PROCESO NOTIFICACION Y GESTION DE INTENTOS DE INTRUSION

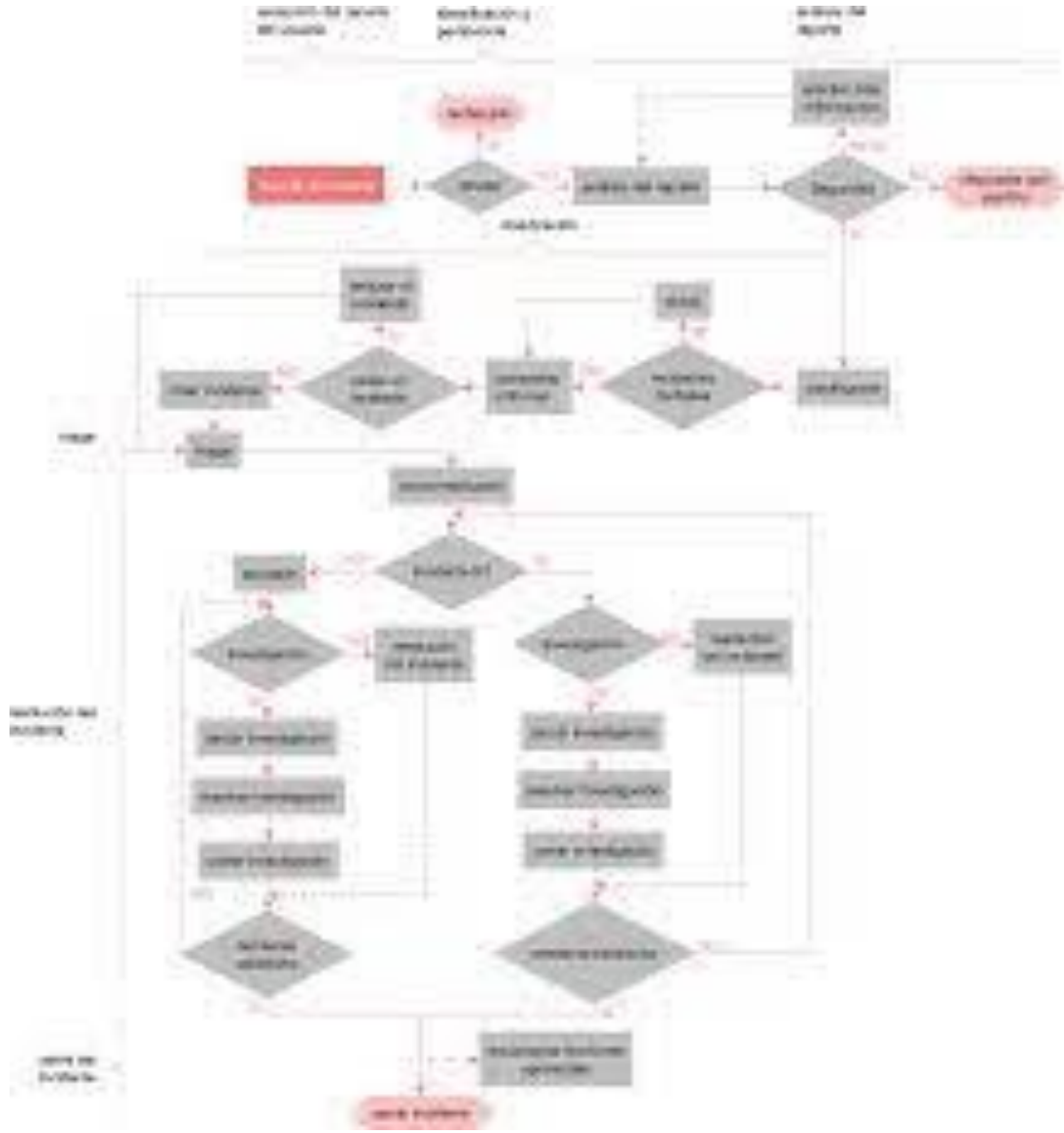


Ilustración 1. Sistema de ventanilla única

Notificaciones de incidentes

- El sujeto afectado enviará un correo electrónico (o ticket) al CSIRT de referencia A (INCIBE-CERT o CCN-CERT) notificando el incidente.
- El CSIRT de referencia, dependiendo del incidente, pone en conocimiento del mismo al organismo receptor implicado o a la autoridad nacional competente.

- Si afecta a la Defensa Nacional, al CSIRT de referencia ESP-DEF-CERT.
- Si afecta a una Infraestructura Crítica de la Ley PIC 8/2011, al CNPIC
- Si afecta al RGPD, a la AEPD.
- Si es un incidente de AAPP bajo el ENS de peligrosidad ALTA, MUY ALTA o CRÍTICA, al CCN-CERT
- Si es un incidente de obligado reporte según el RD 12/2018, a la Autoridad
- Nacional correspondiente:
  - - RGPD: se remite a la URL del portal de la AEPD.
  - - BDE: se remite la plantilla de notificación .XLS del BDE.
  - - PIC: se remite la plantilla de notificación .XLS del CNPIC.
  - - ENS: se remite la plantilla de notificación .DOC al CCN-CERT.
  - - NIS: se remite la plantilla de notificación de la Autoridad Nacional competente.

REPORTE DE INCIDENTES A CCN-CERT

- Se realizará como canal preferente a través de la aplicación habilitada al efecto: LUCIA1 , y de forma secundaria a través del correo electrónico de gestión de incidentes de ciberseguridad incidentes@ccn-cert.cni.es preferiblemente mediante mensajería cifrada con la clave PGP de este CERT2 .

REPORTE DE INCIDENTES A INCIBE-CERT

- Los ciberincidentes se reportan a INCIBE-CERT a través de un usuario que, como afectado final o identificado como punto de contacto por la entidad afectada, accede al servicio de respuesta a través de los medios proporcionados por este CERT. Si el reporte se realiza a través de correo electrónico, el buzón de correo genérico para la notificación de incidentes es incidencias@incibe-cert.es.

Criterios peligrosidad

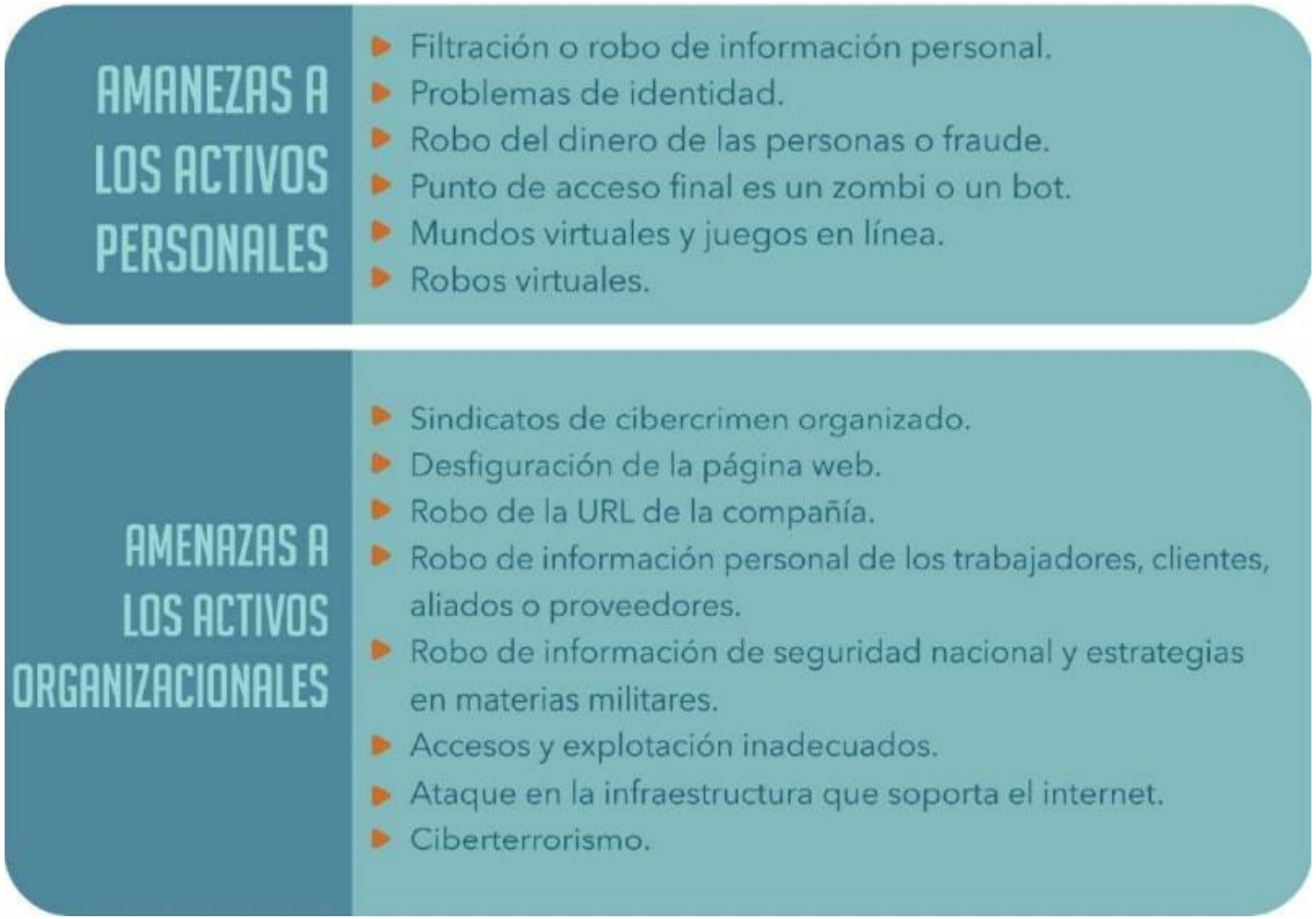
CRITERIOS DE DETERMINACIÓN DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES		
Nivel	**Clasificación**	**Tipo de incidente**
CRÍTICO	Otros	APT
MUY ALTO	Código dañino	Distribución de malware
		Configuración de malware
	Intrusión	Robo
	Disponibilidad	Sabotaje
		Interrupciones
ALTO	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Código dañino	Sistema infectado
		Servidor C&C (Mando y Control)
	Intrusión	Compromiso de aplicaciones
		Compromiso de cuentas con privilegios
	Intento de intrusión	Ataque desconocido
	Disponibilidad	DoS (Denegación de servicio)
		DDoS (Denegación distribuida de servicio)
	Compromiso de la información	Acceso no autorizado a información
		Modificación no autorizada de información
		Pérdida de datos
	Fraude	Phishing
MEDIO	Contenido abusivo	Discurso de odio
	Obtención de información	Ingeniería social
	Intento de intrusión	Explotación de vulnerabilidades conocidas
		Intento de acceso con vulneración de credenciales
	Intrusión	Compromiso de cuentas sin privilegios
	Disponibilidad	Mala configuración
	Fraude	Uso no autorizado de recursos
		Derechos de autor
		Suplantación
	Vulnerable	Criptografía débil
		Amplificador DDoS
		Servicios con acceso potencial no deseado
		Revelación de información
		Sistema vulnerable
BAJO	Contenido abusivo	Spam
	Obtención de información	Escaneo de redes (scanning)
		Análisis de paquetes (sniffing)
	Otros	Otros

Tabla 4. Criterios de determinación del nivel de peligrosidad de un ciberincidente

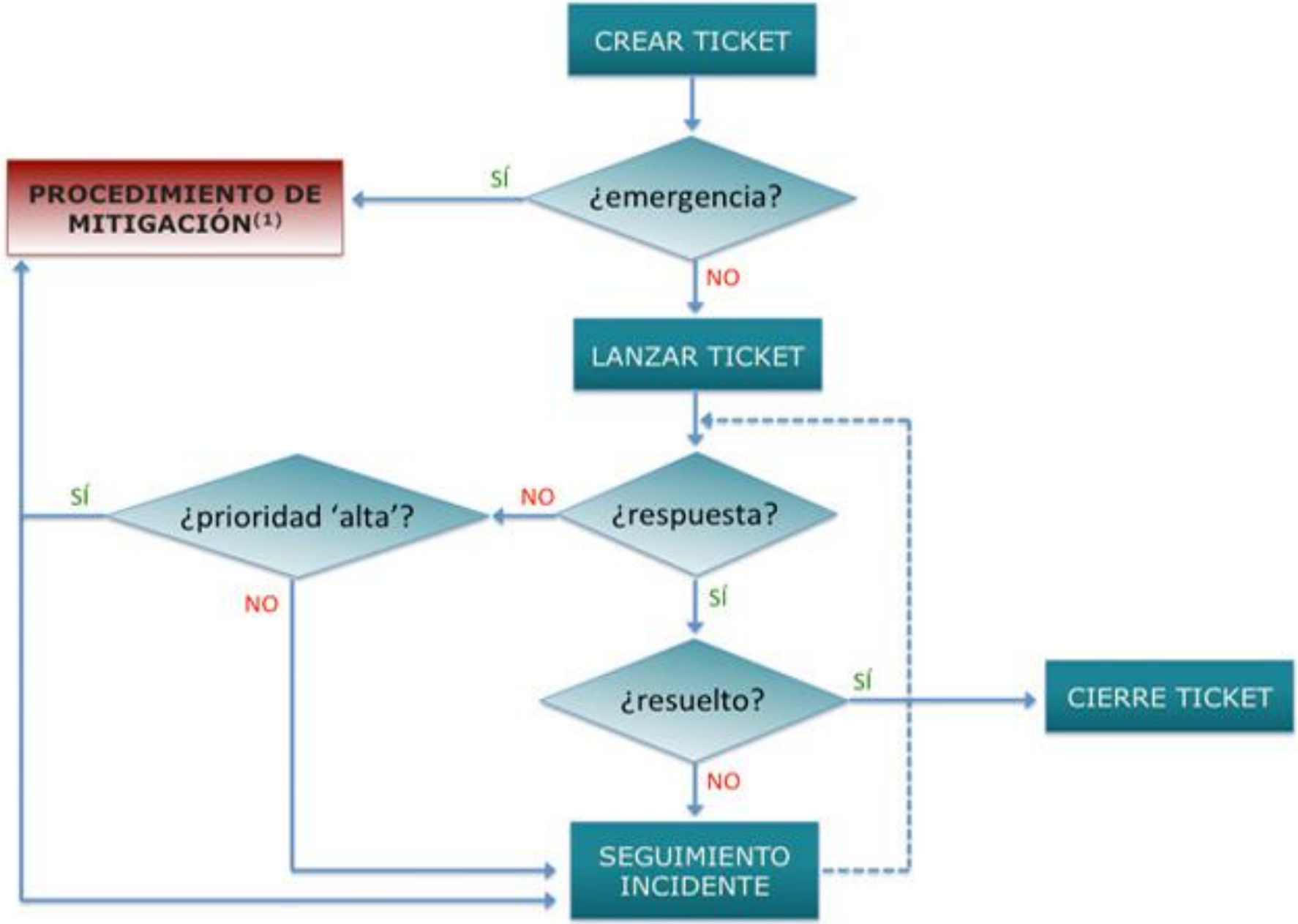
Nivel de Peligrosidad	Obligación de notificación del ciberincidente al CCN-CERT(*)	Cierre del ciberincidente (días naturales)	Prohibiciones
BAJO	No	15	- Se cierran automáticamente por los Sistemas de Alerta Temprana a los 60 días con el estado "Cerrado – Sin respuesta". - El Sistema de Alerta Temprana no renotifica el aviso al organismo afectado.
MEDIO	No	30	
ALTO	Sí	45	
MUY ALTO	Sí	90	- No debe asignarse nunca el estado "Cerrado – Sin respuesta) - El Sistema de Alerta Temprana re-notifica el aviso al organismo afectado cada siete días hasta recibir respuesta.
CRÍTICO	Sí	120	

Tabla 6 - Tipo de seguimiento a realizar por parte del CCN-CERT, según Nivel de Peligrosidad

Amenazas


AMANEZAS A LOS ACTIVOS PERSONALES
Filtración o robo de información personal.
Problemas de identidad.
Robo del dinero de las personas o fraude.
Punto de acceso final es un zombi o un bot.
Mundos virtuales y juegos en línea.
Robos virtuales.
AMENAZAS A LOS ACTIVOS ORGANIZACIONALES
Sindicatos de cibercrimen organizado.
Desfiguración de la página web.
Robo de la URL de la compañía.
Robo de información personal de los trabajadores, clientes, aliados o proveedores.
Robo de información de seguridad nacional y estrategias en materias militares.
Accesos y explotación inadecuados.
Ataque en la infraestructura que soporta el internet.
Ciberterrorismo.

Proceso interno



Webs utiles

- https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

- https://www.incibe.es/protege-tu-empresa/reporta-tu-incidente