UN RETO GESTIÓN DE TICS

Gestionando la ciberseguridad, una cuestión de madurez

El concepto de Ciberseguridad está escalando rápidamente posiciones en la lista de prioridades de las empresas, y existen **dos factores fundamentales** que están liderando este cambio. Por un lado, el crecimiento exponencial del **cibercrimen**, entendido como una industria altamente lucrativa y que supone una amenaza de alcance global para el conjunto del tejido empresarial. Por otro lado, la creciente **presión regulatoria** a nivel sectorial, nacional y europeo que obliga a tomar medidas que evidencien una actitud diligente frente a estas amenazas.

La manera en la que las organizaciones gestionan la Ciberseguridad depende en gran medida de su nivel de madurez, que determina la forma de enfocar el problema.

Enfoque tecnológico

La Ciberseguridad se entiende como un problema de tecnología, la gestión se centra en la implantación de controles técnicos para la protección de las infraestructuras IT, y la responsabilidad se delega en las áreas técnicas.

Enfoque regulatorio

Se entiende como una obligación que hay que cumplir para evitar sanciones o limitaciones a la hora de desarrollar negocio, se centra en evidenciar la conformidad con los requisitos de la norma de turno (NIS2, CRA, ENS, GDPR...), y la responsabilidad queda en las áreas de cumplimiento.

Enfoque estratégico

La Ciberseguridad se entiende como un proceso de gestión integral de los riesgos orientada al negocio, se centra en priorizar los recursos para mitigar aquellos riesgos que supongan un mayor impacto, y la responsabilidad recae en la alta dirección.

Es fundamental que cada empresa entienda cuál es su **nivel de madurez** y defina una hoja de ruta con un plan personalizado de mejora. Del mismo modo, es vital establecer un entorno de confianza y colaboración donde los equipos directivos de las organizaciones puedan compartir sus inquietudes, experiencias y estrategias.

Desde este **entendimiento estratégico** del concepto de Ciberseguridad que el Gobierno Foral, a través del Departamento de Universidad, Innovación y Transformación Digital, ha impulsado la creación del **Navarra Cybersecurity Center** como centro de referencia en Navarra en esta materia.

Juan Ramón Aramendía
Coordinador del Navarra Cibersecurity Center

TESTIMONIOS DE NUESTRAS EMPRESAS

Gorka Hernández - Responsable IT de Industrial Barranquesa

"Es interesante ver cómo otras empresas abordan el reto de la ciberseguridad. Tenemos mucho que aprender de normativa"

Aún existe un amplio margen de mejora en la implementación de marcos de cumplimiento, la gestión de riesgos y la respuesta ante incidentes. Analizar buenas prácticas en sectores regulados puede contribuir al fortalecimiento de las políticas internas y a una mejor preparación frente a futuras exigencias legales y tecnológicas.

Raúl Otazu - Information Technology Administrator de ZF Group

"En ciberseguridad la información es clave. Es importante hacer un autoanálisis de la empresa desde una visión externa"

En un entorno volátil, ambiguo e incierto el desarrollo de competencias debe ser una prioridad para cualquier empresa que busque mejorar su capacidad y competitividad en el mercado. Es esencial proporcionar a tus empleados de la capacitación necesaria para mejorar sus habilidades y conocimientos. Es por ello que la implantación de estrategias adecuadas que fomenten el aprendizaje y la mejora continua es fundamental en nuestra empresa.

Adrián Miguel - Responsable de IT de Atecna

"La responsabilidad ya no es solo de IT, sino de todos los empleados. El CIO debe estudiar el reglamento y no aislarse en lo tecnológico"

La figura del CIO siempre ha sido una figura aislada en la "cueva de IT". Esta imagen parecía inamovible en el imaginario colectivo, pero, hoy es un perfil estratégico. El CIO gestiona la información de la empresa en su conjunto y es el encargado de estudiar el reglamento para asegurar su cumplimiento. Además, colabora estrechamente con el CISO para proteger los datos y garantizar su integridad. Por ello, debe liderar, formar y acompañar a las distintas áreas de negocio para que todos se sientan completamente comprometidos con la información y la concienciación en materia de seguridad.

MESA DE GESTIÓN DE TICS | JUNIO 2025

CIBERSEGURIDAD EN LA ERA DE LA IA

La interrelación entre la inteligencia artificial y la ciberseguridad puede entenderse desde **tres grandes perspectivas.**

En primer lugar, como **motor de evolución tecnológica**: la IA está transformando el desarrollo de herramientas de seguridad, permitiendo la detección proactiva de amenazas, la automatización de respuestas y la reducción de los tiempos de reacción. Su **integración con plataformas** de monitorización y el análisis predictivo facilitan la identificación de comportamientos anómalos y vectores de ataque con mayor precisión.

En segundo lugar, como **herramienta al servicio del cibercrimen**. La IA ha sofisticado técnicas como el phishing, generando mensajes más creíbles y dirigidos, difíciles de detectar para los sistemas de seguridad tradicionales. Además, el uso de deepfakes o vishing ha incrementado notablemente el **riesgo de fraude** dentro de las organizaciones, incluso entre usuarios entrenados.

Y en tercer lugar, como **tecnología vulnerable** en sí misma. Modelos de IA pueden ser manipulados mediante **data poisoning o ataques adversariales,** permitiendo accesos indebidos o respuestas erróneas. La opacidad de ciertos sistemas —dificultad para auditar cómo toman decisiones— añade un desafío adicional en contextos críticos.

Junto a estos desafíos técnicos, las empresas deben afrontar un marco normativo en expansión. La **Directiva NIS2 de la Unión Europea** amplía los sectores afectados, impone nuevas obligaciones y atribuye responsabilidad directa a la alta dirección. Por su parte, el **Reglamento de Ciberresiliencia (CRA)** establece medidas obligatorias de ciberseguridad para productos con componentes digitales, desde su diseño hasta su ciclo de vida completo. La necesidad de **garantizar productos más seguros y actualizados** se convierte, por tanto, en una prioridad tanto para los fabricantes como para los consumidores.

¿Te ha interesado este tema?

"Existen dos tipos de empresa: las que han sufrido un ciberataque y las que lo sufrirán en algún momento".

Formación online en Ciberseguridad

Objetivo: ayudar a las empresas a identificar, prevenir y defender sus sistemas frente a las amenazas. Formación técnica y práctica con herramientas reales. Refuerza tu conocimiento sobre protocolos de redes industriales como paso previo a su correcta protección.

CLAVES DE NUESTRA MESA

¿Cómo gestionar la ciberseguridad en la era de la IA? Estrategias para una protección integral

1

Ciberseguridad como prioridad estratégica

El aumento del cibercrimen y la presión regulatoria han colocado a la ciberseguridad en el centro de las prioridades empresariales. Las organizaciones deben adaptarse rápidamente para evitar ser víctimas de ataques globales.

Tres enfoques de gestión de ciberseguridad

Las empresas abordan la ciberseguridad desde tres perspectivas: tecnológica, regulatoria y estratégica. Definir el enfoque adecuado es clave para gestionar los riesgos y asegurar la protección de las infraestructuras críticas.

2

3

La alta dirección en la gestión de riesgos

La responsabilidad de la ciberseguridad debe recaer en la alta dirección, alineando la seguridad con los objetivos de negocio. Los órganos de dirección de las empresas tendrán responsabilidad directa en la protección, asegurando que los recursos se asignen para mitigar los riesgos más críticos.

NIS2: nuevas obligaciones regulatorias

La Directiva NIS2 impone nuevas responsabilidades a las empresas en términos de ciberseguridad, ampliando su ámbito y exigiendo un cumplimiento más estricto. Las organizaciones deben adaptar sus procesos a estas normativas para evitar sanciones.

4