PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

Índice

CONTROL DE REVISIONES

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	ELABORADO
1.0	Primera versión del documento	19/06/2020
2.0	Actualización del documento	24/03/2022
3.0	Se incorporan las medidas urgentes	19/09/2022
4.0	Actualización al RD311/2022	12/12/2023
5.0	Actualización tras NC	17/05/2024
6.0	Cambio de criterios de impacto potencial	01/07/2025

1 Objeto

El objeto de este procedimiento es definir la sistemática establecida por RADMAS TECHNOLOGIES para la gestión del ciclo de vida de incidentes de seguridad con el propósito de asegurar una respuesta eficaz y eficiente.

Se da así cumplimiento a las medidas de seguridad, establecidas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad:

- op.exp.7 Gestión de incidentes
- op.exp.9 Registro de la gestión de incidentes

Asimismo, se da cumplimiento al requisito establecido por el Reglamento General de Protección de Datos en lo relación con la comunicación de brechas de seguridad.

2 Alcance

Este procedimiento aplica a todos los sistemas y al personal que intervienen en la prestación de servicios de RADMAS TECHNOLOGIES, así como a todos aquellos que tengan acceso a los mismos.

3 Referencias

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (Reglamento General de Protección de Datos).
- Política de Seguridad de la Información de RADMAS TECHNOLOGIES.

4 Responsabilidades

Es responsabilidad del Responsable de Seguridad velar por el cumplimiento del presente procedimiento, realizando un seguimiento de los incidentes ocurridos.

Será responsabilidad de todos los usuarios:

- Notificar cualquier incidente de seguridad mediante los medios establecidos.
- Notificar cualquier debilidad en el sistema aunque esta todavía no haya dado lugar a un fallo de seguridad.

5 Procedimiento

5.1 Notificación de incidentes de seguridad

En el registro de incidentes se reflejan todos aquellos incidentes de seguridad que se detecten, entendiéndose por incidente de seguridad un suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información. Asimismo, se notificará si se detecta una vulnerabilidad o debilidad que pueda afectar a la seguridad de la información o de los servicios.

Todo usuario que detecte un incidente de seguridad o debilidad en los sistemas de información deberá notificarlo al Responsable del Sistema por vía telefónica, o correo electrónico, y se dan de alta en la aplicación de incidencias de la organización (Jira).

La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación.

Se dispone de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas.

5.2 Clasificación de los incidentes de seguridad

Dentro de incidentes de seguridad se tienen en cuenta los siguientes:

5.2.1 Contenido abusivo

Tipo de incidente	Descripción y ejemplos prácticos
Spam	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
Delito de odio	Contenido difamatorio o discriminatorio. Ej: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
Pornografía infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.

5.2.2 Contenido dañino

Tipo de incidente	Descripción y ejemplos prácticos
Sistema infectado	Sistema infectado con malware. Ej: Sistema, computadora o teléfono móvil infectado con un rootkit
Distribución de malware	Recurso usado para la distribución de malware. Ej: recurso de una organización empleado para distribuir malware.
Configuración de malware	Recurso que aloje ficheros de configuración de malware Ej: ataque de webinjects para troyano.

5.2.3 Obtención de información

Tipo de incidente	Descripción y ejemplos prácticos
Escaneo de redes (scanning)	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos.
Análisis de paquetes (sniffing)	Observación y grabación del tráfico de redes.
Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ej: mentiras, trucos, sobornos, amenazas.

5.2.4 Intento de intrusión

Tipo de incidente	Descripción y ejemplos prácticos
Explotación de vulnerabilidades conocidas	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).
Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ej: intentos de ruptura de contraseñas, ataque por fuerza bruta.
Ataque desconocido	Ataque empleando exploit desconocido.

5.2.5 Intrusión

Tipo de incidente	Descripción y ejemplos prácticos
Compromiso de cuenta con privilegios	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegios.
Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej: inyección SQL.
Robo	Intrusión física. Ej: acceso no autorizado a Centro de Proceso de Datos.

5.2.6 Disponibilidad

Tipo de incidente	Descripción y ejemplos prácticos
DoS (Denegación de servicio)	Ataque de denegación de servicio. Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
DDoS (Denegación distribuida de servicio)	Ataque de denegación distribuida de servicio. Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
Sabotaje	Sabotaje físico. Ej: cortes de cableados de equipos o incendios provocados. Sabotaje virtual. Ej: ejecución de código con intención de perjudicar a la empresa.
Interrupciones causas ajenas	Ej: desastre natural.
Interrupciones causas propias	Ej: Despliegues fallidos, bugs de código, intervención fallida de personal de sistemas, etc.

5.2.7 Compromiso de la información

Tipo de incidente	Descripción y ejemplos prácticos
Acceso no autorizado a información	Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
Modificación no autorizada de información	Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
Pérdida de datos	Ej: pérdida por fallo de disco duro o robo físico.

5.2.8 Fraude

Tipo de incidente	Descripción y ejemplos prácticos
Uso no autorizado de recursos	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.
Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej: Warez.
Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.

5.2.9 Vulnerable

Tipo de incidente	Descripción y ejemplos prácticos
Criptografía débil	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: servidores web susceptibles de ataques POODLE/FREAK.
Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej: DNS open-resolvers o Servidores NTP con monitorización monlist.
Servicios con acceso potencial no deseado	Ej: Telnet, RDP o VNC.
Revelación de información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej: SNMP o Redis.
Sistema vulnerable	Sistema vulnerable. Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.

5.2.10 Otros

Tipo de incidente	Descripción y ejemplos prácticos
Otros	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.

5.3 Impacto potencial

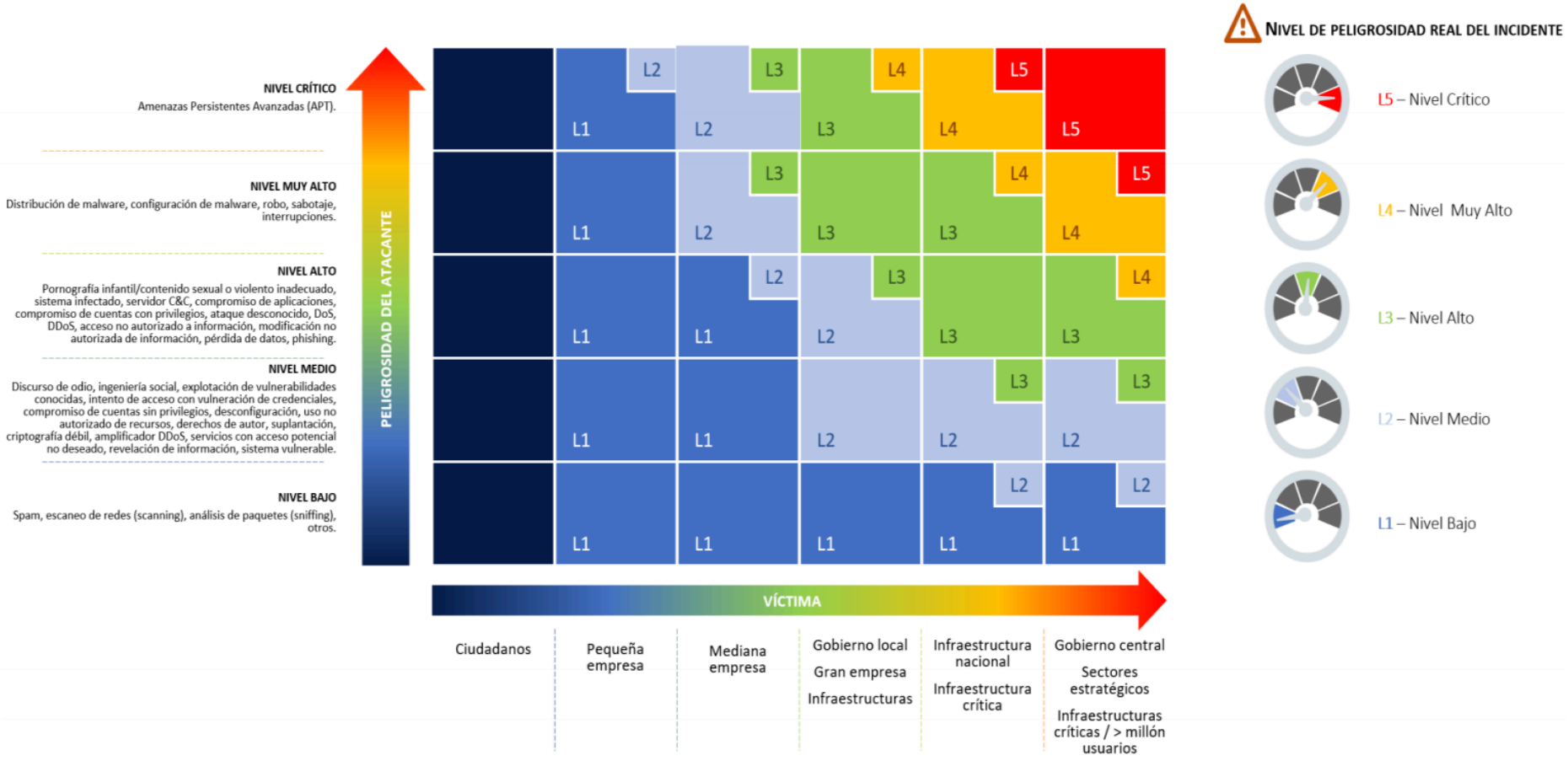
Se define impacto potencial como una estimación del daño que podría causar un incidente de seguridad. Se aplican los siguientes criterios para evaluar el impacto potencial de los incidentes de seguridad:

Nivel	Criterios
Sin impacto	• No hay ningún impacto apreciable.
Bajo	• Afecta a los sistemas de la organización. • Interrupción de la prestación de un servicio. • El ciberincidente precisa para resolverse menos de 1 Jornadas-Persona. • Impacto económico entre el 0,0001% y el 0,001% del P.I.B. actual. • Extensión geográfica superior a 1 CC.AA. • Daños reputacionales puntuales, sin eco mediático
Medio	• Afecta a más del 20% de los sistemas de la organización. • Interrupción en la presentación del servicio superior al 5% de usuarios. • El ciberincidente precisa para resolverse entre 1 y 5 Jornadas-Persona. • Impacto económico entre el 0,001% y el 0,03% del P.I.B. actual. • Extensión geográfica superior a 2 CC.AA. • Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).
Alto	• Afecta a más del 50% de los sistemas de la organización. • Interrupción en la prestación del servicio superior a 1 hora y superior al 10% de usuarios. • El ciberincidente precisa para resolverse entre 5 y 10 Jornadas–Persona. • Impacto económico entre el 0,03% y el 0,07% del P.I.B. actual. • Extensión geográfica superior a 3 CC.AA. • Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
Muy Alto	• Afecta a la seguridad ciudadana con potencial peligro para bienes materiales. • Afecta apreciablemente a actividades oficiales o misiones en el extranjero. • Afecta a un servicio esencial. • Afecta a sistemas clasificados RESERVADO. • Afecta a más del 75% de los sistemas de la organización. • Interrupción en la prestación del servicio superior a 8 horas y superior al 35% de los usuarios. • El ciberincidente precisa para resolverse entre 10 y 30 Jornadas-Persona. • Impacto económico entre el 0,07% y el 0,1% del P.I.B. actual. • Extensión geográfica superior a 4 CC.AA. o 1 T.I.S. • Daños reputacionales a la imagen del país (marca España). • Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.

Nivel	Criterios
Crítico	• Afecta apreciablemente a la Seguridad Nacional. • Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas. • Afecta a una Infraestructura Crítica. • Afecta a sistemas clasificados SECRETO. • Afecta a más del 90% de los sistemas de la organización. • Interrupción en la prestación del servicio superior a 24 horas y superior al 50% de los usuarios. • El ciberincidente precisa para resolverse más de 30 Jornadas-Persona. • Impacto económico superior al 0,1% del P.I.B. actual. • Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.

5.4 Peligrosidad del incidente

En el siguiente gráfico se muestra el nivel de peligrosidad, atendiendo a la repercusión de la materialización de la amenaza de que se trate, podría tener en los sistemas de información de las entidades del ámbito de aplicación del ENS:


NIVEL CRÍTICO
Amenazas Persistentes Avanzadas (APT).
NIVEL MUY ALTO
Distribución de malware, configuración de malware, robo, sabotaje, interrupciones.
NIVEL ALTO
Pornografía infantil/contenido sexual o violento inadecuado, sistema infectado, servidor C&C, compromiso de aplicaciones, compromiso de cuentas con privilegios, ataque desconocido, DoS, DDoS, acceso no autorizado a información, modificación no autorizada de información, pérdida de datos, phishing.
NIVEL MEDIO
Discurso de odio, ingeniería social, explotación de vulnerabilidades conocidas, intento de acceso con vulneración de credenciales, compromiso de cuentas sin privilegios, desconfiguración, uso no autorizado de recursos, derechos de autor, suplantación, criptografía débil, amplificador DDoS, servicios con acceso potencial no deseado, revelación de información, sistema vulnerable.
NIVEL BAJO
Spam, escaneo de redes (scanning), análisis de paquetes (sniffing), otros.
PELIGROSIDAD DEL ATACANTE
L1 L2 L3 L4 L5
VÍCTIMA
Ciudadanos
Pequeña empresa
Mediana empresa
Gobierno local
Gran empresa
Infraestructuras
Infraestructura nacional
Infraestructura crítica
Gobierno central
Sectores estratégicos
Infraestructuras críticas / > millón usuarios
NIVEL DE PELIGROSIDAD REAL DEL INCIDENTE
L5 – Nivel Crítico
L4 – Nivel Muy Alto
L3 – Nivel Alto
L2 – Nivel Medio
L1 – Nivel Bajo

5.5 Gestión y tratamiento de incidentes de seguridad

El técnico que registra el incidente en Jira, incluye como mínimo la siguiente información:

- **Resumen**: redacta un título breve y descriptivo que identifique claramente el suceso. Un buen resumen permite una rápida identificación de la incidencia.
- **Descripción**: en base al apartado "**5.2 Clasificación de los incidentes de seguridad**" de esta documentación, hay que indicar el tipo de incidente correspondiente dentro de la categoría de "Seguridad".
- **Impacto potencial**: en base al apartado "**5.3 Impacto potencial**" de esta documentación, hay que seleccionar el nivel que mejor represente la severidad del incidente. La regla es que el impacto potencial de un incidente se clasifica siempre según la consecuencia más grave que haya provocado o pueda provocar. Esto quiere decir que si un incidente cumple con criterios de varios niveles de impacto, siempre prevalecerá el más alto.
- **Información adicional**: especificar el número y el tipo de sistemas o activos de información que se han visto comprometidos con el incidente.
- **Responsable**: indica el usuario que recibió la notificación.
- **Dimensiones de seguridad afectadas**: indica qué pilares de la seguridad (confidencialidad, disponibilidad, integridad, datos personales, trazabilidad y autenticidad) se han visto comprometidos. Si las dimensiones de trazabilidad y autenticidad se ven afectadas, se considerará como un caso en que se encuentre afectada la integridad de la información.
- **Contexto y observaciones**: describe los efectos observados o las posibles consecuencias derivadas del incidente. Explica el "qué ha pasado" o "qué podría pasar".
- **Adjunto**: adjunta cualquier archivo que sirva como prueba o facilite la comprensión del incidente.
- **Comentarios del Jira**: después de crear la incidencia hay que indicar en los comentarios del ticket creado las acciones llevadas a cabo (si aplica) para solucionar el incidente y medidas para prevenir la repetición del incidente.

Una vez registrado el incidente, los propios técnicos del Responsable del Sistema, intentarán dar solución al mismo. Si consiguen solucionarlo, introducirán una descripción de las acciones realizadas y procederán a cambiar el estado del incidente a "Hecho" en el registro del incidente.

La gestión del incidente o la vulnerabilidad se iniciará con la identificación de las causas o posibles causas que dan lugar a las mismas, así como de los efectos por éstas producidos.

Se conservarán los registros asociados a los incidentes de, al menos, los tres últimos años.

5.6 Medidas urgentes

Ante incidentes considerados críticos para la seguridad del sistema, se tomarán las siguientes medidas urgentes:

- Detección del servicio
- Aislamiento del sistema afectado
- Recogida de evidencias
- Protección de los registros

RADMAS TECHNOLOGIES considerará incidentes críticos, aquellos incidentes considerados como prioritarios para el CCN-CERT:

- Incidentes que afecten a información clasificada
- Ciberespionaje: APTs, campañas de malware, incidentes especiales
- Interrupción de los Servicios IT
- Exfiltración de datos
- Existencia de algún servicio comprometido
- Toma de control de algún sistema
- Robo y publicación o venta de información sustraído
- Ciberdelito
- Suplantación de identidad

5.7 Recolección y custodia de evidencias

El Responsable del Sistema registra las tareas de análisis de los incidentes, las evidencias obtenidas durante los análisis y los resultados de éstos.

Otras Direcciones de RADMAS TECHNOLOGIES implicadas deberán recoger y mantener las evidencias que se recaben durante los análisis de forma que se asegure su precisión y completitud.

Adicionalmente, cuando se sospeche que los incidentes han sido consecuencia de actos maliciosos, a fin de garantizar su admisibilidad en juicio en caso de que se decidiese ejercitar acciones contra los

responsables de los incidentes, en la recolección de las evidencias se tomarán las siguientes precauciones:

- Se archivarán los originales de las evidencias en papel usando medios que eviten cualquier posibilidad de que sean modificados, reemplazados, sustraídos o destruidos de forma intencionada o no deseada, registrando:
    - La identidad y los datos de contacto de quienes los recogieron.
    - El lugar en que fueron encontrados.
    - La fecha y hora en la que fueron recogidos.
    - Los accesos autorizados que sean realizados dejando constancia de la identidad de quienes acceden a las evidencias, además de la fecha, hora y demás datos relevantes sobre los accesos realizados.
- Para la recopilación de evidencias de los sistemas informáticos se asegurará que:
    - Se realicen copias de los discos duros, memorias y soportes removibles de información en los que se hallen almacenadas las evidencias electrónicas (copias completas bit a bit).
    - Se recaben los registros de monitorización generados por los sistemas durante la realización de las copias.
    - Se archiven los registros originales de forma tal que se evite todo acceso que pudiera comprometer su integridad o disponibilidad.
    - Se realicen todas las actividades necesarias para determinar la causa y los responsables de los incidentes exclusivamente sobre las copias realizadas a partir de los originales, registrando la identidad y los datos de contacto de las personas que realicen y presencien las mismas, todos los pasos dados y los recursos empleados.

5.8 Comunicación a lNCIBE

Cuando se haya determinado que el incidente tiene nivel de Peligrosidad o Impacto Alto, Muy Alto o Crítico, de acuerdo con los criterios previstos en el **apartado 5.4** del presente procedimiento, el Responsable de Seguridad deberá notificar a INCIBE, a los clientes afectados y coordinar la comunicación a INCIBE/CCN con cada cliente.

La notificación se realizará a través del formulario de INCIBE: https://www.incibe.es/protege-tu-empresa/reporta-tu-incidente

5.9 Comunicación al Centro Criptológico Nacional

Cuando se haya determinado que el incidente tiene nivel de impacto potencial Alto, Muy Alto o Crítico, de acuerdo con los criterios previstos en el **apartado 5.3** del presente procedimiento, el Responsable de Seguridad deberá notificar a los clientes que sean administraciones públicas afectados tales circunstancias y coordinar la comunicación al CCN con cada cliente, siempre que sea posible a través de la plataforma LUCIA suministrada por el CCN.

En el caso de que se acuerde con el cliente que sea **RADMAS** quien realice la comunicación al CCN, el Responsable de Seguridad enviará un correo electrónico a la dirección incidentes@ccn-cert.cni.es indicando:

- Descripción lo más detallada posible del incidente.
- La información de contacto (al menos una dirección de correo y un teléfono).

El correo electrónico debe enviarse cifrado utilizando las claves PGP/GPG disponibles en https://www.ccn-cert.cni.es/sobre-nosotros/contacto.html.

5.10 Comunicación de brechas de seguridad de datos personales

En aplicación del Reglamento General de Protección de Datos, cuando se produzca un incidente de seguridad que suponga una violación de la seguridad de los datos personales, contactaremos con las abogadas expertas en protección de datos para que nos orienten en las acciones a realizar.

El contacto es el siguiente:

- Marta Sagüillo
  - marta.saguillo@dataprolegal.com
  - 659338342
- Cristina González
  - cristina.gonzalez@dataprolegal.com
  - 659338342

En cualquier caso, de forma general, es necesario considerar dos tipos de comunicaciones:

- Comunicación a la Agencia Española de Protección de Datos.
- Comunicación a los interesados afectados.

En cualquier caso, independientemente de los análisis realizados, el incidente deberá ponerse en conocimiento de los clientes de **RADMAS** afectados, proporcionando la información sobre el mismo, y atendiendo a lo previsto en los correspondientes contratos de encargado del tratamiento sobre la responsabilidad de la comunicación de los incidentes o brechas de seguridad.

Para determinar la necesidad de realizar comunicaciones, el responsable de seguridad de **RADMAS**, considerará los siguientes factores:

1. Volumen de datos afectados:
    a. Valor 1: Menos de 100 registros
    b. Valor 2: Entre 101 y 1.000 registros
    c. Valor 3: Entre 1.001 y 100.000 de registros
    d. Valor 4: Entre 100.000 de registros
    e. Valor 5: Más de 1.000.000 de registros
2. Tipología de datos afectados:
    f. Valor 1: datos no sensibles.
    g. Valor 2: datos sensibles.
3. Impacto (Exposición):
    h. Valor 2: Nulo.
    i. Valor 4: Interno, dentro de la empresa, controlado.
    j. Valor 6: Externo.
    k. Valor 8: Pública, accesible en internet.
    l. Valor 10: Desconocido.

Una vez determinados los factores anteriores, el Responsable de Seguridad o en su caso la persona responsable de la protección de datos personales, procede a calcular el riesgo de la brecha de seguridad de acuerdo a la siguiente fórmula:

Riesgo = Volumen x (Tipología x Impacto).

Se aplica la siguiente política de comunicación:

- Comunicación a la Agencia Española de Protección de Datos cuando se cumplan las dos condiciones siguientes:
    - Riesgo superior a 20.
    - Se dan dos, o más, de las siguientes circunstancias:
        - Se han visto afectados más de 100.000 registros.
        - Se han visto afectados datos sensibles.
        - El impacto es externo, público o desconocido.
- Comunicación a los interesados cuando se cumplan las dos condiciones siguientes:
    - Riesgo superior a 40.
    - Se dan dos, o más, de las siguientes circunstancias:
        - Se han visto afectados más de 100.000 registros.
        - Se han visto afectados datos sensibles.

- El impacto es externo, público o desconocido.

5.11 Comunicación a la Agencia Española de Protección de Datos

Si se cumplen las condiciones indicadas anteriormente, el Responsable de Seguridad o persona responsable de la protección de datos de **RADMAS** notificará la brecha de seguridad a la Agencia Española de Protección de Datos sin dilación indebida y, a más tardar en 72 horas después de que haya tenido constancia de ella.

La notificación a la AEPD se realizará a través del formulario destinado a tal efecto publicado en la sede electrónica de la agencia, en https://sedeagpd.gob.es/sede-electronica-web/.

5.12 Comunicación a los interesados afectados

Si se cumplen las condiciones indicadas anteriormente, el Responsable de Seguridad o persona responsable de la protección de datos de **RADMAS**, gestionará la comunicación a los interesados afectados, sin dilación indebida, de la siguiente información:

a) Identificación y datos de contacto del Responsable de Seguridad o persona responsable de la protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

b) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

c) Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

La comunicación a los interesados no será necesaria si se cumple alguna de las siguientes condiciones:

a) Se han adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.

b) Se han tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado.

c) Supone un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

No obstante, esta comunicación deberá realizarse de manera coordinada con los clientes de **RADMAS** afectados.

Las direcciones de correo electrónico habilitadas por cada cliente son:

- Quirónsalud: of.ciberseguridad@quironsalud.es
- Telefónica: comunicacion.brechas@telefonica.com
- IAM: lozanorj@madrid.es

6 Anexos

- N/A