Actividad 1 - Núcleo NIST

Queremos identificar y relacione las **funciones, categorías y subcategorías del núcleo del framework MIST**, aplicándolas a un caso realista en un entorno TI.

1. **CONTEXTO**: Elige un contexto realista en el que sea aplicable la seguridad informática, descríbelo.
2. **FUNCIONES-CATEGORÍAS-SUBCATEGORÍAS:** Elige al menos cuatro subcategorías por función y explica como se podrían aplicar en el entorno descrito.
    - Indica en la práctica como comprobarías en la práctica si esa subcategoría está implementada en el contexto. En caso contrario, como la implementarías.

Contexto:

Pequeña empresa, de una veintena de empleados: Esta empresa desarrolla y aloja aplicaciones de gestión de inventario para sus clientes en la nube.

\\\\\\\\\\\\\\\\\\\\\\

Riesgos Clave:

1. **Datos Sensibles:** Manejamos información de inventario, lo que incluye detalles de la cadena de suministro de nuestros clientes.

2. **Dependencia de la Nube:** Dependemos totalmente de nuestro proveedor de servicios en la nube para el alojamiento y las copias de seguridad.

3. **Amenazas Frecuentes:** El *phishing* (correos falsos) y el *ransomware* (secuestro de datos) son amenazas constantes.

\\\\\\\\\\\\\\\\\\\\

- **Gobernar: se asegura de que la estrategia y las reglas de seguridad cibernética de la organización se establezcan, comuniquen y supervisen.**

1) **GV.RM-02:** Se establecen, se comunican y se mantienen las declaraciones sobre el apetito de riesgo y la tolerancia al riesgo.

Tenemos que decidir cuánto riesgo podemos "tragar". Por ejemplo, acordamos que no podemos permitirnos más de 3 horas de inactividad de nuestra aplicación de inventario porque eso afectaría gravemente a nuestros.

Comprobación: Buscaría un documento aprobado por el director general que indique el tiempo máximo de interrupción aceptable (nuestro límite de tolerancia).

Implementación: Si no existe, pediría a la gerencia que defina qué es "catastrófico" para el negocio y lo pondría por escrito.

2) **GV.RR-02:** Se establecen, comunican, comprenden y aplican las funciones, responsabilidades y autoridades relacionadas con la gestión de riesgos de seguridad cibernética.

Debemos nombrar a alguien (quizás un desarrollador senior a cargo de la seguridad) responsable de los parches de software y que todos sepan que él es la persona a quien acudir en caso de emergencia.

Comprobación: Preguntaría a tres empleados al azar: "¿Quién es el responsable de la seguridad de la red?" Si obtengo tres respuestas diferentes, la responsabilidad no está clara.

Implementación: Crearía un gráfico sencillo y lo pegaría en la pizarra de la oficina y lo enviaría por correo, definiendo los roles de seguridad.

3) **GV.PO-01:** La política de gestión de riesgos de seguridad cibernética se establece... y es comunicada y aplicada.

Necesitamos reglas básicas. Por ejemplo, una política que diga que todos los empleados deben usar una contraseña de al menos 12 caracteres y cambiarla cada 90 días para acceder a los servidores de desarrollo.

Comprobación: Pediría el "Manual de Políticas de Seguridad". Si no existe o está desactualizado, hay que actuar.

Implementación: Empezaría con una política de contraseñas (*password policy*) muy básica y haría que el equipo técnico la implemente forzosamente en el sistema de inicio de sesión.

4) **GV.SC-04:** Los proveedores son conocidos y priorizados por criticidad.

Nuestro principal proveedor es el servicio de alojamiento en la nube. Si cae, caemos nosotros. Nuestro proveedor de café no es tan crítico. Necesitamos saber quién es quién.

Comprobación: Revisaría la lista de proveedores. ¿Hay una columna que dice si el servicio es "Crítico" o "No Crítico"?

Implementación: Si no hay lista, la creo, marcando con una "C" (Crítico) a los proveedores que, si fallan, detienen inmediatamente el negocio.

- **Identificar: se centra en conocer los riesgos actuales de seguridad cibernética de la organización, incluyendo la comprensión de los activos (datos, hardware, software) y los riesgos relacionados.**

1) ID.AM-01: Se mantienen inventarios del hardware gestionado por la organización.

Necesitamos una lista de todos los ordenadores portátiles de la empresa. Si un portátil desaparece, debemos saber qué información contenía.

Comprobación: Compararía la lista de inventario de hardware con el número real de portátiles en uso. Si la lista está incompleta, no funciona.

Implementación: Usaría una hoja de cálculo simple para registrar cada dispositivo, su número de serie y a quién se le asignó.

2) ID.RA-01: Se identifican, validan y registran las vulnerabilidades de los activos.

Debemos escanear nuestra aplicación web mensualmente para buscar errores de programación o configuraciones incorrectas antes de que un atacante los encuentre.

Comprobación: Preguntaría por el informe del último "escaneo de vulnerabilidades". Si no hay informes, no lo estamos haciendo.

Implementación: Instalaría y ejecutaría una herramienta de escaneo de vulnerabilidades básica y registraría los 5 fallos más graves encontrados.

3) **ID.AM-05:** Se priorizan los activos en función de su clasificación, criticidad... e impacto en la misión.

Nuestro activo más crítico es la base de datos de clientes. El código fuente de la aplicación es crítico. El sistema de impresión de facturas es menos crítico.

Comprobación: Revisaría si nuestros activos identificados tienen un nivel de prioridad (Alto/Medio/Bajo) que guía dónde gastamos más recursos de protección.

Implementación: Clasificaría todos los activos principales, asegurándome de que la base de datos de clientes tiene la máxima prioridad.

4) ID.RA-03: Se identifican y registran las amenazas internas y externas a la organización.

Debemos considerar que tanto un hacker externo como un empleado descontento (amenaza interna) podrían causar daño, y registrar qué tipos de ataques son más probables (por ejemplo, ataque de ransomware dirigido).

Comprobación: Buscaría un listado donde se detallen las "5 Peores Cosas que Podrían Pasar" (Modelado de Amenazas).

Implementación: Celebraría una reunión corta con el equipo para identificar y documentar las amenazas más probables para nuestra empresa.

- Proteger: utiliza medidas de protección para gestionar los riesgos, lo que ayuda a prevenir o reducir la probabilidad y el impacto de los eventos adversos.

1) **PR.AA-03:** Los usuarios, servicios y hardware están autenticados.

Todos los empleados que acceden a la aplicación web del cliente deben usar Autenticación Multifactor (MFA) además de la contraseña, ya que esto hace mucho más difícil el acceso a un atacante.

Comprobación: Intentaría acceder a una cuenta crítica solo con la contraseña (sin el código de teléfono o aplicación). Si puedo, esta subcategoría no está implementada.

Implementación: Configurar la MFA como obligatoria en todos los accesos a la nube y al correo electrónico.

> 2) PR.DS-11: Se crean, protegen, mantienen y comprueban copias de seguridad de los datos.

Si somos víctimas de *ransomware*, la única manera de recuperarnos sin pagar es tener copias de seguridad de nuestros datos y de los clientes, y saber que esas copias funcionan.

Comprobación: Pediría una prueba de **restauración**. ¿Funciona la copia de seguridad más reciente en un sistema de prueba? Si no se ha probado la restauración en los últimos 6 meses, no está implementado correctamente.

Implementación: Programar un simulacro de restauración mensual obligatorio.

> 3) PR.AT-01: Se sensibiliza y capacita al personal para que disponga de los conocimientos y habilidades necesarios....

Dar formación a todos los empleados sobre cómo detectar correos electrónicos de *phishing* y qué hacer si reciben uno.

Comprobación: Preguntaría a la directora de recursos humanos cuándo fue la última vez que se impartió formación de seguridad para *todos* los empleados.

Implementación: Usaría una herramienta gratuita para enviar correos electrónicos de *phishing* de prueba y luego daría una charla de capacitación a quienes "cayeron" en la trampa.

> 4) PR.DS-01: La confidencialidad, la integridad y la disponibilidad de los datos en reposo están protegidas.

Cifrar la base de datos de los clientes cuando está guardada en el servidor (datos "en reposo"), para que, si un atacante roba el disco, no pueda leer la información.

Comprobación: Preguntaría al administrador de la base de datos: "¿Está la base de datos cifrada en el disco?".

Implementación: Activar el cifrado de volumen o el cifrado de bases de datos (si la plataforma de nube lo permite) para los datos más críticos.

- Detectar: se centra en el descubrimiento y análisis oportuno de anomalías e indicadores de compromiso para identificar que se están produciendo ataques o incidentes de seguridad cibernética.

1) DE.CM-01: Las redes y los servicios de red se monitorean para detectar acontecimientos potencialmente adversos.

Configurar alertas para que si un servidor empieza a enviar gigabytes de datos a un país que no es donde están nuestros clientes, el equipo técnico reciba una notificación inmediata.

Comprobación: Buscaría la lista de alertas automáticas. Si solo hay alertas de que el servidor está *apagado*, pero no de actividad sospechosa, es insuficiente.

Implementación: Configurar reglas de monitoreo en la herramienta de gestión de red que detecten tráfico de datos anormalmente alto.

2) DE.CM-03: Se monitorea la actividad del personal y el uso de la tecnología para detectar posibles acontecimientos adversos.

Si un administrador de base de datos accede a 500 registros de clientes a las 3:00 a.m., eso es sospechoso y debe generar una alerta.

Comprobación: Preguntaría: "¿Revisamos los registros de acceso a los datos sensibles, especialmente fuera del horario de oficina?".

Implementación: Configurar el sistema para que registre cada acceso a la base de datos y revisar un resumen de esa actividad semanalmente.

3) DE.AE-03: Se correlaciona la información procedente de diversas fuentes.

Si vemos un intento de inicio de sesión fallido en la VPN y, al mismo tiempo, vemos una descarga masiva de archivos desde una cuenta de correo electrónico, debemos correlacionar esos dos eventos como parte del mismo posible ataque.

Comprobación: Si detectamos una alerta, ¿el proceso de investigación exige mirar los registros de otros sistemas relacionados (red, correo, VPN)?

Implementación: Crear un proceso manual (hasta que tengamos una herramienta SIEM) para que el analista revise *siempre* los logs de la red y del servidor para buscar conexiones.

4) DE.AE-07: La inteligencia sobre amenazas cibernéticas y otra información contextual se integran en el análisis.

Cuando se produce un incidente, necesitamos saber si el ataque que estamos viendo (por ejemplo, el uso de un código de explotación específico) es algo que está sucediendo a otras empresas del sector.

Comprobación: Preguntaría al equipo si están suscritos a algún boletín de seguridad (como los del NIST o proveedores de antivirus) para conocer las amenazas recientes.

Implementación: Suscribir al equipo técnico a fuentes de inteligencia de amenazas gratuitas y obligarlos a revisar las alertas relevantes cada mañana.

- **Responder: se centra en las acciones tomadas en relación con un incidente de seguridad cibernética detectado, incluyendo la contención, el análisis, la mitigación y la comunicación.**

1) RS.MA-01: Se ejecuta el plan de respuesta a incidentes en coordinación con los terceros pertinentes una vez que se declara un incidente.

Si se detecta un *ransomware*, debemos seguir un plan predefinido (por ejemplo: Paso 1: desconectar el servidor; Paso 2: avisar al gerente; Paso 3: llamar al proveedor de nube).

Comprobación: Preguntaría si se han realizado ejercicios o simulacros del plan. Si el plan existe, pero nunca se ha puesto a prueba, es ineficaz.

Implementación: Crear un documento simple de 10 pasos llamado "Plan de Respuesta Rápida" y simular un ataque al menos una vez al año.

2) **RS.MI-01:** Se contienen los incidentes.

Si un ordenador está infectado con *malware*, debemos desconectarlo de la red de la oficina inmediatamente para que la infección no se propague a otros sistemas.

Comprobación: Preguntaría al equipo de soporte: "¿Cuánto tardas en aislar un PC de la red si te lo pido ahora?". Si la respuesta es lenta, el proceso necesita mejora.

Implementación: Asegurar que los firewalls tienen reglas listas para aislar segmentos de red con un solo clic en caso de emergencia.

3) RS.AN-03: Se realizan análisis para determinar lo que ocurrió durante un incidente y la causa raíz del mismo.

Después de solucionar un ataque de *phishing* que resultó en la pérdida de credenciales, debemos investigar si el fallo fue por falta de capacitación, falta de MFA, o si la contraseña era demasiado débil.

Comprobación: Buscaría el informe de cierre del incidente. Debe incluir una sección llamada "Causa Raíz". Si falta, hay que exigirlo.

Implementación: Implementar una plantilla de informe post-incidente que obligue a los analistas a listar la causa raíz del problema.

4) RS.CO-02: Se notifican los incidentes a las partes interesadas internas y externas.

Si los datos de nuestros clientes han sido comprometidos, debemos notificar a los clientes y a nuestro asesor legal, según lo exigen las leyes de privacidad que nos aplican.

Comprobación: Comprobaría si el plan de respuesta tiene una lista de contactos internos (gerencia, legal) y externos (clientes, reguladores) para notificaciones.

Implementación: Redactar plantillas de comunicación para diferentes escenarios (p. ej., "solo falló el sistema" vs. "hubo una brecha de datos") y obtener aprobación legal para usarlas.

- **Recuperar: se ocupa de restaurar los activos y las operaciones afectadas por un incidente de seguridad cibernética para volver a la normalidad lo antes posible.**

1) RC.RP-01: La parte de recuperación del plan de respuesta a incidentes se ejecuta una vez que se inicia....

Usar nuestro plan detallado para restaurar la aplicación web y la base de datos de los clientes desde las copias de seguridad una vez que estamos seguros de que el atacante ha sido expulsado.

Comprobación: ¿El equipo sabe exactamente dónde está el plan de recuperación y puede ejecutarlo sin supervisión intensa?

Implementación: El plan de recuperación debe ser un documento separado y fácil de seguir, con pasos claros sobre cómo usar las copias de seguridad de la nube.

2) RC.RP-03: Se verifica la integridad de las copias de seguridad y otros activos de restauración antes de usarlos para la restauración.

Antes de restaurar la copia de seguridad, debemos escanearla para asegurarnos de que no contiene el *malware* que causó el problema. Si restauramos algo infectado, el ataque vuelve a empezar.

Comprobación: ¿El proceso de restauración incluye un paso obligatorio de "verificación de malware" y "validación de datos" de la copia de seguridad?

Implementación: Implementar herramientas que hagan un chequeo rápido de la integridad (checksums) de la copia de seguridad antes de su uso.

3) RC.RP-05: Se verifica la integridad de los activos restaurados, se restauran los sistemas y servicios y se confirma el estado operativo normal.

Una vez que la aplicación vuelve a estar en línea después de la recuperación, el equipo de control de calidad debe verificar que todas las funciones principales (inicio de sesión, actualización de inventario) funcionan correctamente y que no quedan "puertas traseras" abiertas.

Comprobación: Buscaría la lista de "Pruebas Post-Recuperación" que se ejecutaron. Si solo restauramos y cruzamos los dedos, no estamos haciendo esta subcategoría.

Implementación: Crear una lista de verificación de 10 puntos para confirmar que el sistema restaurado es funcional y seguro, y que debe firmarse por el gerente antes de declarar el fin de la crisis.

4) RC.CO-03: Las actividades de recuperación y los progresos... se comunican a las partes interesadas internas y externas designadas.

Informar a los directivos (internos) y a los clientes (externos) sobre el progreso: "Ya estamos al 80% de la recuperación, esperamos estar 100% operativos en 2 horas."

Comprobación: Si el sistema está caído, ¿existe un canal de comunicación (una página web de estado o un correo de difusión) que se actualice cada hora?

Implementación: Establecer un protocolo de comunicación con partes interesadas para dar actualizaciones frecuentes y transparentes sobre el estado de la recuperación.