proactivanet

WHITEPAPER

13 ACCIONES RÁPIDAS PARA CUMPLIR CON LOS MARCOS MÁS EXIGENTES DE SEGURIDAD

ÍNDICE

proactivanet

Introducción

En el entorno digital actual, la ciberseguridad ya no es una opción, sino una prioridad estratégica. Las amenazas evolucionan constantemente, y con ellas, también lo hacen los marcos regulatorios que buscan proteger a las organizaciones. Normativas como el Esquema Nacional de Seguridad (ENS), NIS2 o DORA están diseñadas para asegurar la confidencialidad, integridad y disponibilidad de la información.

Este documento presenta una hoja de ruta práctica compuesta por 13 acciones clave que permiten a cualquier organización avanzar rápidamente en el cumplimiento de estos marcos de seguridad. Aunque se hace referencia al ENS por su claridad y estructura, los principios son fácilmente extrapolables a otras normativas internacionales.

Marco LATAM

En América Latina, aunque no existe un único marco regulatorio regional unificado como el NIS2 o DORA, los países han ido adoptando normativas y buenas prácticas basadas en estándares internacionales como los Controles CIS o el GDPR europeo, con adaptaciones locales. Cada vez más, los organismos públicos y privados exigen niveles mínimos de seguridad y gobernanza de la información, lo que convierte el cumplimiento en un factor clave para la continuidad del negocio.

Por ejemplo:
México ha implementado lineamientos de seguridad de la información para entidades gubernamentales a través del Acuerdo de la Estrategia Digital Nacional.

Chile, la CMF (Comisión para el Mercado Financiero) requiere que las entidades reguladas, como las compañías de seguros, mantengan un inventario de activos de información. Además, el gobierno está impulsando una Ley Marco de Ciberseguridad, que propone la creación de una Agencia Nacional y establece obligaciones de reporte ante incidentes.

Perú y Colombia ya cuentan con estrategias nacionales de ciberseguridad, y están en proceso de fortalecer la supervisión y control sobre operadores críticos de infraestructura.

Panamá: La Estrategia Nacional de Ciberseguridad (ENCS), publicada en 2021 y liderada por la AIG, busca fortalecer la resiliencia digital del país. Se estructura en cinco ejes: protección de la privacidad, lucha contra ciberdelitos, defensa de infraestructuras críticas, fomento de una cultura de ciberseguridad y fortalecimiento del sector público. Destaca la campaña *Panamá Cibersegura* para educar a la ciudadanía, y

alianzas con empresas cromo Fortinet para formación y transferencia tecnológica. El Centro de Operaciones de Ciberseguridad (COCS), financiado por el BID, permite el monitoreo proactivo de amenazas. Panamá se posiciona como líder regional, ocupando el puesto 7 en el Índice Nacional de Seguridad Cibernética (NCSI). La ENCS refleja un compromiso integral del Estado con la protección digital y la transformación tecnológica.

Ecuador cuenta con una Política Nacional de Ciberseguridad vigente desde 2021, respaldada por la Ley Orgánica de Protección de Datos Personales y el Esquema Gubernamental de Seguridad de la Información (EGSI), adaptado a ISO/IEC 27001. El Ministerio de Telecomunicaciones (MINTEL) lidera las políticas, apoyado por el ECU-CERT, que gestiona incidentes cibernéticos. También opera el Consejo Nacional de Ciberseguridad para fortalecer la coordinación interinstitucional. La legislación incluye normativas como la Ley de Telecomunicaciones y el Código Penal, que tipifican y sancionan los ciberdelitos. Se promueve el uso seguro de tecnologías en sectores educativos y empresariales. Ecuador participa en iniciativas internacionales de cooperación para mejorar sus capacidades y adaptarse a estándares globales. Estas acciones buscan proteger la infraestructura crítica y los datos personales de los ciudadanos.

Si bien los niveles de madurez varían entre países, hay una clara tendencia hacia la adopción de marcos normativos que exigen:

- Inventario actualizado de activos críticos.
- Gestión de riesgos documentada y activa.
- Planes de respuesta ante incidentes.
- Capacitación continua del personal.
- Supervisión del cumplimiento por entidades reguladoras.

Acciones Clave y Beneficios

En toda auditoría hay que cumplir con tres puntos básicos:

1. Tener generada y publicada la documentación.
2. Haber aplicado las medidas que recomienda la norma o la regulación aplicable.
3. Generar evidencias de la aplicación de esas medidas y de las revisiones posteriores.

A continuación, se detallan algunas acciones clave para cumplir con los controles del ENS, junto con los beneficios asociados:

1. Gestión de Activos e Inventario

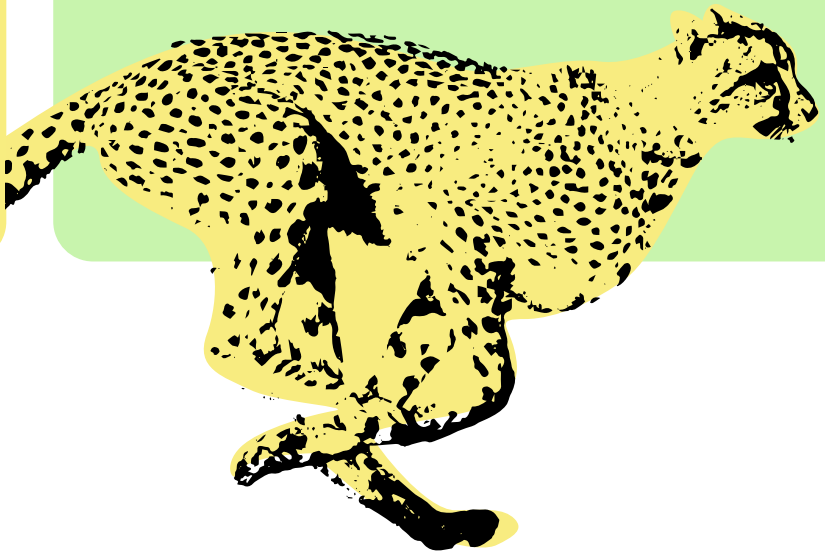
Contar con un inventario completo y actualizado de hardware, software y datos es el primer paso para asegurar la infraestructura.

Acciones Recomendadas

- Despliega los agentes específicos de cada Sistema Operativo dentro de la organización.
- Despliega los agentes que detectan equipos virtualizados, tanto OnPremise como en la nube (IaaS).
- Revisa y hazle seguimiento al listado de equipos “Pdtes. de inventariar” para inventariar todos los equipos de la organización y eliminar la “Shadow IT” de la organización.
- Asignar responsables a cada equipo o servicio.
- Genera las etiquetas de los equipos con un QR identificativo.
- Realiza revisiones periódicas de inventario para asegurar que la información esté actualizada.

Beneficios

- Conocimiento preciso de los activos y sus responsables.
- Identificación de activos críticos y sus dependencias.
- Facilitación de la gestión de riesgos y vulnerabilidades.
- Acceso rápido y sencillo a los datos del equipo leyendo QR.



2. Supervisión del Estado de Seguridad

Una organización no puede proteger lo que no sabe que está en riesgo. Supervisar continuamente el estado de los sistemas es clave.

Acciones Recomendadas

- Estado del Antivirus & Antispyware (instalado, activo, caducado, detenido)
- Estado del Firewall (instalado, activo)
- Equipos Windows con parches de seguridad pendientes de aplicar.
- Equipos con software instalado pendiente de actualizar.
- Control de las VPNs instaladas en la organización.
- Unidades de disco no encriptadas.

Beneficios

- Control automático y exhaustivo del estado de ciberseguridad del parque inventariado.
- Identificación clara de los equipos expuestos a diferentes riesgos de seguridad.
- Automatización de la actualización de parches de Windows y del software de terceros instalados.
- Evidencias sobre la mejora del estado de ciberseguridad general del parque.

3. Gestión de Incidentes

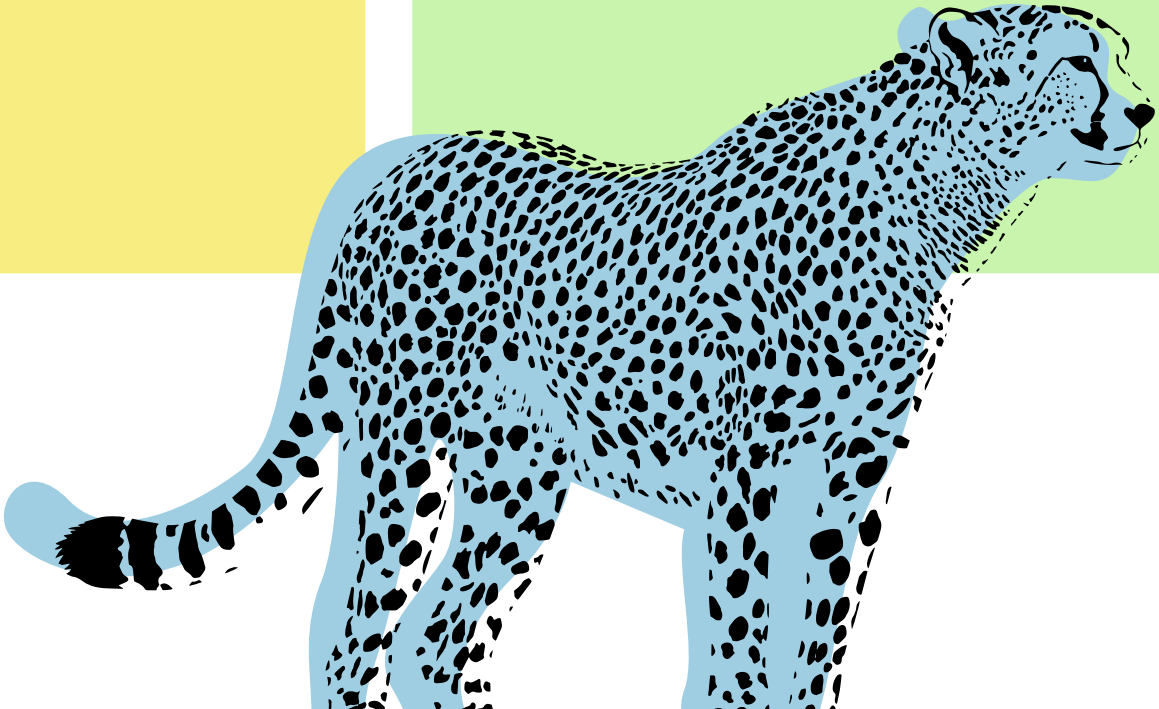
Una respuesta eficaz ante incidentes de seguridad puede marcar la diferencia entre un contratiempo y una crisis.

Acciones Recomendadas

- Tipifica de manera diferente los incidentes de seguridad del resto.
- Prioriza adecuadamente el incidente de seguridad en función del servicio impactado o del personal afectado.
- Establece flujos de trabajo para la respuesta a incidentes y la notificación a las partes interesadas.
- Documenta todos los campos necesarios en la herramienta.

Beneficios

- Respuesta rápida y coordinada ante incidentes de seguridad.
- Registro y seguimiento de los incidentes para análisis y mejora continua.
- Generación de informes y evidencias para auditorías y cumplimiento normativo.



4. Procesos de Autorización y Control de Accesos

La gestión de accesos es un pilar del control interno y del cumplimiento normativo.

Acciones Recomendadas

- Genera diferentes plantillas predefinidas para los procesos requerimientos más frecuentes (compras, accesos, credenciales de autenticación, etc...)
- Genera procesos de autorización diferenciados en función de cada tipo de requerimiento.
- Gestiona los autorizadores suplentes de manera transparente para cada autorizador.
- Crea reglas claras de asignación del proceso de autorización, para que los requerimientos del mismo tipo se trate siempre de la misma manera.
- Automatiza el proceso de solicitud de autorización en función a esas reglas.
- Permite que el usuario que hace el requerimiento tenga visibilidad del estado del proceso de autorización y de las personas que deben autorizarlo.
- Activa las notificaciones a los autorizadores para mejorar el tiempo de autorización de los requerimientos.

Beneficios

- Procesos de autorización más rápidos y transparentes.
- Control de los permisos de acceso y privilegios de los usuarios.
- Evidencia del proceso de entrega y aceptación de credenciales.
- Más alternativas para aprobar los requerimientos usando el Portal de usuarios, la aplicación móvil, el chatbot o la integración con MS Teams.
- Autogestión de los suplentes por cada uno de los autorizadores.

5. Políticas y Normativas de Seguridad

Tener políticas bien documentadas, actualizadas y difundidas es una exigencia en todos los marcos de seguridad.

Acciones Recomendadas

- Utiliza la Base de Conocimiento (KWB) para documentar y publicar la Política de Seguridad de la Información (PSI) y otras normativas internas.
- Organiza estos tópicos con una estructura comprensible y publícalos después a los técnicos y/o a toda la organización en el Portal de Usuarios.
- Activa el modo completo de la KWB de tu herramienta.
- Documenta la fecha de la próxima revisión para recibir notificaciones automáticas de revisión.
- Genera un “borrador” para aplicar los cambios a cada tópico sin necesidad de modificar el publicado.
- Aplica el proceso de revisión y autorización por parte del responsable de cada tópico antes de ponerlo en producción.

Beneficios

- Centralización de la documentación de seguridad.
- Fácil acceso y difusión de las políticas a todos los empleados.
- Registro de revisiones y versiones de los documentos.
- Evidencia de la publicación y aceptación de las normativas.
- Evidencia de la cantidad de consultas y gestión del feedback de los usuarios.

6. Gestión de Proveedores y Contratos

El riesgo también puede venir del exterior. Una adecuada gestión de terceros es esencial.

Acciones Recomendadas

- Da de alta los proveedores y vincularlos a los contratos relacionados e identifica los que son críticos para el negocio.
- Documenta toda la información relevante del proveedor y de los contratos vinculados incluyendo datos financieros y legales.
- Crea campos personalizados adicionales para almacenar información estratégica si fuera necesario.
- Si tienes un contrato general y otros más específicos, vincula el contrato marco y los contratos anexos entre sí.
- Relaciona los servicios que estén externalizados de manera total o parcial con cada contrato y proveedor. Vincula también cada activo con los contratos y proveedores de alquiler, mantenimiento preventivo y correctivo, outsourcing, etc.
- Documenta cada acuerdo de nivel de servicio de cada proveedor para aplicarlo en los tickets relacionados con el proveedor.

Beneficios

- Información más clara al tener centralizada la gestión de proveedores y contratos.
- Atención más rápida de tickets de servicios tercerizados al tener los contactos del proveedor y las condiciones del contrato vinculados a los activos y servicios.
- Evidencia de seguimiento en el cumplimiento de los acuerdos de servicio del proveedor.
- Evidencias de la revisión periódica de los proveedores.

7. Revisión periódica de Contratos y Proveedores

Genera revisiones periódicas de los proveedores y sus contratos de manera automatizada.

Acciones Recomendadas

- Por cada proveedor y/o contrato que haya que revisar, informa de la próxima fecha de revisión.
- Crea una plantilla de creación programada para la revisión anual/semestral de los proveedores estratégicos.
- Genera diferentes actividades dentro de la plantilla o diferentes plantillas para cada tipo de proveedor (estratégico, corporativo, local, etc...)
- Si es posible involucra al proveedor en las reuniones de revisión.
- Documenta en la ficha del proveedor y en la ficha de sus contratos asociados (si aplica) las conclusiones y haz una valoración general poniendo enfasis en la calidad percibida y la ausencia o no de incidencias.
- Relacionar los tickets de peticiones fuera del contrato o incidencias con el proveedor y/o contrato te ayudarán en el futuro a realizar esta valoración.

Beneficios

- Ahorro de tiempo a la hora de revisar el estado de los contratos y proveedores.
- Mejor toma de decisión sobre la continuidad o no de un contrato o proveedor al tener mayor información disponible.
- Previsión ante cambio de proveedor ante una situación de incidencias recurrentes o valoraciones poco positivas.
- Crecimiento de la relación proveedor/cliente debido a las revisiones periódicas.
- Generación de evidencias de revisión de proveedores y contratos.

8. Análisis y Gestión de Riesgos

Identificar, evaluar y mitigar riesgos es una obligación para cualquier entidad bajo marcos como ENS, NIS2 o DORA.

Acciones Recomendadas

- Registra los riesgos, las amenazas y acciones mitigadoras.
- Usa la CMDB para vincular y hacer la valoración de cada uno de los riesgos a los CIs afectados.
- Relaciona cada riesgo con las amenazas y acciones mitigadoras.
- Establece revisiones periódicas para actualizar el análisis de riesgos.

Beneficios

- Identificación y evaluación de los riesgos de seguridad.
- Documentación de las acciones para mitigar los riesgos.
- Visión más clara de la postura de seguridad de la organización.
- Integración con la CMDB y el catálogo de servicios para identificar los riesgos de cada uno de los servicios.

SECURITY BOULEVARD
Home of the Security Bloggers Network

Según Gartner, para 2025, el 45% de las organizaciones a nivel mundial experimentarán un ataque a su cadena de suministro de software, un aumento de tres veces desde 2021. Esto resalta la importancia de implementar prácticas de seguridad avanzadas requeridas por NIS2, incluso para organizaciones que no están obligadas a cumplir con la normativa.

Fuente. Security Boulevard

proactivanet

9. Gestión de Cambios

No hay seguridad sin control del cambio. Cualquier modificación no autorizada puede introducir vulnerabilidades.

Acciones Recomendadas

- Documenta los planes de roll-out y back-out e identifica a los stakeholders, para facilitar la aprobación del comité de cambios.
- Tipifica la naturaleza de los cambios y gestiona con flujos diferentes los cambios preautorizados, estándar y urgentes.
- Planifica cada uno de los pasos a realizar de cada cambio asociando tanto los responsables como el equipo de trabajo.
- Detecta tareas dependientes entre sí para evitar bloqueos en el desarrollo del cambio.

Beneficios

- Documenta los planes de roll-out y back-out e identifica a los stakeholders, para facilitar la aprobación del comité de cambios.
- Tipifica la naturaleza de los cambios y gestiona con flujos diferentes los cambios preautorizados, estándar y urgentes.
- Planifica cada uno de los pasos a realizar de cada cambio asociando tanto los responsables como el equipo de trabajo.
- Detecta tareas dependientes entre sí para evitar bloqueos en el desarrollo del cambio.

10. Capacidad y Disponibilidad

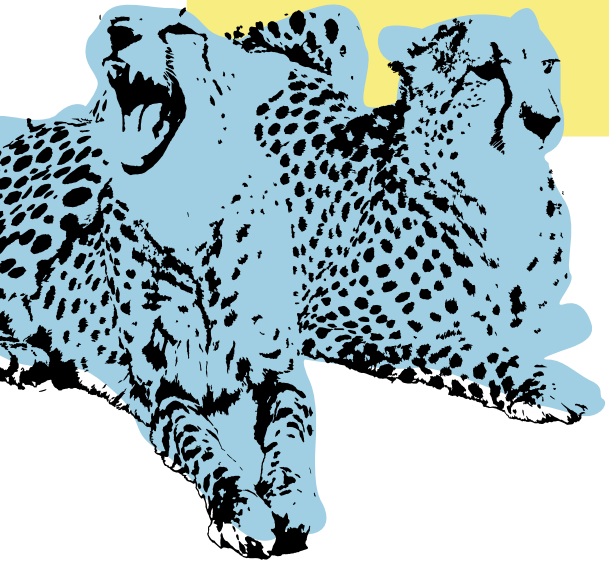
La seguridad también tiene que ver con asegurar la continuidad. Sin capacidad ni disponibilidad, no hay servicio.

Acciones Recomendadas

- Integra cada uno de los planes con cualquier herramienta de monitorización del mercado.
- Integra la creación y cierre automático de tickets cuando se detectan faltas de capacidad y de disponibilidad.
- Analiza mediante la integración con la CMDB el origen de las indisponibilidades o de la falta de capacidad de tus servicios.

Beneficios

- Mejor planificación de los cambios y gestión eficiente de los recursos de TI.
- Mejor toma de decisiones para fortalecer y mejorar la prestación de los servicios mejor informadas.
- Monitorización de la capacidad y la disponibilidad de los sistemas.
- Evidencias de planes de capacidad y disponibilidad y usos de herramientas específicas de monitorización.



11. Formación y Concienciación

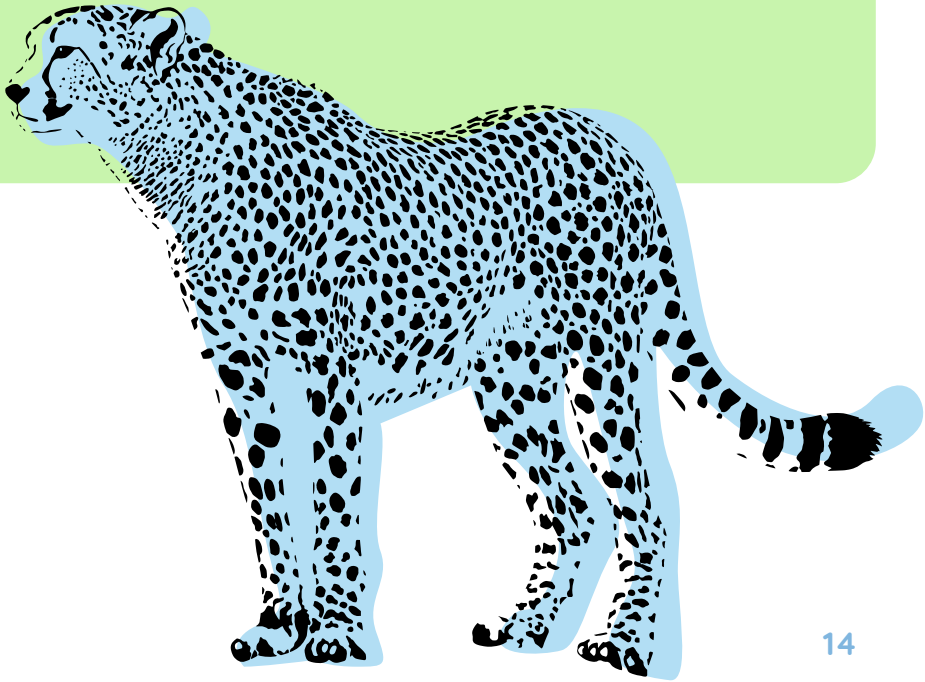
Los empleados son el primer firewall de una organización. Invertir en formación es proteger el negocio.

Acciones Recomendadas

- Crea tópicos públicos en la KWB para documentar noticias o ejemplos de ataques y concienciar a los usuarios del peligro al que se exponen.
- Gestiona el acceso a los tópicos a través de grupos de usuarios.
- Obtén feedback tanto de los técnicos del departamento como de los usuarios finales, sobre la utilidad y el contenido de los tópicos publicados.
- Contabiliza los accesos a los tópicos y obten el “Top 10” de los tópicos más vistos.

Beneficios

- Mejora de la cultura de seguridad en la organización.
- Reducción de errores humanos y riesgos de seguridad.
- Cumplimiento de los requisitos de formación del ENS.



12. Auditoría y Revisión Continua

Revisar para mejorar. La auditoría interna es la base de la mejora continua.

Acciones Recomendadas

- Mantener un registro de los hallazgos y las acciones de mejora.
- Configura plantillas de tickets con creación programada para realizar las revisiones semestrales o anuales necesarias para pasar con éxito cualquier auditoría de seguridad.
- Registra en el ticket los hallazgos encontrados en esa revisión y relaciónalo a un ticket de gestión de cambios para abordar las modificaciones de mejora contínua de la seguridad.

Beneficios

- Identificación de áreas de mejora en la seguridad.
- Seguimiento del cumplimiento de las políticas y procedimientos de seguridad.
- Generación de evidencias de las revisiones y del proceso de mejora contínua.
- Preparación para auditorías externas y certificaciones.

WITH secure

NIS2 no es solo una obligación legal, sino una oportunidad estratégica para fortalecer la gestión de riesgos y la resiliencia organizacional. Destacan que NIS2 proporciona un marco para una gestión adecuada de riesgos, permitiendo expandir los esfuerzos de seguridad en toda la organización, ya que la seguridad es más que una preocupación de TI: es crítica para el negocio.

Fuente: WithSecure Consulting

proactivanet

13. Evidencias y Documentación

Sin evidencias no hay cumplimiento. Documentar es tan importante como actuar.

Acciones Recomendadas

- Generar informes automáticos de acciones clave.
- Conservar registros de autorizaciones, accesos y revisiones.
- Centralizar toda la documentación relevante.

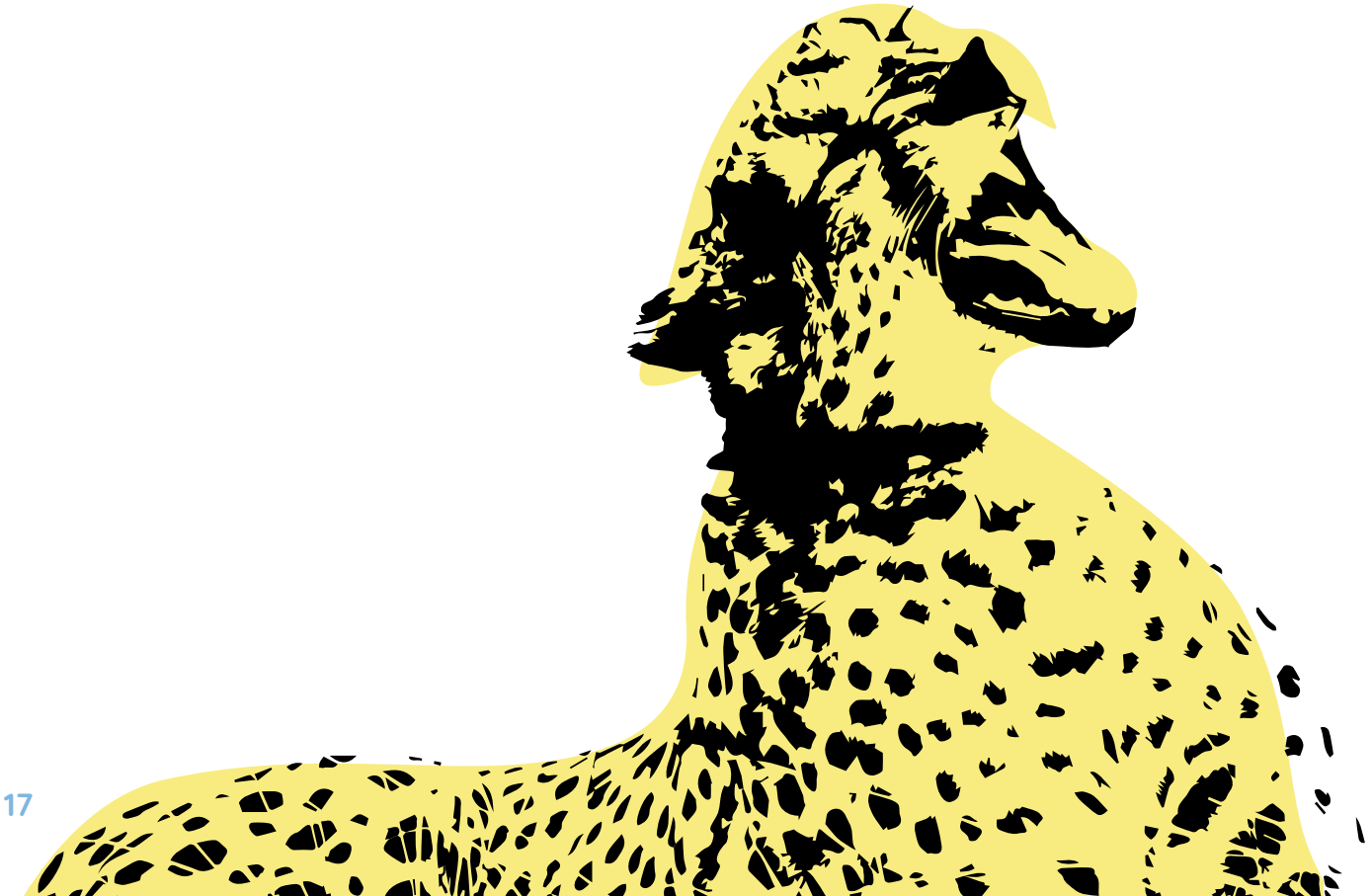
Beneficios

- Cumplimiento demostrable.
- Facilidad para afrontar auditorías.
- Confianza institucional y reputacional.

CONCLUSIÓN

Avanzar hacia el cumplimiento de marcos de seguridad como ENS, NIS2 o DORA no requiere comenzar desde cero, sino entender dónde está la organización y aplicar acciones graduales, efectivas y documentadas. Esta guía ofrece una base práctica para construir una estrategia de ciberseguridad robusta, adaptable y auditable.

Cumplir no es solo evitar sanciones: es proteger lo que más importa.



proactivanet

WHITEPAPER: Acciones Rápidas para Cumplir con Marcos de Seguridad

En este documento se presentan 13 acciones concretas para facilitar el cumplimiento de marcos normativos como ENS, NIS2 o DORA. El objetivo es ofrecer una hoja de ruta práctica para mejorar la postura de ciberseguridad de cualquier organización.

Control / Acción	Acciones Recomendadas	Beneficios
Gestión de Activos e Inventario	• Registrar y clasificar todos los activos tecnológicos. • Eliminar Shadow IT. • Asignar responsables.	• Visibilidad total de la infraestructura. • Facilitación de auditorías. • Identificación de riesgos.
Supervisión del Estado de Seguridad	• Monitorear antivirus, firewall, parches pendientes, software desactualizado, configuraciones inseguras.	• Detección temprana de brechas. • Evidencias automáticas. • Reducción de superficie de ataque.
Gestión de Incidentes	• Clasificar incidentes, establecer flujos de respuesta y documentar todo el proceso.	• Agilidad de respuesta. • Trazabilidad. • Cumplimiento de normativas.
Control de Accesos y Autorizaciones	• Automatizar flujos de aprobación. Controlar accesos privilegiados y temporales.	• Prevención de accesos indebidos. • Evidencias claras. • Reducción del error humano.
Políticas y Normativas de Seguridad	• Publicar, versionar y revisar periódicamente las políticas de seguridad.	• Mayor alineación interna. • Base sólida para auditorías. • Cultura de cumplimiento.
Gestión de Proveedores y Contratos	• Clasificar proveedores. • Relacionar contratos con activos y servicios. • Evaluar desempeño.	• Reducción de riesgos externos. • Mejores decisiones sobre continuidad. • Control legal y operativo.
Revisión de Contratos	• Establecer revisiones periódicas. • Documentar hallazgos y decisiones.	• Optimización de contratos. • Prevención de incumplimientos. • Relación más sólida.
Análisis y Gestión de Riesgos	• Registrar amenazas. • Asociar medidas de mitigación. • Revisar periódicamente.	• Visión clara de riesgos. • Priorización efectiva. • Alineación con objetivos de seguridad.
Gestión de Cambios	• Documentar cambios. • Planificar despliegues y retrocesos. • Diferenciar tipos de cambios.	• Estabilidad operativa. • Menos errores. • Cumplimiento documental.
Capacidad y Disponibilidad	• Estudiar consumo. • Planificar ampliaciones. • Analizar causas raíz de fallos.	• Reducción de interrupciones. • Mejora en decisiones. • Cumplimiento de SLAs.
Formación y Concienciación	• Difundir contenidos educativos. • Medir comprensión. • Repetir campañas periódicas.	• Menor exposición a riesgos. • Cultura organizacional segura.
Auditoría y Revisión Continua	• Planificar auditorías. • Documentar hallazgos. • Ejecutar planes de acción.	• Preparación para certificaciones. • Mejora continua. • Evidencias disponibles.
Evidencias y Documentación	• Generar informes. • Centralizar registros de acciones clave.	• Cumplimiento demostrable. • Facilidad en auditorías. • Confianza institucional.

Gartner
Peer Insights
Customers' Choice 2024

SPRING 2025
Momentum Leader

SPRING 2025 LATIN AMERICA
High Performer

SPRING 2025
Best Meets Requirements
ENTERPRISE

¿Quieres saber más?
Potencia y moderniza
tu organización

proactivanet.com

Gartner®
THE GARTNER MARKET GUIDE FOR
ITSM PLATFORMS 2024 & 2025

PinkVERIFY® Certified
16 PROCESSES

PinkVERIFY es una marca registrada por Pink Elephant.

ITIL®
PRACTICES 15
ACCREDITED TOOL VENDOR
Proactivanet v10
Bronze
by PeopleCert