Violaciones de seguridad de datos personales

1. Introducción

El Reglamento Europeo de Protección de Datos establece las obligaciones de las Administraciones responsables relativas a las violaciones o los incidentes de seguridad.

Por medio del protocolo que se presenta a continuación, se pretenden indicar las actuaciones a seguir por parte del responsable de tratamiento cuando los datos de carácter personal que obran en su poder sufran una violación o quiebra de seguridad, así como los requisitos y condiciones necesarias que deben cumplir cada una de estas actuaciones. Este protocolo está elaborado teniendo en cuenta, además de la normativa de aplicación, la "Guía para la gestión y notificación de brechas de seguridad" de la AEPD, en colaboración con el Centro Criptológico Nacional y el Instituto Nacional de Ciberseguridad, la "Guía de Implantación del ENS para Entidades Locales", del Centro Criptológico Nacional, de mayo de 2019 y otros materiales objeto de difusión a través de *www.incibe.es* y *www.ccn-cert.cni.es*.

Toda Administración responsable debe estar preparada para detectar las quiebras de seguridad que puedan ocurrir, y por ello debe aplicar mecanismos

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

de detección apropiados y suficientes para valorar convenientemente el incidente de seguridad.

El RGPD define las "violaciones de seguridad de los datos personales" como *"todas aquellas violaciones de seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos"*. Por otro lado, el Esquema Nacional de Seguridad, Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS), define incidente de seguridad como aquel *"suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información"*. Además, el Grupo de Trabajo del Artículo 29 (WP29) incide en que la referencia del RGPD se aplica en la medida en que afecte a datos de carácter personal, y en consecuencia dicho incidente pueda comprometer al responsable en el cumplimiento de los principios relativos al tratamiento de los datos, de manera que no todos los incidentes de seguridad son necesariamente brechas de datos personales.

De cada violación de la seguridad de los datos de carácter personal se recabarán los datos a los que se refiere el apartado "Gestión de las brechas de seguridad".

El RGPD establece la obligación, en determinadas circunstancias, de notificar la violación de seguridad a la autoridad de control competente en materia de protección de datos, y, en su caso, también a las personas afectadas. La comunicación a la autoridad de control no debe entenderse como "una inculpación" ante la misma por una posible falta de diligencia en el adecuado tratamiento de los datos, sino, por el contrario, como una muestra del ejercicio de la responsabilidad proactiva del responsable, que permite a dicha autoridad conocer los posibles ataques de seguridad que se pudieran estar produciendo y qué debilidades se están explotando para, de esta forma, poder realizar actuaciones de divulgación y de prevención contra los mencionados ataques.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

2. Protocolo de actuación ante violaciones de seguridad

2.1. Gestión de las brechas de seguridad

2.1.1. Detección, identificación y clasificación

Para detectar un incidente de seguridad, la entidad debe concretar aquellas situaciones que suponen una quiebra de seguridad y son posibles de detectar, bien mediante herramientas o sistemas de alerta, como mecanismos internos que involucran al personal y que lo posibilitan, tales como sistemas de videovigilancia, control y registro de acceso a determinados departamentos o zonas, bien a través de fuentes externas, como puede ser la comunicación del incidente por parte de un tercero, por ejemplo un prestador de servicios, un llamante, etc. Estos mecanismos permitirán a la entidad identificar un incidente de seguridad.

Asimismo, puede darse el caso de que sea un encargado del tratamiento el que detecte la existencia de una violación de seguridad, y, de acuerdo con el contrato de prestación de servicios o acto jurídico que regule la relación, tiene la obligación de notificar al responsable, sin dilación indebida, las violaciones de seguridad de los datos personales de las que tenga conocimiento.

A partir de la detección y posterior identificación de la brecha de seguridad, el responsable del tratamiento debe determinar si se encuentra ante una violación de la seguridad de los datos. Para ello, se analizan la naturaleza, la clase y el tipo de incidente, y si el mismo constituye una "brecha de los datos de carácter personal".

Para llevar a cabo la clasificación, la entidad tendrá en cuenta los siguientes aspectos:

- ✓ El tipo de amenaza, incluyendo una descripción de la misma.
- ✓ El origen interno o externo de la misma.
- ✓ La categoría de seguridad de los sistemas y datos afectados.
- ✓ El perfil de usuarios afectados.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

- ✓ Número y tipología de los sistemas afectados.

- ✓ Impacto del incidente en la Administración responsable y en los derechos y las libertades de los afectados.

- ✓ Medio por el que se ha materializado el incidente.

Las brechas de seguridad, tal y como se establece en la Guía para la gestión y notificación de brechas de seguridad de la AEPD, se clasifican en:

- ✓ Brecha de confidencialidad: "La severidad de la pérdida de confidencialidad varía según el alcance de la divulgación, es decir, el número potencial y el tipo de partes que pueden haber accedido ilegalmente a la información".

- ✓ Brecha de integridad: "se produce cuando se altera la información original y la sustitución de datos puede ser perjudicial para el individuo".

- ✓ Brecha de disponibilidad: "se produce al no poder acceder a los datos originales cuando es necesario".

2.1.2. Registro y valoración

Una vez identificada la existencia de la violación de seguridad, será documentada e incluirá en ese registro los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas, de acuerdo con lo establecido en el art. 33 RGPD.

Asimismo, la entidad debe valorar el incidente de seguridad, a los efectos de determinar la peligrosidad potencial del mismo, para lo cual deberán tenerse en cuenta los siguientes factores:

- ✓ La categoría o el nivel de criticidad respecto a la seguridad de los sistemas afectados:
  - Crítico, si afecta a datos valiosos, gran volumen y en poco tiempo.
  - Muy alto, cuando dispone de capacidad para afectar a información valiosa, en cantidad apreciable.
  - Alto, si afecta a información valiosa.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

- Medio, si afecta a un volumen apreciable de información.
- Bajo, si de forma escasa o nula capacidad afecta a un volumen apreciable de información.

✓ Naturaleza, sensibilidad y categorías de los datos personales afectados:

- Datos de escaso riesgo: datos de contacto e identificativos.
- Datos de comportamiento: localización, hábitos y preferencias.
- Datos financieros: transacciones, posiciones, ingresos, cuentas, facturas, etc.
- Datos sensibles: de salud, biométricos, datos relativos a la vida sexual, etc.
- Datos legibles/ilegibles: Datos protegidos mediante algún sistema de seudonimización, por ejemplo, cifrado o *hash*.

✓ Volumen de datos personales: expresados en cantidad, tales como registros, ficheros, documentos, y/o en periodos de tiempo.

✓ Facilidad de identificación de individuos: facilidad con la que se puede deducir la identidad de los individuos a partir de los datos involucrados en la brecha.

✓ Severidad de las consecuencias para los individuos:

- Baja: Las personas no se verán afectadas.
- Media: Las personas pueden encontrar inconvenientes importantes.
- Alta: Las personas pueden enfrentar consecuencias importantes.
- Muy alta: Las personas pueden enfrentar consecuencias significativas.

✓ Características especiales de los individuos: Si afectan a individuos con características especiales o con necesidades especiales.

✓ Número de individuos afectados.

✓ El perfil de los usuarios afectados, su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

- ✓ El número y tipología de los sistemas afectados.

- ✓ El impacto que la brecha puede tener en la Administración, desde los puntos de vista de la protección de la información, la prestación de los servicios, la conformidad legal y/o la imagen pública:
  - Bajo
  - Medio
  - Alto

- ✓ Valoración, que supone un comentario del responsable, así como la determinación sobre su notificación a la autoridad de control.

2.2. Notificación de la violación a la autoridad de control competente

2.2.1. Obligación de notificar la violación de la seguridad

Si no se toman a tiempo medidas adecuadas, las violaciones de seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio social o económico significativo para la persona física en cuestión.

La notificación de la violación de seguridad a la autoridad de control competente se realizará, por parte del responsable del tratamiento, por el medio que cada una de ellas hubiera dispuesto.

En el caso de la AEPD se realiza a través de su sede electrónica (*https://sedeagpd.gob.es/sede-electronica-web*), siguiendo el formulario electrónico oficial dispuesto a tal efecto, y contendrá la siguiente información:

- Descripción de la naturaleza de la violación de la seguridad.
- Datos identificativos y de contacto de la entidad, así como del delegado de protección de datos, e indicación de si la notificación es completa o parcial, en cuyo caso se señalará si se trata de la primera notificación o de una complementaria.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

- Fecha y hora de la violación de seguridad.
- Pérdida de control sobre los datos personales.
- Restricción de los derechos.
- Discriminación.
- Usurpación de identidad.
- Pérdidas financieras.
- Reversión no autorizada de la seudonimización.
- Daño para la reputación.
- Pérdida de la confidencialidad de los datos sujetos al secreto profesional.
- Cualquier otro perjuicio económico o social significativo para la persona física.

A cada notificación, le será asignada por la AEPD una referencia con el fin de proporcionar un seguimiento completo del incidente.

Para el caso de que la violación de seguridad pueda afectar a los datos de personas en más de un Estado miembro de la Unión Europea, la entidad notificará, como mínimo, a la autoridad de control local donde el incidente tuviese lugar. Además, la autoridad de control principal será la del establecimiento principal del responsable, es decir, la Agencia Española de Protección de Datos.

Razones para no notificar la violación de seguridad

Como regla general, la entidad notificará a la autoridad de control competente las violaciones de la seguridad; no obstante, en caso de que pueda demostrar, de forma fehaciente y atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas, no es necesario realizar dicha notificación.

En base a lo anteriormente expuesto, el responsable no tendrá que notificar a la autoridad de control competente la violación de seguridad:

- Cuando sea improbable que la vulneración de los datos personales constituya un riesgo para los derechos y las libertades de los interesados.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

- Esta improbabilidad debe basarse, atendiendo al principio de responsabilidad proactiva, en la capacidad del responsable del tratamiento de demostrar el cumplimiento de todos los principios del tratamiento, tales como la licitud, la limitación de los fines, la minimización de los datos, la exactitud, la limitación del plazo de conservación, la integridad y la confidencialidad de los mismos.

2.2.2. Plazo para la notificación de la violación de seguridad a la autoridad de control competente

Tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales debe, sin dilación indebida, y a más tardar en un plazo de 72 horas desde que se haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente.

Sintetizando, debe notificarse la violación de seguridad a la autoridad de control:

- Sin dilación indebida.
- Máximo de 72 horas desde que se haya tenido constancia.
- Pasadas las 72 horas, se deberá acompañar de una justificación motivada de los motivos de la dilación.

2.2.3. Contenido de la notificación de la violación de seguridad a la autoridad de control competente

La notificación de la violación de seguridad a la autoridad de control contendrá la siguiente información:

- Una descripción de la naturaleza de la violación de la seguridad.
- Los datos identificativos y de contacto del responsable.
- La fecha y hora de la violación de seguridad.
- Las circunstancias en las que se ha producido el incidente de seguridad (si ha tenido lugar como consecuencia de una pérdida de datos, de un acceso no autorizado a los mismos, etc.).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

- Una descripción de la naturaleza y las circunstancias de la violación de la seguridad.
- Las categorías y el número aproximado de interesados, cuando sea posible.
- Las categorías y el número aproximado de registros de datos personales afectados, cuando sea posible.
- Una descripción de sus consecuencias y de las medidas adoptadas o propuestas por el responsable de tratamiento para poner remedio a la violación, incluyendo las medidas adoptadas para mitigar los posibles efectos negativos, si es posible.
- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- La indicación de si la notificación es completa o parcial, en cuyo caso se señalará si se trata de la primera o de una complementaria.
- En caso de existir, posibles cuestiones de carácter transfronterizo, indicando la posible necesidad de notificación a otras autoridades de control.

Las notificaciones deberán ser claras, concisas, e incluir la información necesaria para que la autoridad de control pueda analizarlas adecuadamente.

El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de las obligaciones inherentes al responsable en materia de violaciones de la seguridad. Por ello, la Administración responsable trabaja para establecer procedimientos de respuesta ante las quiebras de seguridad, vinculados a las políticas de seguridad de la información y protección de datos, que requieren su difusión entre todos los trabajadores con el objetivo de que estén informados de cómo proceder ante una brecha de seguridad.

Si no es posible facilitar toda la información en una comunicación, se notificará por etapas, sin dilación indebida.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

2.3. Comunicación de la violación de la seguridad al interesado

2.3.1. Obligación de notificar la violación de la seguridad al interesado

La entidad debe comunicar al interesado sin dilación indebida la violación de seguridad de los datos personales, en caso de que pueda entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. Dichas comunicaciones deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

En conclusión, notificar la violación de seguridad al interesado será obligatorio:

- Para cualquier responsable de tratamiento, cuando sea probable que presente un alto riesgo para los derechos y las libertades del interesado.
- Cuando al responsable de tratamiento le sea exigido por la autoridad de control, debiendo seguir sus instrucciones o las de otras autoridades competentes.

Asimismo, existen otra serie de factores a valorar para determinar la necesidad de comunicación de la brecha de seguridad a los afectados:

- La existencia de obligaciones legales o contractuales al respecto.
- Los riesgos que comporta la pérdida de los datos.
- La existencia de un riesgo razonable de suplantación de identidad o fraude.
- Hasta qué punto puede el afectado evitar o minimizar daños posteriores.

En cuanto a la forma en que la entidad debe llevar a cabo la comunicación a los interesados, preferentemente se realizará de forma directa a través de teléfono, con grabación de llamada, correo electrónico, correo postal, o a través de cualquier otro medio dirigido al afectado que resulte adecuado y probatorio.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

Asimismo, también es posible la notificación indirecta, mediante avisos públicos en sitios web, blogs corporativos, comunicados de prensa, siempre y cuando la notificación directa suponga un alto costo o no sea posible contactar con las personas afectadas.

Razones para no notificar la violación de seguridad al interesado

La comunicación al interesado de la violación de la seguridad no será necesaria cuando la entidad haya adoptado medidas de protección técnicas y organizativas apropiadas, y estas medidas hayan sido aplicadas a los datos personales afectados por la violación de la seguridad; en particular: cuando se hayan aplicado aquellas medidas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como, por ejemplo, el cifrado; cuando el responsable haya tomado medidas ulteriores que garanticen la ausencia de alto riesgo para los derechos y las libertades del interesado; y cuando la notificación de la violación de la seguridad a este suponga un esfuerzo desproporcionado para el responsable, en cuyo caso se optará por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

En definitiva, el responsable estará exento de notificar la violación de la seguridad al interesado:

- Cuando se hayan adoptado medidas técnicas y organizativas apropiadas de protección para hacer ininteligibles los datos a personas no autorizadas y estas se hayan aplicado a los datos afectados.
- Cuando se hayan tomado medidas posteriores que garanticen que ya no sea probable un alto riesgo para los derechos y las libertades del interesado.
- Cuando supusiera un esfuerzo desproporcionado. En este caso, se podrá optar por una comunicación pública que sea igualmente efectiva para informar al interesado.

Si el responsable todavía no ha comunicado al afectado la brecha de la seguridad de los datos personales considerando el alto riesgo potencial, la autoridad de control podrá exigirle:

- Que lo comunique.
- Que se cumpla alguna de las condiciones mencionadas para que la comunicación a los afectados no sea obligada.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

2.3.2. Plazo para la notificación al interesado de la violación de la seguridad

La entidad debe comunicar al interesado sin dilación indebida la violación de seguridad de los datos personales, en caso de que pueda entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias.

2.3.3. Contenido de la notificación de violación de seguridad al interesado

La comunicación al interesado debe describir, en un lenguaje claro y sencillo:

- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Una descripción general del incidente y momento en que se ha producido.
- Las posibles consecuencias de la brecha de la seguridad de los datos personales.
- Una descripción de los datos y la información personal afectados.
- Un resumen de las medidas implantadas hasta el momento para controlar los posibles daños.
- Cualquier otra información útil para proteger los datos de los afectados o prevenir posibles daños.

2.4. Notificación de la violación de seguridad al CCN-CERT

Además de la obligatoriedad de la notificación de los incidentes de seguridad a la autoridad de control y a los interesados en los casos previstos legalmente y explicados a lo largo del presente documento, las Administraciones públicas pueden tener la obligación de notificar al CCN-CERT sus incidentes de seguridad de la información con o sin datos personales, si bien dicha comunicación puede realizarse a través de otros centros autonómicos o de otro ámbito.

El CCN-CERT es el servicio de Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia (CNI). Entre sus funciones se encuentra la de colaborar con los organismos públicos y las empresas de interés estratégico

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

en la detección, notificación, evaluación, respuesta, tratamiento y aprendizaje de incidentes de seguridad de información o ciberincidentes que puedan sufrir sus sistemas, ofreciendo apoyo técnico y operativo, y poniendo a la Administración pública responsable en contacto con otros sitios involucrados en el mismo incidente.

En este sentido, y a pesar de contar con grandes infraestructuras de seguridad, las Administraciones públicas no pueden garantizar que una intrusión no afecte a sus equipos y, por tanto, a los datos personales de los que son responsables. De este modo, además de las fases del proceso de respuesta a brechas de seguridad, que se analizarán en el siguiente epígrafe, la capacidad del CCN-CERT de coordinar e intercambiar información con los organismos adecuados ayudará a la capacidad de respuesta de la Administración responsable frente a los incidentes de seguridad. Asimismo, resultará útil de cara a prevenir futuros incidentes, ya que el ente responsable podrá utilizar la información obtenida con este objetivo.

2.4.1. Sujetos obligados

Los siguientes sujetos estarán obligados a notificar al CCN-CERT los incidentes de seguridad que se produzcan en el seno de su organización:

- La Administración General del Estado.
- Las Administraciones de las comunidades autónomas.
- Las entidades que integran la Administración local.
- El sector público institucional, incluyéndose en él los organismos públicos y las entidades de derecho público vinculadas o dependientes de las Administraciones públicas, las entidades de derecho privado vinculadas o dependientes de las Administraciones públicas y las universidades públicas.

2.4.2. Obligación de notificar

Una vez detectado un incidente se utilizará la Guía *CCN-STIC 817. Esquema Nacional de Seguridad. Gestión de Ciberincidentes*, la cual se puede encontrar en el apartado "Guías" de la página web del CCN-CERT (*https://www.ccn-cert.cni.es*), a los efectos de clasificarlo de acuerdo con su tabla *Criterios de determinación del Nivel de Impacto Potencial*, que incluye los siguientes niveles:

- **Irrelevante**:
  - No hay impacto apreciable sobre el sistema.
  - No existen daños reputacionales apreciables.

- **Bajo**:
  - La categoría más alta de los sistemas de información afectados es básica.
  - El incidente precisa para resolverse menos de 1 jornada-persona.
  - No existen más que daños reputacionales puntuales, sin eco mediático.

- **Medio**:
  - La categoría más alta de los sistemas de información afectados es media.
  - Afecta a más de 10 equipos con información cuya máxima categoría es básica.
  - El incidente precisa para resolverse entre 1 y 10 jornadas-personas.
  - Existen daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).

- **Alto:**
  - La categoría más alta de los sistemas de información afectados es alta.
  - Afecta a más de 50 equipos con información cuya máxima categoría es básica.
  - Afecta a más de 10 equipos con información cuya máxima categoría es media.
  - El incidente precisa para resolverse entre 10 y 20 jornadas-personas.
  - 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 sistemas clasificados como reservados.
  - Afecta a más de 100 equipos con información cuya máxima categoría es básica.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

- Afecta a más de 50 equipos con información cuya máxima categoría es media.
- Afecta a más de 10 equipos con información cuya máxima categoría es alta.
- El incidente precisa para resolverse entre 20 y 50 jornadas-personas.
- Daños reputacionales a la imagen del país (marca España).
- Afecta apreciablemente a actividades oficiales o misiones en el extranjero.
- Afecta apreciablemente a una infraestructura crítica.

• **Crítico**:

- Afecta a sistemas clasificados como secretos.
- Afecta a más de 100 equipos con información cuya máxima categoría es media.
- Afecta a más de 50 equipos con información cuya máxima categoría es alta.
- Afecta a más de 10 equipos con información clasificada como reservada.
- El incidente precisa para resolverse más de 50 jornadas-personas.
- Afecta apreciablemente a la seguridad nacional.
- Afecta gravemente a una infraestructura crítica.

Una vez determinado el nivel de impacto potencial del incidente, se procederá a notificarlo al CCN-CERT, siempre y cuando el mismo se encuentre en uno de los siguientes niveles:

• Alto

• Muy alto

• Crítico

2.4.3. Legitimación para el tratamiento de los datos

Las autoridades públicas competentes, como pueden ser la AEPD o las agencias de protección de datos autonómicas, los equipos de respuesta a emergen-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

cias informáticas (CERT), los equipos de respuesta a incidentes de seguridad informática (CSIRT), así como los proveedores de redes y servicios de comunicaciones electrónicas y de tecnologías y servicios de seguridad, están legitimados para tratar los datos personales contenidos en las notificaciones de las violaciones de seguridad.

Esta legitimación se extiende única y exclusivamente durante el tiempo y alcance necesario para su análisis, detección, protección y respuesta ante incidentes, y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

2.4.4. Remisión de estadísticas

El registro de todos los incidentes de seguridad que se produzcan y de las acciones de tratamiento que se sigan será utilizado para la mejora continua de la seguridad del sistema, a cuyo fin los sujetos obligados elaborarán estadísticas de incidentes de seguridad que, al menos con carácter anual, remitirán al CCN.

2.5. Herramienta LUCIA

LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) es la herramienta que el CCN-CERT pone a disposición de los sujetos obligados para gestionar los incidentes de seguridad.

Esta herramienta está basada en el sistema de incidencias *Request Tracker* (RT) y en su extensión para equipos de respuesta a incidentes *Request Tracker for Incident Response* (RT-IR), que han sido personalizados para cumplir los requerimientos y procedimientos del CCN-CERT y se encuentran alineados con el cumplimiento del Esquema Nacional de Seguridad (ENS).

El propósito de LUCIA es automatizar los mecanismos de notificación, comunicación e intercambio de información sobre incidentes de seguridad, ofreciendo para ello un lenguaje común de peligrosidad y clasificación del incidente, y manteniendo la trazabilidad y el seguimiento del mismo.

Asimismo, la herramienta permite automatizar las tareas e integrarse con otros sistemas ya implantados.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

A través de LUCIA, el organismo responsable puede gestionar tres tipos de ciberincidentes:

- Los propios del organismo.
- Los provenientes del Sistema de Alerta Temprana de Red SARA (SAT-SARA).
- Los provenientes del Sistema de Alerta Temprana de Internet (SAT-INET).

Para más información y acceso al manual de usuario de la herramienta, se debe acudir al siguiente enlace: *https://www.ccn-cert.cni.es/soluciones-seguridad/lucia.html*

2.6. Respuestas a brechas de seguridad

Una vez detectado e identificado un incidente de seguridad, la entidad deber dar respuesta al mismo, procediendo a su contención en un primer momento y a su solución con posterioridad, para finalizar con la adopción de las acciones de recuperación correspondientes.

2.6.1. Contención de la brecha de seguridad

La contención del incidente es el primer paso dentro de las fases de respuesta al incidente de seguridad. Básicamente, se trata de procurar detener la situación que está generando la brecha de seguridad a través de la adopción de una serie de medidas ágiles, que proporcionen tiempo a la Administración responsable para definir una estrategia de respuesta. Lógicamente, si existe una estrategia previa definida por parte del responsable para cada tipo de incidente, las medidas a aplicar en cada caso concreto serán mucho más fáciles de adoptar.

Las medidas de contención podrán ser aplicadas directamente por el usuario, o bien quedar en manos de personal especializado, dependiendo de la complejidad técnica de las mismas. También podrán ser de aplicación inmediata o progresiva, en función de la tipología del incidente.

Algunos ejemplos de medidas de contención a adoptar de modo inmediato, según el caso, serían los siguientes:

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

- Si un usuario detecta archivos con caracteres extraños en un equipo informático, desconectar rápidamente el cable de red y notificar la incidencia.
- Si se sospecha un acceso no autorizado, cambiar las contraseñas de acceso a los sistemas y equipos informáticos.

Asimismo, la contención del incidente proporcionará a la Administración responsable tiempo para desarrollar una estrategia de respuesta apropiada al incidente de seguridad en cuestión.

2.6.2. Erradicación de la brecha de seguridad

Tras la contención de la brecha de seguridad, se procederá a la erradicación de la misma, describiéndose de manera extensiva las tareas a realizar y la responsabilidad de cada una de ellas, y fijándose un plazo temporal para la implementación de las mismas.

Algunas tareas de erradicación serán las siguientes:

- Análisis completo de los equipos informáticos, discos duros y memorias con antivirus.
- Comprobación de la integridad de los datos almacenados en el sistema, a través de un sistema que garantice que no han sido modificados, como un sistema de *hashes*.
- Restauración paulatina de conexiones.

Una vez llevadas a cabo las mismas, la Administración responsable procederá a la verificación de su correcto funcionamiento, con el objeto de determinar su idoneidad, y finalmente tomará las medidas necesarias para garantizar que las vulnerabilidades explotadas no vuelvan a serlo, esto es, que procuren garantizar la no repetición del incidente de seguridad en el futuro.

2.6.3. Recuperación

El objetivo de esta fase es el restablecimiento del servicio en su totalidad, confirmando su normal funcionamiento y evitando la repetición de nuevos incidentes basados en la misma causa.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

Para ello, además de medidas activas, se podrán implementar controles periódicos en la Administración responsable para el seguimiento detallado de los procesos de mayor riesgo.

2.6.4. Recopilación de evidencias

En esta fase, la entidad debe documentar todo el proceso de respuesta, por ser necesario para posibles comunicaciones, de naturaleza tanto interna como externa, así como para la elaboración de un informe de respuesta, que se detallará en el siguiente punto.

Con este objetivo, será necesario:

- De cara a la recolección de evidencias: determinar previamente en la fase de detección la necesidad de uso de la información.
- Establecer la cadena de custodia adecuada al uso de la información.

Por su parte, y en relación con los incidentes de seguridad de nivel alto-muy alto resulta obligatorio proceder, tras su detección y con carácter inmediato, a recopilar las evidencias del incidente, documentándolas y custodiándolas de forma que se pueda determinar el modo de obtención y se garantice la cadena de custodia.

En estos casos, debe mantenerse un registro exhaustivo de las evidencias, que deberá incluir:

- Identificación de la información (por ejemplo, número de serie o de modelo de los equipos afectados, dirección IP de los ordenadores afectados, etc.).
- Nombre, cargo y teléfono de cada persona que haya recogido o gestionado evidencias durante la investigación del incidente.
- Fecha y hora de cada ocasión en la que haya sido tratada cada evidencia.
- Ubicaciones donde se custodiaron las evidencias.

Resultará fundamental comenzar la recopilación de evidencias tan pronto como el incidente sea detectado.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

Finalmente, la Administración responsable deberá aprobar unas normas sobre la custodia de evidencias en caso de ciberaccidente que tengan en cuenta los siguientes factores:

- **Persecución del delito**: la entidad debe custodiar adecuadamente las pruebas en caso de que se trate de un delito perseguible, hasta que se hayan completado todas las acciones legales.
- **Retención de datos**: los entes responsables deben mantener políticas de retención de datos que determinen cuánto tiempo pueden conservarse ciertos tipos de datos, respetando la legislación vigente.
- **Coste de la custodia**: se deberá tener en cuenta el coste de la custodia de los elementos físicos que puedan contener evidencias, como por ejemplo discos duros.

2.6.5. Comunicación/Informe de resolución

2.6.5.1. Comunicación

La comunicación debe ser continua a lo largo del proceso de respuesta a las brechas de seguridad, de manera que tanto la dirección como los responsables de seguridad puedan formarse una idea clara y concreta del incidente, para poder cumplir con sus propias obligaciones.

2.6.5.2. Informe de resolución

El informe de resolución tiene naturaleza interna y su objetivo es servir de base para la realización en el futuro de ejercicios de "lecciones aprendidas".

La forma del mismo debe seguir la línea temporal de los hechos, de manera que se puedan comprobar fácilmente las acciones y medidas adoptadas.

En él, deberán incluirse, como mínimo, los siguientes aspectos:

- Alcance e impacto del incidente.
- Existencia de controles preventivos y descripción de los mismos.
- Medidas adoptadas para la solución de la brecha.
- Medidas adoptadas tomadas para evitar futuros incidentes de seguridad.
- Impacto de las medidas adoptadas para la solución de la brecha.
- Acciones para el seguimiento.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7

2.6.6. Respuesta del CCN-CERT

Además de lo indicado con anterioridad, y sin perjuicio de las capacidades de respuesta que pueda tener cada Administración pública, el CCN-CERT articulará la respuesta a los incidentes de seguridad.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 31
ISBN: 978-84-120267-5-7