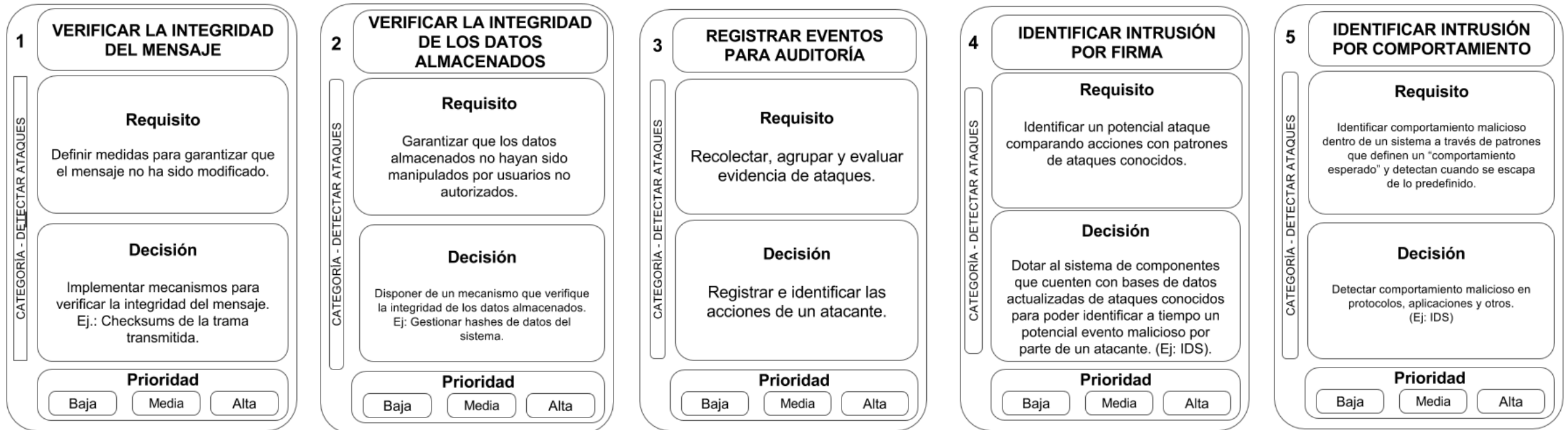


Detectar ataques



Detener o mitigar ataques

CATEGORÍA - DETENER o MITIGAR ATAQUES

6

AUTENTICAR USUARIOS

Requisito

Verificar que un usuario o una máquina remota es quien dice ser.

Decisión

Implementar mecanismos de autenticación basados en password, one-time password, certificados digitales, autenticación biométrica, entre otros.

Prioridad

BajaMediaAlta

CATEGORÍA - DETENER o MITIGAR ATAQUES

7

AUTORIZAR USUARIOS

Requisito

Garantizar que un usuario autorizado tenga los derechos para acceder y modificar los datos o servicios

Decisión

Implementar mecanismos de control de acceso.
Ej: Control de acceso basado en roles (RBAC), control de acceso discrecional (DAC), etc.

Prioridad

BajaMediaAlta

CATEGORÍA - DETENER o MITIGAR ATAQUES

8

GESTIONAR DATOS DE SEGURIDAD

Requisito

Mantener la integridad de los datos, garantizar que terceros no autorizados no puedan acceder a estos y que los datos no sean susceptibles de corrección

Decisión

Gestionar llaves criptográficas, passwords, almacenamiento seguro de reglas de autorización u otras formas de proteger los datos.

Prioridad

BajaMediaAlta

CATEGORÍA - DETENER o MITIGAR ATAQUES

9

FILTRAR DATOS

Requisito

Evitar ataques provenientes del ingreso de datos maliciosos o de fuentes no confiables

Decisión

Implementar filtros de contenidos en los datos recibidos a través de peticiones de usuarios al sistema

Prioridad

BajaMediaAlta

CATEGORÍA - DETENER o MITIGAR ATAQUES

10

VERIFICAR EL ORIGEN DEL MENSAJE

Requisito

Determinar la autenticidad del mensaje

Decisión

Implementar mecanismo de verificación del remitente.

Ej: Utilizar firma digital para verificar que la fuente sea fidedigna y con ello evitar suplantación del emisor.

Prioridad

BajaMediaAlta

CATEGORÍA - DETENER o MITIGAR ATAQUES

11

ESTABLECER UN CANAL SEGURO

Requisito

Generar una transmisión de datos segura entre emisor y receptor

Decisión

Implementar mecanismo que permita tanto autenticación de endpoints como de mensajes, además del cifrado de éstos.

Prioridad

BajaMediaAlta

CATEGORÍA - DETENER o MITIGAR ATAQUES

12

OCULTAR DATOS A TRAVÉS DE CIFRADO

Requisito

Proteger los datos de accesos no autorizados.

Decisión

Implementar mecanismos de protección de datos.
Ej.: Virtual Private Network (VPN), Secure Sockets Layer (SSL).

Prioridad

BajaMediaAlta

CATEGORÍA - DETENER o MITIGAR ATAQUES

13

OCULTAR DATOS A TRAVÉS DE ESTEGANOGRAFÍA

Requisito

Ocultar datos secretos dentro de otros datos de apariencia inocente, llamados 'contenedores'

Decisión

Proteger la información a través del uso de algoritmos o técnicas para la ocultación de datos.

Prioridad

BajaMediaAlta

Recuperarse de ataques

Reaccionar a ataques

CATEGORIA - RECUPERARSE DE ATAQUES

16

REALIZAR AUDITORÍA

Requisito

Inspeccionar el sistema para identificar eventos críticos que permitan dimensionar el grado de compromiso luego de un ataque con el propósito de ejecutar de una estrategia de recuperación.

Decisión

Realizar escaneos de vulnerabilidades de seguridad, revisar logs y controles de acceso de aplicaciones y sistemas operativos, y analizar acceso físico a los sistemas.

Prioridad

Baja

Media

Alta

CATEGORIA - RECUPERARSE DE ATAQUES

17

APLICAR POLÍTICAS INSTITUCIONALES (RECUPERARSE DE ATAQUES)

Requisito

Asegurar la información de una organización.

Decisión

Aplicar políticas de aseguramiento de datos.

Prioridad

Baja

Media

Alta

CATEGORIA - REACCIONAR A ATAQUES

14

NOTIFICAR A USUARIOS

Requisito

Notificar a un determinado actor.

Decisión

Reportar cuando el sistema ha detectado un ataque.

Prioridad

Baja

Media

Alta

CATEGORIA - REACCIONAR A ATAQUES

15

APLICAR POLÍTICAS INSTITUCIONALES (REACCIONAR A LOS ATAQUES)

Requisito

Asegurar la información de una organización.

Decisión

Aplicar políticas de aseguramiento de datos

Prioridad

Baja

Media

Alta

Tácticas de seguridad

