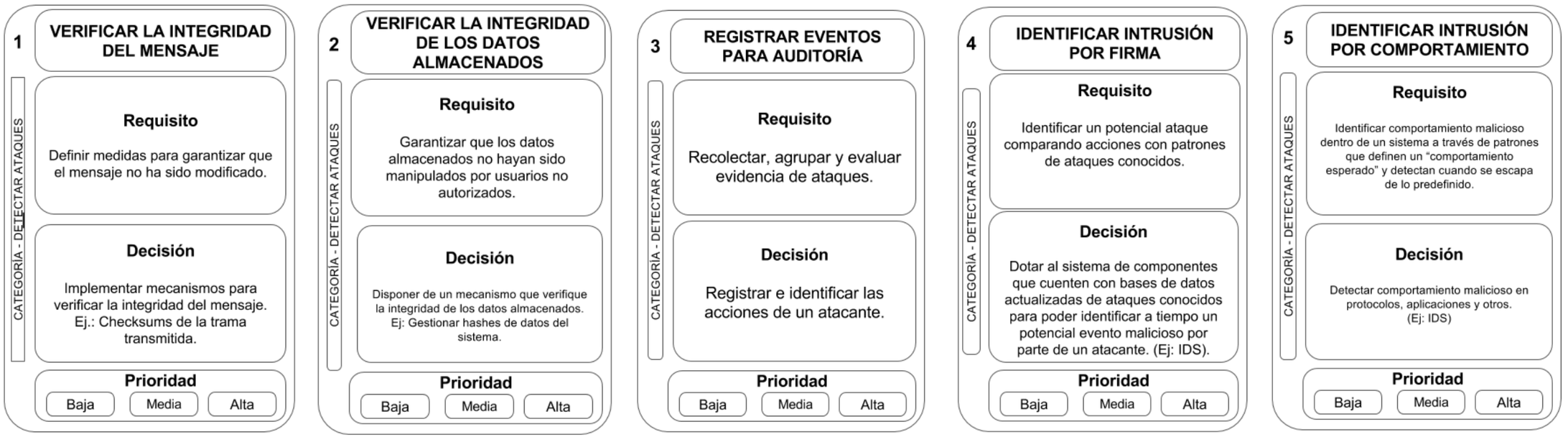
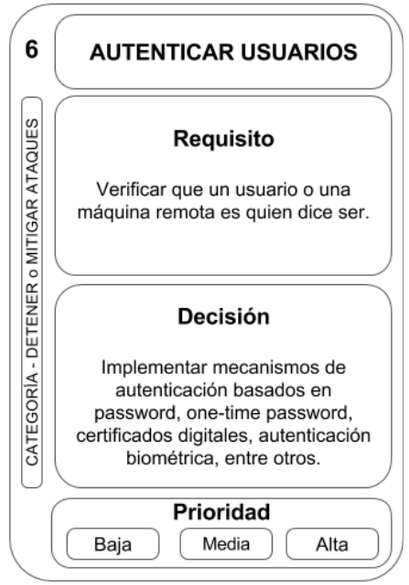
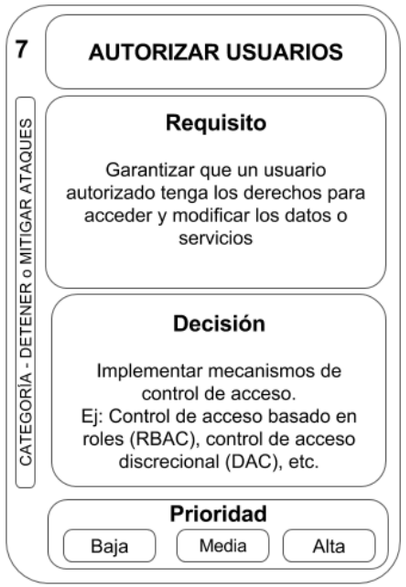
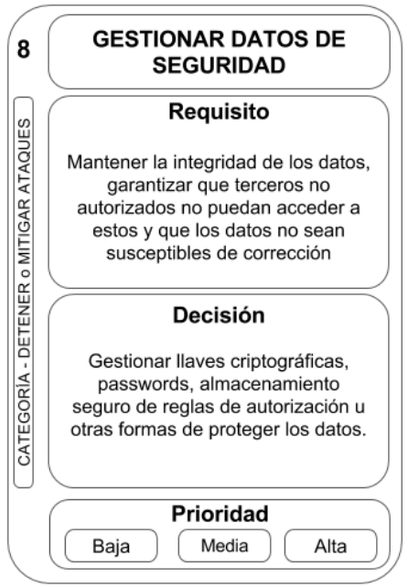
Detectar ataques

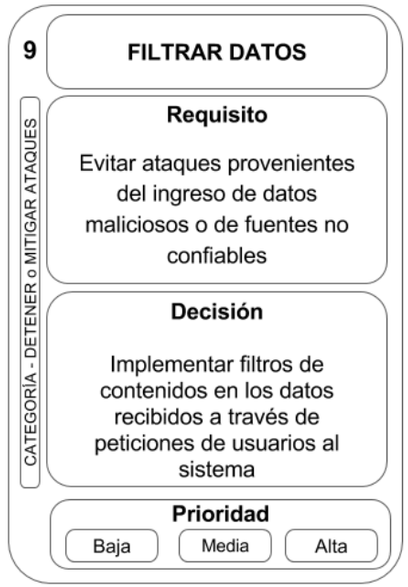


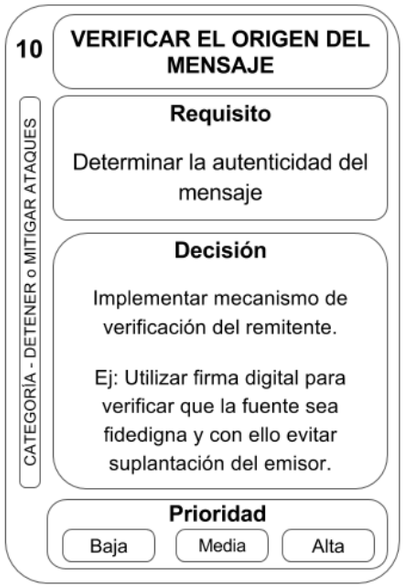
Detener o mitigar ataques

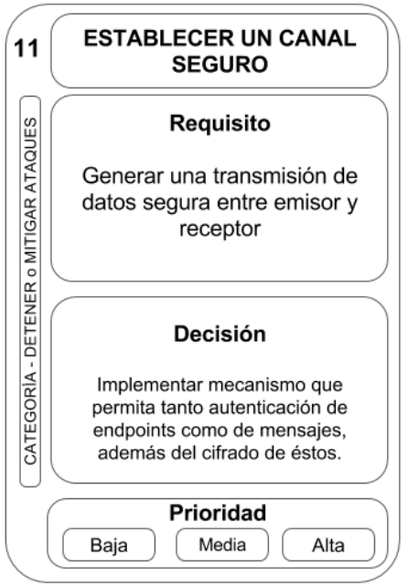


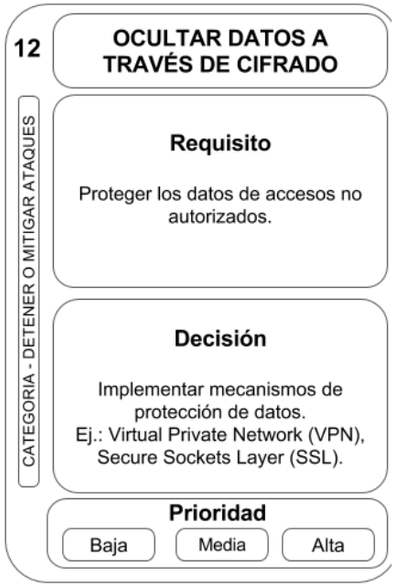


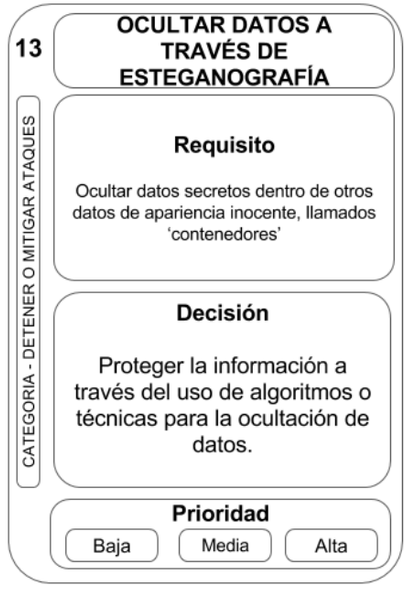












Reaccionar a ataques

14 NOTIFICAR A USUARIOS

CATEGORIA - REACCIONAR A ATAQUES

Requisito

Notificar a un determinado actor.

Decisión

Reportar cuando el sistema ha detectado un ataque.

Prioridad

Baja | Media | Alta

15 APLICAR POLÍTICAS INSTITUCIONALES (REACCIONAR A LOS ATAQUES)

CATEGORIA - REACCIONAR A ATAQUES

Requisito

Asegurar la información de una organización.

Decisión

Aplicar políticas de aseguramiento de datos

Prioridad

Baja | Media | Alta

Recuperarse de ataques

16 REALIZAR AUDITORÍA

CATEGORIA - RECUPERARSE DE ATAQUES

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

17 APLICAR POLÍTICAS INSTITUCIONALES (RECUPERARSE DE ATAQUES)

CATEGORIA - RECUPERARSE DE ATAQUES

Requisito

Asegurar la información de una organización.

Decisión

Aplicar políticas de aseguramiento de datos.

Prioridad

Baja | Media | Alta