ACELERACIÓN EXPRÉS PARA EMPRESAS

Cómo Fortalecer tu Seguridad Digital en 20 Horas

INSTITUTO INTERNACIONAL DE
INTRAEMPRENDIMIENTO
Emprendiendo dentro de las organizaciones

Introducción:

Lo que debes saber para proteger tu EMPRESA en un entorno cada vez más digitalizado, las ciberamenazas avanzan con rapidez. Ataques como ransomware, phishing o brechas de datos ya no son un problema exclusivo de grandes compañías: afectan también a pymes de 3 a 50 empleados.

Proteger tu negocio ante estos riesgos es clave para garantizar la continuidad de tus operaciones y salvaguardar la confianza de tus clientes.

Tabla de Contenidos

INSTITUTO INTERNACIONAL DE INTRAEMPRENDIMIENTO
Emprendiendo dentro de las organizaciones

01 Diagnóstico de Madurez en Ciberseguridad

Antes de reforzar tu defensa, necesitas evaluar con precisión en qué punto te encuentras. Este diagnóstico te permitirá:

- Conocer tu nivel real de protección.
- Priorizar las acciones de alto impacto.
- Planificar recursos y plazos de forma eficiente.

El modelo de Madurez NIST CSF El NIST Cybersecurity Framework (CSF) organiza la seguridad en cinco funciones clave:

Identificar: Conocer y gestionar tus activos, datos, personas y riesgos.

Proteger: Implementar salvaguardas para limitar el impacto de un evento.

Detectar: Definir procesos y sistemas que alerten de actividades anómalas.

Responder: Establecer procedimientos para contener y mitigar un incidente.

Recuperar: Asegurar la restauración ágil de sistemas y datos tras un suceso.

Niveles de madurez

Inicial: no hay procesos definidos.
Parcial: acciones aisladas sin coherencia.
Definido: existe un procedimiento documentado.
Gestionado: se mide su eficacia y se revisa periódicamente.
Optimizado: mejora continua e integración con el negocio.

Checklist Avanzado con Ejemplos de Evidencias Identificar:

- Inventario actualizado de hardware y software.
- Mapa de flujos de datos internos y externos.
- Políticas de seguridad aprobadas por dirección.
- Roles y responsabilidades documentados
- Evaluación de riesgos periódica.

Proteger

- Políticas de contraseñas y 2FA habilitadas.
- Cortafuegos y segmentación de red.
- Copias de seguridad automáticas y cifradas.
- Control de accesos por mínimos privilegios.
- Sistemas y aplicaciones actualizados.

Detectar

- Sistema de logging centralizado.
- Alertas por accesos anómalos.
- Revisión diaria de registros.
- Scan de vulnerabilidades mensual.
- Antivirus empresarial en endpoints.

Responder

- Plan de respuesta a incidentes documentado.
- Roles y equipo definidos para crisis.
- Comunicación interna y externa.
- Simulacros anuales.
- Informe post-incidente.

Recuperar

- Procedimiento de restauración probado.
- SLA de recuperación.
- Plan de continuidad mínima.
- Revisión tras simulacro.
- Soporte externo especializado.

Ejercicio Práctico: Autoevaluación y Prioridades

Paso	Acción	Detalles
1	Suma tu puntuación	Asigna 1 punto por cada ✓ marcado (puntuación máxima: 25).
2	Interpreta tu nivel	0–5: Crítico (Actúa ya) 6–12: Básico (Refuerza áreas clave) 13–19: Intermedio (Optimiza procesos) 20–25: Avanzado (Consolida)
3	Prioriza tus acciones	Ordena las funciones (Identificar, Proteger, Detectar, Responder, Recuperar) de menor a mayor puntuación y enfoca primero allí.

02 Plan de Acción Basado en NIST & ISO

Utiliza los controles de ISO 27001 y NIST CSF para traducir el diagnóstico en acciones:

Control de accesos (ISO A.9 / NIST PR.AC)

- Políticas de contraseñas robustas y caducidad.
- Gestión de identidades y accesos (IAM).
- Revisión trimestral de usuarios y privilegios.

Criptografía (ISO A.10 / NIST PR.DS)

- Cifrado de datos en reposo y tránsito (TLS, AES-256).
- Gestión y rotación de claves.
- Verificación de cifrado en backups.

Copias de seguridad y recuperación (ISO A.12.3 / NIST PR.DS-5, RC.RP)

- Copias diarias de datos críticos, semanales del resto.
- Almacenamiento on-premise y en la nube.
- Pruebas de restauración trimestrales.

Monitorización y logging (ISO A.12.4 / NIST DE.CM-1)

- Centralización de logs con SIEM.
- Alertas por fallos de acceso y cambios sensibles.
- Revisión diaria y escalado inmediato.

Respuesta a incidentes (ISO A.16 / NIST RS.RP-1)

- Plan documentado con roles y flujos de comuni[illegible]ión.
- Simulacros semestrales.
- Ajustes basados en lecciones aprendidas.

Cumplimiento normativo (RGPD & NIS2)

- Registro de tratamientos de datos personales.
- DPIAs para procesos críticos.
- Verificación de conformidad de proveedores.

Plantilla de Plan de Acción

01

Políticas de contraseña

- Responsable: Responsable TI
- Plazo: 2 semanas
- Estado: Pendiente
- Métrica de éxito: 100 % de usuarios actualizados

02

Cifrado backups

- Responsable: Proveedor nube
- Plazo: 1 mes
- Estado: En curso
- Métrica de éxito: 3 backups diarios verificados

03

SIEM básico

- Responsable: Equipo Seguridad
- Plazo: 1 mes
- Estado: Pendiente
- Métrica de éxito: Alertas configuradas y probadas

04

Simulacro incidente

- Responsable: Dirección
- Plazo: 3 meses
- Estado: Pendiente
- Métrica de éxito: Incidentes contenidos en < 2 h

03 Implementación Rápida de Controles Críticos

En este bloque de trabajo intensivo desplegamos, en 20 horas, las defensas esenciales para tu empresa:

- **Arquitectura mínima viable:** Instalamos y configuramos cortafuegos perimetral, segmentación de red, VPN para accesos remotos y antivirus corporativo en todos los endpoints.

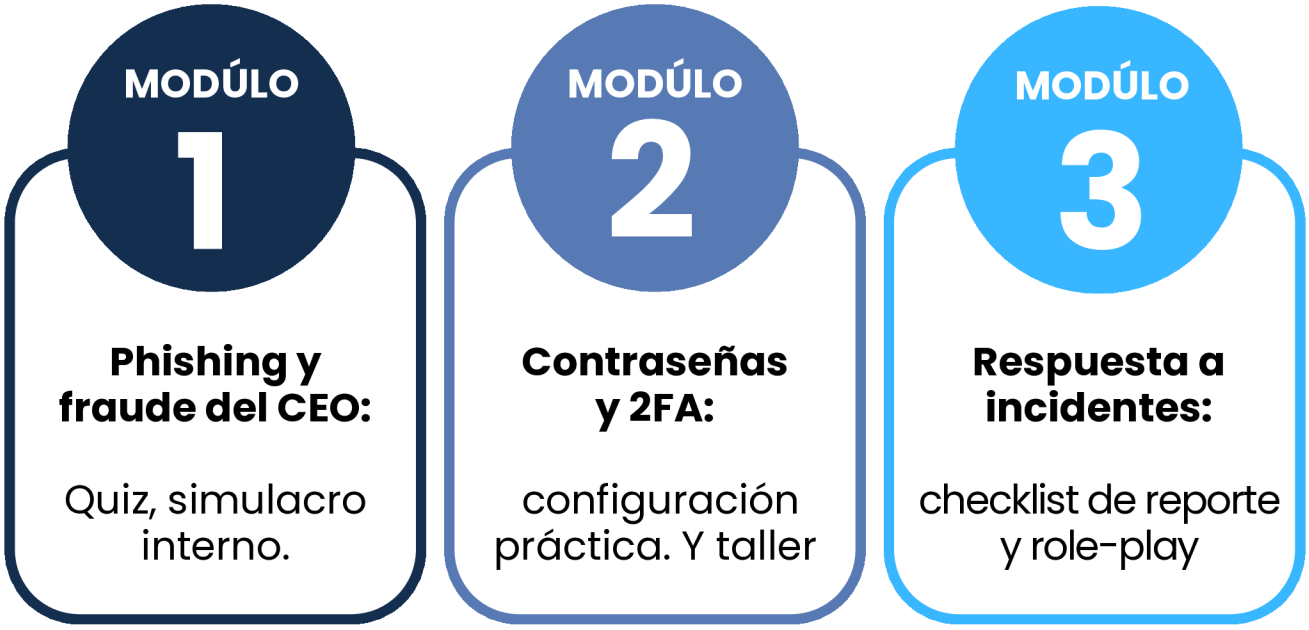
- **Backups y cifrado:** Desplegamos scripts preconfigurados que realizan copias de seguridad automáticas y cifradas, con mecanismos de verificación de integridad para asegurar que los datos se están guardando correctamente.

- **Dashboard de monitorización:** Configuramos un SIEM ligero con cinco alertas clave (intentos de acceso fallidos, cambios en carpetas sensibles, elevación de privilegios, etc.) y un panel web intuitivo para visualizar el estado de cada área crítica en tiempo real.

- **Pruebas de funcionamiento:** Ejecutamos una simulación interna de ataque y validamos la restauración de datos desde los backups, ajustando procedimientos según los resultados obtenidos.

04

Formación Concienciación Efectiva



Módulo 1: Phishing y fraude del CEO

- **Objetivo clave:** Sensibilizar ante correos y peticiones falsas, reduciendo el riesgo de engaño.
- **¿Qué vas a lograr?**

  Detectar +85 % de intentos de phishing reales.

  Conocer las tácticas de ingeniería social más usadas.
- **Argumento de impacto:** El 92 % de los incidentes corporativos arrancan con un clic imprudente → un pequeño descuido puede costarte miles.

Módulo 2: Contraseñas y 2FA

- **Objetivo clave:** Fortalecer el acceso a tus sistemas con políticas sólidas y verificación adicional.

- **¿Qué vas a lograr?**

  Implantar un gestor de contraseñas corporativo con adopción > 90 %.

  Reducir los accesos no autorizados en un 70 % gracias al segundo factor.

- **Argumento de impacto:** El 80 % de las brechas se deben a credenciales débiles o reutilizadas.

Módulo 3: Respuesta a incidentes

- **Objetivo clave:** Definir una reacción rápida y coordinada para contener cualquier ataque.

- **¿Qué vas a lograr?**

  Tener un plan de comunicación interno listo en < 2 h tras el incidente.

  Ensayar el proceso y reducir el tiempo medio de contención a < 30 min.

- **Argumento de impacto:** Cada minuto sin respuesta puede generar hasta 1000 € en costes de remediación y pérdida de negocio.

05 Plan Para Blindar la Ciberseguridad de tu Empresa

Concepto y alcance

- La ISO 27032 extiende la ciberseguridad a todo el “ciberespacio”: no solo sistemas internos, sino también Internet, partners, proveedores y usuarios finales.

Ecosistema del ciberespacio

- Activos: datos, infraestructuras, servicios en la nube.
- Actores: usuarios, desarrolladores, proveedores, organismos CERT/CSIRT.

Roles y responsabilidades

- CISO / Responsable de seguridad: diseño y supervisión del Plan Director.
- Analistas de seguridad: identificación de amenazas y vulnerabilidades.
- Equipos de TI: implementación técnica de controles.
- Comunicación: interacción con CERTs, proveedores y organismos reguladores.

Comunicación y coordinación

- Marco para compartir incidentes y alertas con CERT nacionales e internacionales.
- Protocolos de intercambio de inteligencia de amenazas y buenas prácticas.

Diseño y ejecución del Plan Director

- Pasos clave: diagnóstico estratégico → definición de objetivos → selección de controles (ISO 27032, ISO 27001, NIST) → implementación → monitorización → mejora continua.
- Simulaciones de ataque y defensa incorporadas en cada fase.

Certificación y evaluación de competencias

- Requisitos: aprobar examen teórico en cada módulo, presentar un Plan Director aplicado a un caso real y superar la evaluación práctica.
- Competencias acreditadas: gestión de riesgos, respuesta a incidentes, cumplimiento normativo y uso de IA en ciberdefensa.

06 Conclusión: El Imperativo de la Ciberseguridad Exprés para tu Empresa

En un entorno cada vez más digital, cada minuto sin protección expone tu empresa a pérdidas económicas, interrupciones y daños reputacionales. Tener un antivirus ya no basta: necesitas un plan urgente, preciso y alineado con estándares internacionales.

La Aceleración Exprés es más que un lema: es tu hoja de ruta práctica. Aquí has aprendido a evaluar tu madurez en ciberseguridad, definir un plan de acción inmediato, desplegar controles esenciales y formar a tu equipo para actuar como primera línea de defensa. Todo bajo el paraguas de NIST, ISO 27001 e ISO 27032, y reforzado con casos reales de éxito.

Pero la guía es solo el punto de partida. Nuestro equipo de consultores certificados convierte la teoría en resultados tangibles: desde el diseño de tu **Plan Director de Ciberseguridad** hasta la implementación de arquitecturas robustas y la monitorización 24/7.

Invertir en una Aceleración Exprés no solo te protege, sino que fortalece tu ventaja competitiva y la confianza de tus clientes. Contáctanos y en tan solo 20 horas transformaremos tu seguridad digital en un activo estratégico.

07 Anexos
Recursos y Apoyos Esenciales

1. Guías y Marcos

- INCIBE Emprende: Guías y herramientas gratuitas para pymes.
- NIST CSF: Estructura tus defensas en 5 fases probadas.
- ENISA Threat Landscape: Informe europeo de amenazas emergentes.

2. Subvenciones Clave

- AceleraPyme (INCIBE): Diagnóstico y asesoría 100 % subvencionados.
- Kit Digital – Ciberseguridad: Bono de hasta 12 000 € para soluciones de protección.
- NextGenerationEU: Fondos para transformación y resiliencia digital.

3. Certificaciones Top

- ISO 27001 Lead Implementer: Gestiona tu Sistema de Seguridad de la Información.
- CISSP: Lidera la estrategia de seguridad global.
- GSEC: Valida habilidades prácticas en ataques y defensas.

Combina estas guías, ayudas y certificaciones para convertir tu Aceleración Exprés en un activo estratégico y mantener tu empresa siempre un paso adelante.

INSTITUTO INTERNACIONAL DE
INTRAEMPRENDIMIENTO
Emprendiendo dentro de las organizaciones

www.institutodeintraemprendimiento.es