18.2.3** 18.2.3 Comprobación del cumplimiento.	Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Encontrar una herramienta que genere y almacene los back-ups de forma automática, libera al equipo técnico de la necesidad de ir dispositivo a dispositivo generando un back-up y llevarlo a un repositorio centralizado donde se tendrán que organizar de manera lógica y a su vez realizar el respectivo mantenimiento. Así como esta buena práctica de generación y almacenamiento de backups requiere un esfuerzo técnico, además de cierta infraestructura, todas las adecuaciones de framework demandan acciones que a menudo se soportan sobre infraestructura tecnológica y tareas iterativas de los recursos humanos. Optimizar un proceso de auditoría de **ISO 27001** requiere herramientas tecnológicas que liberen al recurso humano de tareas por medio de la automatización y estén alineados con los requerimientos del framework.

Existen diversas soluciones en el mercado de seguridad digital que facilitan la adecuación de estándares de seguridad para las compañías. **OpenNAC Enterprise** apoya la implementación de la **ISO 27001** en las organizaciones, soporta de manera parcial o total el despliegue de 27 de los 114 controles de la norma, entre ellos los que incluimos en la tabla anterior.

NIST

El marco de trabajo NIST (National Institute of Standards and Technology) es un marco que propone un curso de acciones futuras de protección gracias a que sus directrices definen una correcta gestión de los riesgos asociados a la ciberseguridad de las organizaciones.

NIST surge de la Orden Ejecutiva del entonces Presidente de los EEUU, Barack Obama, quien en su preocupación por la seguridad nacional de su país producto de una serie de ciberataques delegó al NIST (National Institute of Standards and Technology) la creación de un marco de trabajo de modernización de la ciberseguridad de sus infraestructuras críticas.

De acuerdo con un estudio realizado por Deloitte, el 37% de las empresas que realizan sus operaciones de seguridad en España usa NIST como marco de referencia.

NIST FRAMEWORK tiene un marco básico o Framework Core, que está integrado por una serie de iniciativas de ciberseguridad y posee cuatro elementos: funciones, categorías, subcategorías y referencias informativas.

- Adicionalmente, ofrece una serie de prácticas necesarias para lograr cada objetivo de seguridad y provee referentes de orientación. **NIST considera en el centro de las actividades la gestión de riesgos y se divide en tres secciones: el núcleo, los perfiles y los niveles de implementación:**
- **El núcleo comprende cinco funciones (Identificar, Proteger, Detectar, Responder y Recuperar), que se dividen a su vez en categorías y subcategorías.**

Identificar: busca la visibilidad de los activos que componen la red informática.

Proteger: efectúa la aplicación de políticas de control que aseguren la red informática.

Detectar: genera un contexto de monitorización continua de la red informática.

Responder: propone actividades para la gestión de incidencias en la red informática.

Recuperar: establece una serie de actividades para la recuperación después de una incidencia en la red informática (resiliencia).

NIST tiene descritos a su vez sus Niveles de implementación. Los niveles tienen como finalidad enmarcar a la organización dentro de un contexto predefinido de acuerdo a su entorno, sus prácticas y sus políticas:

- **Parcial:** la gestión de riesgos no es una actividad formal, más bien reactiva.
- **Riesgo informado:** las prácticas de gestión de riesgos están aprobadas por los directivos y administradores pero no están generalizadas en todas las áreas de la organización.
- **Repetible:** las prácticas de gestión de riesgos se formalizan y generalizan dentro de la organización bajo la denominación de políticas.
- **Adaptativo:** las políticas se adaptan a los cambios y evolucionan a partir de las lecciones obtenidas en experiencias pasadas.

Los perfiles son selecciones de funciones, categorías y subcategorías centrales que ayudan a las organizaciones a priorizar los resultados y las actividades que mejor satisfacen sus riesgos o necesidades comerciales. El perfil actual de una organización establece sus resultados de gestión de riesgos de ciberseguridad existentes, y un perfil objetivo indica los resultados que desea lograr.

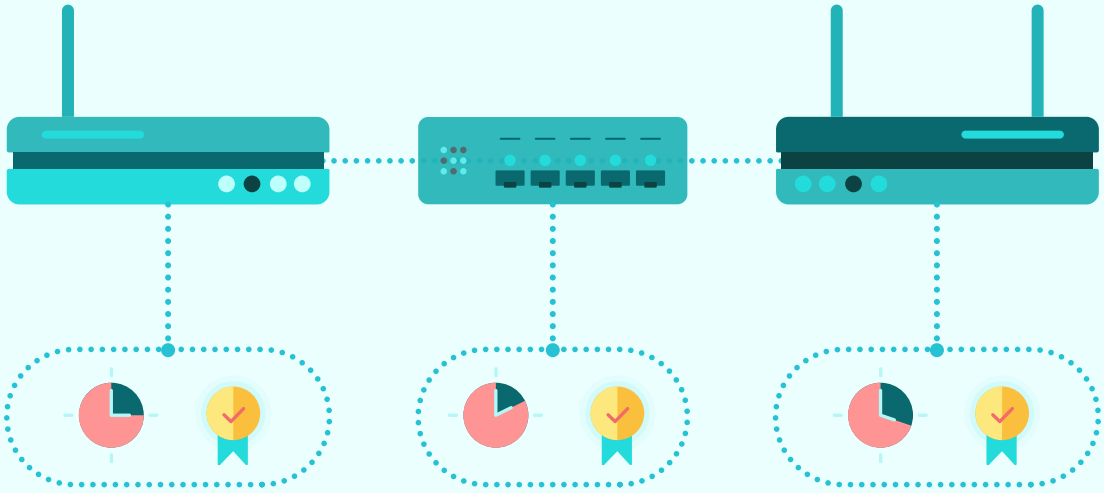
Al igual que en ISO 27001, con el objetivo de evidenciar cómo los distintos estándares abordan iniciativas comunes para la gestión de un compilado de riesgos identificados hemos extraído las subcategorías específicas para la gestión de las vulnerabilidades, y el bastionado (hardening) de configuración de dispositivos de red. Nuevamente, estas subcategorías aterrizan en acciones técnicas que generalmente se apoyan en infraestructura tecnológica y recursos humanos.

NIST			
Función	**Categoría**	**ID**	**Subcategoría**
Identificar	Evaluación de Riesgos	ID-RA-1/6	Las vulnerabilidades de los activos se identifican y documentan
		ID-RA-5/6	Las amenazas, vulnerabilidades, probabilidades e impactos se utilizan para determinar el riesgo.
Proteger	Procesos y procedimientos de protección de la información	PR.IP-1/12	Se crea y mantiene una configuración base de equipos TI / sistemas de control industrial incorporando principios de seguridad.
		PR.IP-4/12	Se realizan, mantienen y prueban copias de seguridad de la información
	Tecnología de Protección	PR-PT-3/5	El principio de funcionalidad mínima se incorpora configurando sistemas para proporcionar solo capacidades esenciales

Los procesos de adecuación de **NIST** generan tareas operativas repetitivas que sobrecargan al equipo técnico con actividades tales como el reporting o la remediación de los hallazgos. Algunas de estas tareas pueden perfectamente automatizarse con la ayuda de soluciones tecnológicas.

Supongamos que un auditor durante el proceso de adecuación de **NIST** ha encontrado habilitados los protocolos que no se usan en los dispositivos de red de la organización. Su hallazgo para este caso ha sido que los dispositivos de red no cumplen con el principio del mínimo privilegio. La compañía tiene 100 switches. Para incorporar el principio de mínima funcionalidad tenemos entonces que deshabilitar los protocolos SNMP v1 y SNMP v2 ya que la versión recomendada y que se utiliza en la compañía es SNMP v3. El tiempo necesario para realizar esta tarea sin una herramienta que automatice la configuración necesaria para deshabilitar los protocolos obsoletos sería de entre 2 y 3 horas aproximadamente (considerando en promedio 1.5 minutos por switch).

Este tiempo se puede incrementar drásticamente si hablamos de configuración de interfaces. Con una solución que nos ayude a automatizar la evaluación de la configuración actual y la remedición de parámetros de configuración se podría realizar de forma inmediata y programarse dentro de horarios de baja carga, liberando a los recursos humanos de las tareas y minimizando el riesgo del cambio.



Optimizar un proceso de adecuación de **NIST** requiere de soluciones tecnológicas que liberen al recurso humano de tareas por medio de la automatización. **OpenNAC Enterprise** apoya la implementación de la **NIST** CSF en las organizaciones, soporta de manera parcial o total el despliegue de 26 de las 108 subcategorias incluidas en el estandar, entre ellos los que incluimos en la tabla anterior.

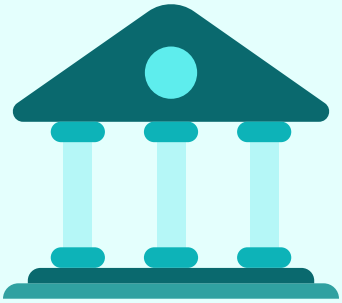
ENS

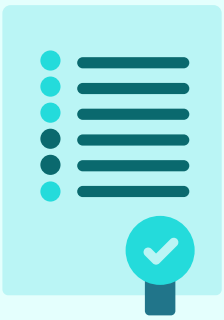
El Esquema Nacional de Seguridad de España se regula a través del Real Decreto 3/2010, del 8 de enero. Es de obligatorio cumplimiento para entidades del gobierno y para proveedores que deseen contratar con entidades de gobierno, por lo que este estándar persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

Este framework está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

El objeto último de la seguridad de la información es asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad, deberán tenerse en cuenta los siguientes principios básicos:

a. **Seguridad integral.**
b. **Gestión de riesgos.**
c. **Prevención, reacción y recuperación.**
d. **Líneas de defensa.**
e. **Reevaluación periódica.**
f. **Función diferenciada.**





Dentro del **ENS** existen75 medidas de seguridad que serían los equivalentes a los controles de la **ISO 27001** o las subcategorías de **NIST.** Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos, se aplicarán las medidas de seguridad.

Las medidas de seguridad se dividen en tres grupos:

1. **Marco organizativo [org]:**
   Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.

2. **Marco operacional [op]**
   Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

3. **Medidas de protección [mp]**
   Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

De la misma forma que hemos hecho para **NIST** e **ISO 27001** anteriormente en este documento, vamos a extraer las iniciativas concretas en el **ENS** que abordan la necesidad de gestionar y realizar bastionado (hardening) de las configuraciones de los dispositivos de red y sus back-ups. En la siguiente tabla se han consolidado las medidas de seguridad del **ENS** que hacen referencia a la gestión del bastionado (hardening) de configuración de dispositivos de red y la recolección de back-ups de configuración.

En este documento recomendamos la solución **EMMA**, y más concretamente su módulo Cumplimiento, para abordar la cuestión relacionada con el cumplimiento del Esquema Nacional de Seguridad. **EMMA - Cumplimiento** es un módulo dentro de la solución **EMMA** que centraliza y automatiza parte del proceso de auditoría de las configuraciones de la electrónica con las configuraciones de las guías STIC (ROCÍO). Esta solución facilita la adecuación a estándares como el **ENS** y garantiza la implementación segura de la tecnología de control de acceso a la red.

EMMA - Cumplimiento

Esquema Nacional de Seguridad				
Medidas de Seguridad	**Marco operacional (OP)**	**Explotación (exp)**	Configuración de Seguridad	Se configurarán los equipos previamente a su entrada en operación, de forma que: **a.** Se retiren cuentas y contraseñas estándar. **b.** Se aplicará la regla de “mínima funcionalidad” **c.** Se aplicará la regla de “seguridad por defecto”
			Gestión de la Configuración	Se gestionará de forma continua la configuración de los componentes del sistema de forma que: **a.** Se mantenga en todo momento la regla de “funcionalidad mínima? ([op.exp.2]). **b.** Se mantenga en todo momento la regla de “seguridad por defecto? ([op.exp.2]). **c.** El sistema se adapte a las nuevas necesidades, previamente autorizadas ([op.acc.4]). **d.** El sistema reaccione a vulnerabilidades reportadas ([op.exp.4]). **e.** El sistema reaccione a incidentes (ver [op.exp.7]).
			Mantenimiento	Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente: **a.** Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas. **b.** Se efectuará un seguimiento continuo de los anuncios de defectos. **c.** Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.
	Medidas de Protección (MP)	**Protección de Información (si)**	Copias de seguridad (backup)	Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada. Estas copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad, según proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad. Las copias de seguridad deberán abarcar: **a.** Información de trabajo de la organización. **b.** Aplicaciones en explotación, incluyendo los sistemas operativos. **c.** Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga. **d.** Claves utilizadas para preservar la confidencialidad de la información.

¿Cuál es la problemática de las compañías en este contexto?

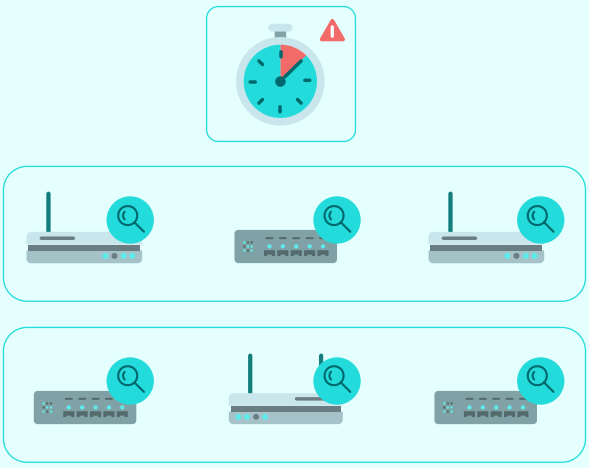
La incorporación de estas medidas de seguridad a la operación de las organizaciones toma bastante trabajo por parte del equipo técnico y, eventualmente, requiere de tecnología de apoyo para el soporte e implementación de estas buenas prácticas.

Supongamos que un organismo de la administración pública de España ha realizado una renovación tecnológica y ha cambiado todos sus switches corporativos (80 en total) de campus que daban servicio a usuarios, impresoras y teléfonos entre otros. Los nuevos switches tienen usuarios con contraseña creados por defecto y durante el proceso de adecuación del ENS, un auditor identificó que estas cuentas genéricas de usuario existen y están habilitadas, lo cual constituye un agujero de seguridad.

Para la remediación de este hallazgo, el auditor ha solicitado que estas cuentas se eliminen. De media, para la realización de esta tarea es necesario un aproximado de 1 minuto y medio por cada switch. De este modo se necesitarán aproximadamente 2 horas de un recurso que trabajaba en la migración de una base de datos.

En el mercado existe una variedad de soluciones para la gestión de la configuración de manera centralizada. Con una herramienta capaz de lanzar esta configuración de manera estándar a todos los switches tomaría un par de minutos, e incluso se podría programar para que se ejecute en la noche, evitando interrupciones de servicio.

La adecuación de estándares de buenas prácticas en los modelos de gestión de seguridad de la información dentro de las compañías y los organismos requiere de herramientas tecnológicas que faciliten y apoyen su implementación. Dichas soluciones deben proporcionar un soporte para la operación en el día a día de las compañías que se gestionan bajo un estándar. La adecuación de un framework supone carga laboral adicional, por lo que las soluciones tecnológicas están llamadas a cobrar un rol importante asumiendo esta carga y liberando, por tanto, al equipo técnico de la consecución de las tareas más mecánicas.



Los estándares se implementan bajo procesos iterativos de mejora continua. El hecho de que los procesos sean cíclicos representa trabajo repetitivo.

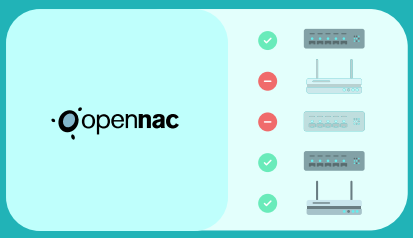
Por ello es necesario encontrar soluciones tecnológicas que automaticen las tareas repetitivas. Cuando se asume la gestión bajo un esquema de buenas prácticas el trabajo debe optimizarse: la gestión a través de buenas prácticas debe ser viable sin suponer una sobrecarga de trabajo para el personal técnico al tiempo que se optimizan los procesos. Para ello se deben adquirir plataformas que soporten los procesos o, al menos, parte de los mismos.

La optimización de los procesos y procedimientos implementados en una empresa tras la adecuación de un framework de buenas prácticas depende de las dinámicas entre el personal técnico operativo y las plataformas tecnológicas, siendo la automatización de las tareas repetitivas el factor clave para lograr este objetivo.

La solución: Network Device Compliance **(NDC)**

Network Device Compliance es un módulo dentro de la solución OpenNAC Enterprise que centraliza y automatiza parte del proceso de auditoría de las configuraciones de la electrónica con configuraciones de referencia, líneas base y best practices.

Facilita la adecuación de estándares y frameworks como ISO2700x, NIST, ENS etc. y garantiza la implementación segura de la tecnología NAC (Pure & Sure NAC). Centraliza el almacenamiento de back-ups y establece un punto de gestión de configuraciones de dispositivos de red.



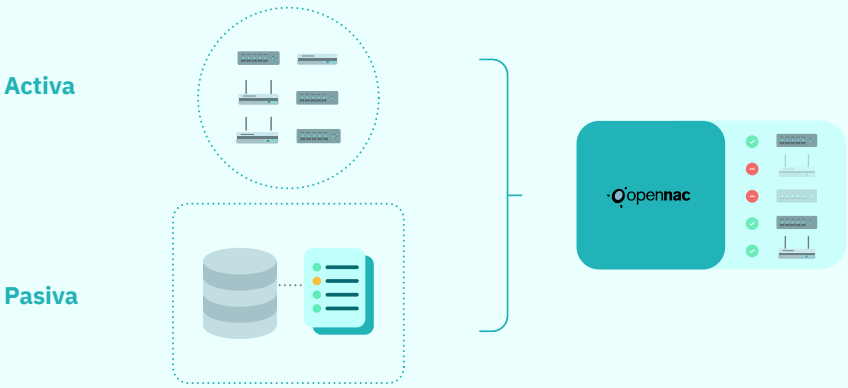
Network Device Compliance (NDC) de forma activa o pasiva

De forma activa

NDC puede lanzar reglas de comprobación activas de manera dinámica (directamente) contra dispositivos de red y de manera estática (primero generando un backlog de la configuración para posteriormente realizar la comprobación)

De forma pasiva

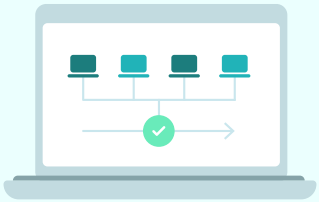
También puede realizar el mismo proceso de manera pasiva contra un repositorio de configuraciones sin tener que consultar la electrónica en ningún momento.



Puesta en marcha en 3 pasos

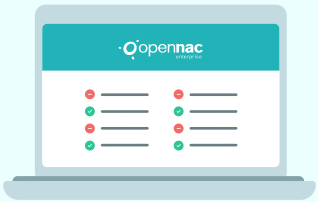
1. Dar de Alta

1. Un dispositivo de red (por SSH)
2. Un repositorio de configuraciones en el caso de una comprobación pasiva (por SCP)



2. Definir reglas y lanzar

1. Definir las reglas, grupo de reglas correspondientes para el dispositivo y/o grupo de dispositivos
2. Posibilidad de lanzar las comprobaciones en el momento o programarlas.



3. Revisar resultados

1. Desde los cuadros de mando centralizados se muestran los resultados (comprobaciones con éxito, fallos / hallazgos etc.)

"Debido a la visibilidad centralizada del dispositivo y capacidad de remediación centralizada sobre la electrónica, pudimos reducir nuestros tiempos de respuesta a incidentes de usuarios finales (en incidentes típicos) entre un 60-70%; fue un valor añadido inesperado de un proyecto NAC"

Testimonio del responsable de infrastructura y comunicaciones de uno de nuestros clientes. (Empresa multinacional de seguros)

Principales beneficios de Network Device Compliance (NDC)

1 Centraliza

Las comprobaciones de toda la electrónica se realizan desde una solución e interfaz única, simplificando y acelerando el trabajo de auditoría.

2 Automatiza

Las comprobaciones se puedan lanzar bajo demanda o de manera programada para alinearse con las tareas de auditoría.

3 Facilita la adecuación con estándares y frameworks

Se pueden implementar las reglas de comprobación de configuraciones necesarias para la adecuación de estándares y frameworks.

4 Garantiza la implementación segura de NAC

Se puede asegurar que la electrónica está correctamente configurada para que NAC funcione de manera óptima.

opencloud factory

Reconocimientos

Gartner

Único fabricante europeo de tecnología NAC incluido tres veces consecutivas en el Market Guide de Gartner

Common Criteria

Plataforma certificada en Common Criteria 3.1 release 5 por parte del Organismo de Certificación del Centro Criptológico Nacional OC-CCN de España.

CCN-CERT centro criptológico nacional

Incluido en el catálogo de productos de Seguridad de las Tecnologías de la Información y la Comunicación del Centro Criptológico Nacional, Ministerio de Defensa - Gobierno de España.

Contacta con nosotros

opencloudfactory.com

+34 91 614 53 22

Twitter
Linkedin
YouTube

Ubicaciones de Open Cloud Factory

SPAIN

MADRID.
Sede principal
Calle Segundo Mata,
6 Planta 1 Oficina 4B
Pozuelo de Alarcón, 28224

SPAIN

BILBAO.
OCF Industrial Cybersecurity
C/ Gran Vía Don Diego López
De Haro, 19-21 planta 2ª
48001

SPAIN

BARCELONA.
Centro de Desarrollo
Carrer Sant Leopold 101,
oficina 109, Terrassa,
08221

BRAZIL

SÃO PAULO.
Market Place Tower.
Av. Dr. Chucri Zaidan, 920
9º andar Cordeiro,
CEP: 04583-904

USA

BOSTON, MASSACHUSETTS.
Independence Wharf 470
Atlantic Avenue
02210

MEXICO

CIUDAD DE MÉXICO.
Presidente Masaryk 111
Piso 1, Miguel Hidalgo
Polanco V Sección
11560

opennac enterprise