Contexto:

Pequeña empresa de unos 20 empleados que desarrolla y aloja **aplicaciones de gestión de inventario** para clientes empresariales en la nube.
Cuenta con un pequeño equipo de desarrollo, un administrador de sistemas y un responsable de soporte técnico. Los servidores están alojados en un proveedor cloud y los empleados trabajan en modo híbrido (oficina y remoto).

🏛️ **Función: Gobernar**

Se asegura de que la estrategia y las normas de ciberseguridad se establezcan, comuniquen y supervisen adecuadamente.

GV.RM-02:

Se establecen, comunican y mantienen las declaraciones sobre el apetito y la tolerancia al riesgo.

Ejemplo:
La empresa define que **no puede asumir más de 1 hora de caída del servicio** sin afectar a los clientes, ni perder más de 1 día de datos por una posible corrupción de base de datos.

Comprobación:
Verificar si existe un documento o correo interno que especifique los tiempos máximos de inactividad aceptables (RTO y RPO).
Implementación:
Si no existe, el responsable técnico elaborará una breve matriz de riesgos con tres niveles (bajo, medio, alto) y la presentará a la dirección para su aprobación formal.

GV.RR-02:

Se establecen y comunican las responsabilidades y autoridades en la gestión del riesgo cibernético.

Ejemplo:
El responsable de soporte se encargará de las alertas de seguridad; el desarrollador líder será responsable de revisar vulnerabilidades del código antes de subir nuevas versiones.

Comprobación:
Pedir a tres miembros del equipo que indiquen quién es el encargado de revisar actualizaciones o responder ante incidentes.
Implementación:
Crear un **organigrama digital** en la intranet con las funciones clave y difundirlo por correo a todo el personal.

GV.PO-01:

Se establece y comunica la política de gestión de riesgos de ciberseguridad.

Ejemplo:
La empresa establece una política que exige **actualizar el sistema operativo y dependencias de software cada mes**, y que prohíbe usar cuentas personales para tareas de trabajo.

Comprobación:
Revisar si existe un documento de políticas actualizado y si todos los empleados lo conocen.
Implementación:
Redactar un documento breve en formato PDF con las políticas más básicas (actualizaciones, contraseñas, acceso remoto) y hacerlo firmar digitalmente a los empleados.

GV.SC-04:

Los proveedores son conocidos y priorizados según su criticidad.

Ejemplo:
El proveedor de servicios en la nube y el proveedor de correo corporativo son críticos; el proveedor de marketing no lo es.

Comprobación:
Ver si la empresa dispone de una lista actualizada de proveedores con un nivel de criticidad definido.
Implementación:
Crear una tabla sencilla en Excel con tres columnas: *Proveedor – Servicio – Nivel de criticidad (Alto/Medio/Bajo)* y mantenerla revisada trimestralmente.

🧭 Función: Identificar

Se centra en conocer los activos, vulnerabilidades y amenazas que afectan a la organización.

ID.AM-01:

Se mantienen inventarios del hardware gestionado por la organización.

Ejemplo:
Registrar los portátiles, monitores y dispositivos móviles usados por los empleados, incluyendo los que se llevan a casa en modo teletrabajo.

Comprobación:
Comparar la lista del inventario con los equipos que aparecen conectados en la red Wi-Fi de la oficina.
Implementación:
Implementar un pequeño sistema de inventario con etiquetas QR en cada dispositivo que registre modelo, usuario y ubicación.

ID.RA-01:

Se identifican y registran las vulnerabilidades de los activos.

Ejemplo:
Realizar un **análisis mensual con una herramienta como OpenVAS** o Nessus para detectar vulnerabilidades del servidor web y de las librerías del backend.

Comprobación:
Revisar si existen reportes recientes de escaneo de vulnerabilidades.
Implementación:
Programar un escaneo automático cada mes y guardar los informes en un repositorio interno para su revisión por el responsable técnico.

ID.AM-05:

Se priorizan los activos según su criticidad e impacto.

Ejemplo:
El servidor de base de datos del cliente tiene prioridad máxima; los servidores de pruebas tienen prioridad baja.

Comprobación:
Ver si los activos críticos están documentados y protegidos con medidas adicionales (por ejemplo, acceso restringido).
Implementación:
Crear una hoja de clasificación de activos con niveles de criticidad (1 a 3) y aplicar mayor protección al nivel 1.

ID.RA-03:

Se identifican y registran amenazas internas y externas.

Ejemplo:
Amenazas externas: intentos de ataque a la API desde direcciones desconocidas.
Amenazas internas: un empleado podría subir código sin revisión o extraer datos sin permiso.

Comprobación:
Revisar si existen registros de incidentes previos o listas de amenazas evaluadas.
Implementación:
Celebrar una reunión trimestral de 15 minutos para actualizar la lista de amenazas según las últimas tendencias de seguridad y la experiencia reciente.

🔒 **Función: Proteger**

Incluye las medidas preventivas para evitar o reducir los impactos de ciberincidentes.

PR.AA-03:

Los usuarios y servicios están autenticados.

Ejemplo:
Todo acceso al panel de administración requiere **autenticación multifactor (MFA)** y contraseñas de al menos 14 caracteres.

Comprobación:
Intentar acceder con solo usuario y contraseña. Si es posible, la MFA no está correctamente configurada.
Implementación:
Configurar la MFA en todos los sistemas críticos y obligar su uso mediante políticas del proveedor cloud.

PR.DS-11:

Se crean y prueban las copias de seguridad.

Ejemplo:
Las copias de seguridad automáticas diarias se almacenan en una región diferente del proveedor cloud.

Comprobación:
Probar la restauración en un entorno de pruebas una vez al mes.
Implementación:
Crear una tarea planificada para restaurar un archivo aleatorio y verificar su integridad, dejando registro de cada prueba.

PR.AT-01:

El personal recibe capacitación en seguridad.

Ejemplo:
Organizar talleres breves sobre **cómo detectar enlaces sospechosos** en correos y mensajes corporativos.

Comprobación:
Consultar el registro de formaciones impartidas o preguntar al personal si recuerdan el último curso recibido.
Implementación:
Enviar un pequeño test online cada trimestre para evaluar conocimientos básicos de ciberseguridad.

PR.DS-01:

Se protege la confidencialidad e integridad de los datos en reposo.

Ejemplo:
Las bases de datos están cifradas con claves gestionadas por el proveedor cloud, y los accesos son auditados.

Comprobación:
Revisar en la consola del proveedor si el cifrado está activado.
Implementación:
Habilitar el cifrado de disco completo y rotar las claves cada seis meses.

🦹 **Función: Detectar**

Permite descubrir y analizar incidentes y comportamientos anómalos.

DE.CM-01:

Se monitorean redes y servicios para detectar anomalías.

Ejemplo:
Activar un sistema de alertas que avise si hay **tráfico saliente inusual o múltiples intentos de inicio de sesión fallidos.**

Comprobación:
Revisar si hay registros de alertas o si el monitoreo se limita a comprobar disponibilidad.
Implementación:
Configurar alertas automáticas por correo y panel visual de tráfico en la herramienta de supervisión (como Zabbix o Grafana).

DE.CM-03:

Se monitorea la actividad del personal y uso de la tecnología.

Ejemplo:
Registrar y auditar cada cambio en el código fuente y cada acceso a la base de datos del cliente.

Comprobación:
Ver si el sistema de control de versiones (GitLab, GitHub) tiene habilitado el registro de auditoría.
Implementación:

Configurar alertas que notifiquen accesos a ramas protegidas o descargas masivas de datos.

DE.AE-03:

Se correlaciona la información de diversas fuentes.

Ejemplo:
Combinar registros del firewall, la nube y el sistema de correo para detectar ataques coordinados.

Comprobación:
Revisar si se analizan logs de diferentes sistemas cuando ocurre una alerta.
Implementación:
Crear un procedimiento que obligue a revisar al menos tres fuentes de registros ante cada incidente.

DE.AE-07:

Se integra la inteligencia de amenazas en el análisis.

Ejemplo:
Suscribirse a fuentes de inteligencia de seguridad (como US-CERT o INCIBE) para estar al día de nuevas vulnerabilidades.

Comprobación:
Ver si los correos con avisos de seguridad se revisan y aplican.
Implementación:
Designar un responsable para revisar semanalmente los boletines y actualizar medidas si se detecta una amenaza relevante.

🚨 **Función: Responder**

Acciones que se toman tras detectar un incidente.

RS.MA-01:

Se ejecuta el plan de respuesta a incidentes.

Ejemplo:
Cuando se detecta actividad sospechosa, el procedimiento establece contactar con el proveedor cloud, aislar el servidor y analizar el incidente.

Comprobación:
Preguntar si se ha hecho alguna simulación o práctica reciente del plan.
Implementación:
Hacer un simulacro trimestral de incidente (por ejemplo, caída del servidor) para comprobar tiempos de respuesta.

RS.MI-01:

Se contienen los incidentes.

Ejemplo:
Si una cuenta es comprometida, se bloquea inmediatamente el acceso y se fuerza el cambio de credenciales de todos los usuarios con permisos similares.

Comprobación:
Ver si el equipo conoce el procedimiento de contención.
Implementación:
Configurar reglas automáticas que bloqueen cuentas ante múltiples intentos fallidos o actividad inusual.

RS.AN-03:

Se analizan las causas de los incidentes.

Ejemplo:
Tras un ataque por fuerza bruta, se identifica que el fallo fue causado por contraseñas débiles y falta de bloqueo temporal.

Comprobación:
Ver si los informes de incidentes incluyen análisis de causa raíz.
Implementación:
Usar una plantilla obligatoria que documente qué ocurrió, por qué, y qué se hará para evitar que se repita.

RS.CO-02:

Se notifican los incidentes a las partes interesadas.

Ejemplo:
Si un servicio del cliente se interrumpe, se envía un correo de aviso explicando el impacto y el tiempo estimado de recuperación.

Comprobación:
Ver si existe una lista de contactos y plantillas de comunicación.
Implementación:
Crear mensajes prediseñados para incidentes leves, moderados y graves, aprobados por dirección.

🔧 **Función: Recuperar**

Se centra en restaurar la operatividad tras un incidente.

RC.RP-01:

Se ejecuta el plan de recuperación tras un incidente.

Ejemplo:
Tras un ataque o error, se restaura el entorno desde la última copia de seguridad verificada y se revisa la integridad de los datos antes de publicar.

Comprobación:
Comprobar si el personal sabe cómo restaurar un servidor sin ayuda.
Implementación:
Elaborar un manual paso a paso de recuperación con capturas de pantalla y guardarlo en la nube.

RC.RP-03:

Se verifica la integridad de las copias antes de la restauración.

Ejemplo:
Antes de restaurar una copia, se escanea en busca de malware y se comprueban los registros hash.

Comprobación:
Ver si este paso figura en los procedimientos escritos.

Implementación:
Automatizar una validación hash (SHA-256) previa a toda restauración.

RC.RP-05:

Se verifica la integridad del sistema restaurado.

Ejemplo:
Después de la recuperación, el equipo de QA comprueba que la API, la base de datos y el panel web funcionan correctamente y sin errores.

Comprobación:
Ver si existen registros de pruebas post-recuperación.
Implementación:
Crear una lista de verificación de funciones críticas que deben probarse antes de declarar "operativo".

RC.CO-03:

Se comunican los avances de recuperación a las partes interesadas.

Ejemplo:
Mientras el sistema se recupera, el responsable técnico informa a dirección y clientes del progreso mediante un canal de Telegram o página de estado.

Comprobación:
Ver si hay un método oficial de comunicación en incidentes prolongados.
Implementación:
Establecer un canal único (por ejemplo, correo "status@empresa.com