Tipo Incidente	¿Comunicar a los médios de comunicación? (SI/NO)	¿Por qué?
SPAM	No	No lo considero necesario, ya que aunque sea molesto, no presenta una amenaza significativa para la seguridad o integridad de los sistemas.
Pornografía infantil, contenido sexual o violento inadecuado	Sí	Ya que implica contenido ilegal y dañino que debe ser abordado públicamente para proteger a los usuarios.
Servidor C&C	Sí	Porque podría indicar la posible existencia de una red de bots o de un ataque coordinado que podría tener implicaciones significativas para la seguridad en línea.
Distribución de malware	Sí	Porque podría ayudar a alertar al público sobre la amenaza y proporcionar orientación sobre cómo protegerse.
Escaneo de redes (scanning)	No	Ya que el escaneo de redes es común y no necesariamente indica una violación de seguridad.
Ingeniería social	No	Ya que la ingeniería social es difícil de distinguir y puede implicar tácnicas de manipulación que podrían ser copiadas si se divulgan públicamente.
Explotación de vulnerabilidades conocidas	Sí	Ya que sería valioso para todos que se les informase sobre las vulnerabilidades que podrían estar siendo explotadas y saber cómo defenderse.
Intento de acceso con vulneración de credenciales	No	Porque la divulgación pública podría alertar a los atacantes y dificultar la contención del incidente.
Compromiso de cuenta con privilegios y sin privilegios	No	Por la misma razón anteiror, puede exponer la vulnerabilidad de un sistema y poner en riesgo la seguridad de la información sensible.
Compromiso de aplicaciones	Sí	Porque alertariamos a los usuarios sobre posibles riesgos relacionados con aplicaciones específicas.
Robo	Sí	Ya que la divulgación del robo de información confidencial puede ser necesaria para proteger a los usuarios afectados y coordinar una respuesta adecuada.
DoS	Sí	Para informar al público sobre posibles interrupciones en los servicios y proporcionar orientación sobre como mitigar los efectos del ataque.
Sabotaje	Sí	Para concienciar al público sobre posibles ataques dirigidos contra infraestructuras críticas
Interrupciones	Sí	Para informar al público sobre posibles interrupciones en los servicios y proporcionar orientación sobre como mitigar los efectos del incidente.
Modificación no autorizada de información	Sí	Para alertar a los usuarios sobre posibles compromisos de la integridad de los datos y promover medidas adicionales de seguridad y protección de la información.
Pérdida de datos	Sí	Ya que hay que informar a los usuarios sobre posibles riesgos para la privacidad y la seguridad de sus datos personales.
Phishing	Si	Para alertar al público sobre posibles intentos de fraude en línea y promover la concienciación sobre las tácticas de phishing.
Revelación de información	Sí	Sí, especialmente si implica información sensible o confidencial.
Ciberterrorismo	Sí	Debido a la gravedad y el impacto, es importante informar al público para promover la concienciación y preparación ante posibles amenazas.
Daños informáticos PIC	Sí	Especialmente si puede afectar a la disponibilidad o integridad de los sistemas informáticos.