NÚCLEO NIST

Cristóbal Suárez Abad

Seguridad y Alta Disponibilidad - 2º ASIR

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 unos 20 empleados que desarrolla y aloja aplicaciones web para clientes.

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).

Funciones:

- *Gobernar: se asegura de que la estrategia y las normas de ciberseguridad se establezcan, comuniquen y supervisen adecuadamente.*

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

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

Tenemos que decidir cuánto riesgo puede tolerar la compañía. 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: Buscar la existencia de un informe donde se indique los tiempos de interrupción del servicio que son aceptables (mala imagen, incumplimiento del contrato, etc).

Implementación: Si no existe, pediría a la gerencia que defina qué es "catastrófico" para el negocio y elaboraría un informe.

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 designar quien se debe encargar de las medidas de seguridad ante amenazas lógicas (administrador de sistemas, soporte técnico o algún desarrollador senior) y asegurarnos de que todos los empleados sepan a quien tienen que 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 en base al contexto organizativo, la estrategia de seguridad cibernética y las prioridades, y es comunicada y aplicada.

La empresa establece políticas de seguridad:

- Actualizar el sistema operativo y software mínimo cada mes.
- Prohibición de usar dispositivos y cuentas personales para tareas de trabajo.
- Reglas de creación de contraseñas seguras (número caracteres, caducidad, etc.

Comprobación: Revisar si existe un documento de políticas actualizado y si todos los empleados lo conocen y cumplen.

Implementación: Redactar un documento breve en formato PDF con las políticas más básicas (actualizaciones, contraseñas, acceso remoto, actualizaciones) y hacerlo firmar digitalmente a los empleados.

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

Debemos saber cuales son los proveedores de servicios críticos (proveedor de internet, electricidad, etc); y cuales no (material de oficina, etc).

Comprobación: Ver si la empresa dispone de una lista actualizada de proveedores con un nivel de criticidad definido.

Implementación: Crear un “Excel” con listado de proveedores marcando su nivel de criticidad y añadiendo información de contacto y observaciones, lo cual servirá ante futuras incidencias

- ***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.

Listar los portátiles y dispositivos móviles usados por los empleados, incluyendo los que se llevan a casa en modo teletrabajo. Cualquier dispositivo que pueda capacidad para contener información debe ser debidamente inventariado.

Comprobar: ver si existe un inventario y si está actualizado. ¿Ha desaparecido algún dispositivo? ¿Quién fue el último que lo usó?

Implementación: la rápida y sencilla es crear un "Excel". Pero también existe software específico[1] que permite recoger más datos de los equipos a inventariar y automatizar ciertos procesos.

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, es que las cosas no se están haciendo bien.

Implementación: Existen en el mercado herramientas de escaneo como OpenVAS[2] y [3]Nessus que permiten detectar vulnerabilidades en sistemas.

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

Por ejemplo, el servidor con la base de datos de los clientes es primordial y debe ser protegido a toda costa (reputación, demandas legales, etc); el de pruebas no es tan importante.

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.

---

[1] https://blog.invgate.com/es/software-de-inventario-informatico-y-de-gestion-de-activos
[2] https://www.openvas.org/
[3] https://es-la.tenable.com/products/nessus

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

Debemos considerar que qué tipos de ataques son más probables:

- Amenazas Internas: un empleado podría subir un código sin revisión o extraer datos sin permiso.
- Amenazas Externas: hackers, ladrones, etc.

Comprobación: Revisar si existen registros de incidentes previos o listas de amenazas evaluadas. También de otras empresas de la zona, noticias, etc.

Implementación: Celebrar una reunión trimestral de 15 minutos para actualizar la lista de amenazas según las últimas tendencias de seguridad y la experiencia reciente.

- ***Proteger**: Se utilizan medidas de protección para gestionar los riesgos de seguridad cibernética de la organización.*

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

Todo acceso a los activos requiere autenticación multifactor (MFA) y cumplir con la política de contraseñas.

Comprobación: Intentar acceder con solo usuario y contraseña. Si es posible, la MFA no está correctamente configurada.

Implementación: Configurar la MFA como obligatoria en todos los accesos.

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

Las copias de seguridad automáticas diarias se almacenan tanto en la propia empresa como en un lugar externo (solo conocido por responsables de seguridad).

Comprobación: Probar la restauración en un entorno de pruebas una vez al mes.

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 para realizar tareas generales teniendo en cuenta los riesgos de seguridad cibernética.

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

Comprobación: Poner a prueba sus capacidades enviándoles correos trampa para descubrir si están pendientes en los cursos.

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. Los accesos deben ser registrados.

- ***Detectar**: Se detectan y analizan posibles ataques y situaciones comprometedoras en materia de seguridad cibernética.*

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

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).

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

Registrar y auditar cada cambio en el código fuente y cada acceso a la base de datos de clientes.

Ver si el sistema de control de versiones (como en Gitlab[4] y GitHub[5]) tiene habilitado el registro de auditoría.

También se pueden configurar alertas que notifiquen accesos a segmentos protegidos o descargas masivas de datos.

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

Por ejemplo, se deben comparar los registros del firewall, del proveedor de internet y del sistema de correo electrónico (ejemplo: un intento de acceso no autorizado seguido de un envío masivo de correos sospechosos).

Implementación: Usar sistemas SIEM[6] (*Security Information and Event Management*), los cuales permiten analizar de manera automática registros del sistema en busca de vulnerabilidades y comportamientos anómalos.

[4] https://about.gitlab.com/topics/version-control/
[5] https://github.com/resources/articles/software-development/what-is-version-control
[6] https://www.ibm.com/es-es/think/topics/siem

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

Suscribirse a fuentes de inteligencia de seguridad (como US-CERT[7] o INCIBE[8]) para estar al día de nuevas vulnerabilidades. Asegurarse de que se llevan a cabo las recomendaciones.

[7] https://www.cisa.gov/stopransomware/official-alerts-statements-cisa
[8] https://www.incibe.es/incibe-cert/alerta-temprana/avisos

Responder: Se toman medidas en relación con un incidente de seguridad cibernética detectado.

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: contactar con clientes afectados).

Se debería crear un documento con los pasos a seguir para cada servidor: gerente, cliente, etc.

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

Si un dispositivo está infectado, debemos desconectarlo de la red de manera inmediata para evitar que se propague el virus. Para evitar demoras, se debe implementar protocolos para su desconexión (firewalls tienen reglas listas para aislar segmentos de red con un solo clic en caso de emergencia o incluso si es necesario de manera física).

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

Por ejemplo, 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. Para ello se debe instaurar un protocolo ante estas incidencias que obligue a buscar las causas.

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 (si hubiese), según lo exigen las leyes de privacidad que nos aplican (LOPD[9] y según se estipule en el contrato).

[9] https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

- ***Recuperación****: Se restauran los activos y las operaciones afectados por un incidente de seguridad cibernética.*

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

Debe existir un plan detallado para restaurar la aplicación web y la base de datos de los clientes desde las copias de seguridad una vez que se está seguro de que han terminado los ataques. Este documento debe ser un fácil de seguir, con pasos claros sobre cómo restaurar desde las copias de seguridad.

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.

El proceso de restauración debe incluir un paso obligatorio de "verificación de malware" (entendiéndose que se haya descubierto malware o vulnerabilidad que en comprobaciones anteriores pasase por alto) de la copia de seguridad.

Se deben realizar comprobaciones de malware en las copias de seguridad y tener un histórico de copias (cuanto más podamos remontarnos en el tiempo, mejor).

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.

Tras llevar a cabo la restauración de la copia de seguridad, debe confirmarse que las funciones principales funcionan de manera correcta. Para ello debe de haber documentación con los pasos a seguir para comprobar la funcionalidad de cada servicio, servidor, etc.

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

Para los clientes se debe tener creadas una serie de mensajes predefinidos (plantillas) para informales sobre el proceso (se puede establecer cuales son los intervalos mínimos para informarles o en cada que punto del proceso se informa). Para personal interno se deben crear también una serie de mensajes con los tiempos en los que se espera tener resuelta la incidencia para evitar demoras en las actividades laborales.