Detección y documentación de incidentes de ciberseguridad (Incidentes de ciberseguridad)

Desarrollar procedimientos de actuación para la notificación de incidentes

Mediante el sistema de ventanilla única se informa de un incidente, la información solicitada en cada caso, en función de la naturaleza del afectado, deberá ser remitida de acuerdo al cauce establecido por su autoridad competente o CSIRT de referencia.

Notificación interna de incidentes

Mediante el sistema de ventanilla única se informa de un incidente, la información solicitada en cada caso, en función de la naturaleza del afectado, deberá ser remitida de acuerdo al cauce establecido por su autoridad competente o CSIRT de referencia.

Notificación de incidentes a quienes corresponda

Funcionamiento del sistema de ventanilla única:

1. El sujeto afectado enviará un correo electrónico (o ticket) al CSIRT de referencia (INCIBE-CERT o CCN-CERT) notificando el incidente.

2. El CSIRT de referencia, dependiendo del incidente, pone en conocimiento del mismo al organismo receptor implicado o la autoridad nacional competente:
    - Si afecta a la Defensa Nacional, al ESPDEFCERT
    - Si afecta a 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 MUY ALTA o CRÍTICA, al CCN-CERT
    - Si es un incidente de obligatorio reporte según el RD Ley 12/2018, a la autoridad nacional competente correspondiente.
        - RGPD: se remite 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 a CCN-CERT.
        - NIS: se remite la plantilla de notificación de la autoridad nacional competente.
3. El Organismo receptor implicado o autoridad nacional competente se pone en contacto con el sujeto afectado para recabar datos del incidente.
4. El sujeto afectado comunica las datos necesarios al organismo receptor implicado o autoridad nacional competente.
5. Si procede, desde la Oficina de Coordinación Cibernética (CNPIC) se pone la información a disposición de las Fuerzas y Cuerpos de Seguridad del Estado y Ministerio Fiscal para iniciar la investigación policial y judicial (art. 14.3 RD Ley 12/2018).