Procedimiento de resolución de incidencias de seguridad

Esta es la guía de los pasos a seguir como respuesta a una incidencia de seguridad detectada internamente en la ULPGC o remitida por otra autoridad externa reconocida, incluyendo alertas por SPAM, saturación de dispositivos, abusos u otros incidentes que se valoren como graves para el buen funcionamiento de los servicios. Entre paréntesis aparece quien realiza el paso indicado.

1. Por parte del SIC
    a. Si procede, comunicar la incidencia a cert@ulpgc.es aportando toda la información disponible (cualquier persona que detecte la incidencia).
    b. Recibir el incidente en cert@ulpgc.es (SDP[1]).
    c. Identificar el ordenador implicado y el usuario o persona de enlace externa al SIC que administra la red (en adelante responsable), con los datos aportados y, si no se puede, a través de la aplicación DHCP/DNS (SDP).
    d. Comunicar el incidente a la SDC[2] y, si procede, a la SAU[3] (SDP).
    e. Intentar comunicar con el responsable telefónicamente y en su defecto enviarle un mensaje de correo electrónico (SDP).
    f. Desconectar físicamente el equipo de la red (SAU), inhabilitarle la conexión de acceso o bloquearle el paso en los dispositivos de red (SDC).
2. Por parte del responsable
    a. Desconectar físicamente el ordenador de la red.
    b. Confeccionar el informe preliminar (según el modelo de la página web del SIC "Informe preliminar") y enviarlo a cert@ulpgc.es.
    c. Resolver la causa del incidente, sea desinfectando el equipo, desinstalando los programas afectados o cualquier otra configuración que proceda.
    d. Confeccionar el informe final (según modelo de la página web del SIC "Informe final") y enviarlo a cert@ulpgc.es.
3. Por parte del SIC
    a. Validar el informe preliminar recibido y si procede enviar la respuesta preliminar al organismo que remite la incidencia (SDP).
    b. Validar el informe final recibido y según proceda, notificarlo a la SDC, a la SAU y al organismo que remite la incidencia dando por cerrada la misma (SDP).
    c. Habilitar la conexión de acceso y el paso en los dispositivos de red al equipo (SDC) y si procede conectar físicamente el equipo de la red (SAU).

[1] SDP: Subdirección de Producción.
[2] SCD: Subdirección de Comunicaciones.
[3] SAU: Subdirección de Atención al Usuario