Directrices 01/2021 del EDPB sobre ejemplos de notificación de brechas de seguridad: Anexo

Supuesto de hecho	Medidas preventivas y análisis de riesgos	Medidas mitigadoras y correctoras	Acciones	
Ransomware				
N.º 01: Ransomware con una copia de seguridad adecuada y sin filtración. Una pequeña fábrica sufrió un ataque ransomware en sus sistemas. Los datos personales afectados se refieren a clientes y empleados de la empresa (en total pocas docenas de interesados afectados).	· Los datos almacenados estaban encriptados, a través de un algoritmo de última generación. · La clave para su descifrado no fue comprometida. · Se dispone de una copia de seguridad. · No se encuentran evidencias de que se haya filtrado la información. · Brecha que afecta a la disponibilidad de los datos afectados. Sin embargo, gracias a la copia de seguridad existente, permite la restauración de los datos a las pocas horas de sufrir el ataque, mitigando los efectos adversos, y sin que su actividad diaria haya sufrido ningún perjuicio ni retraso.	· Investigar la infracción e identificar las causas y los métodos utilizados por el atacante para prevenir ataques similares. · Actualizar y subsanar las medidas organizativas y técnicas de tratamiento de datos personales y medidas y procedimientos de mitigación de riesgos.	**Registro interno**	✓
			Notificar AC	X
			Notificar afectados	X
N.º 02: Ransomware sin copia de seguridad adecuada y sin filtración. Empresa agrícola, sufrió un ataque ransomware en sus sistemas y sus datos fueron encriptados por el atacante.	· Todos los flujos de datos que salen de la empresa (incluyendo el correo electrónico enviado) están disponibles. · No se dispone de copia de seguridad. · No se encuentran evidencias de que se haya filtrado la información. Sin embargo, dado que los logs no se reenvían o replican en un	· Disponer de una copia de seguridad electrónica. · Investigar la infracción e identificar las causas y los métodos utilizados por el atacante para prevenir ataques similares.	**Registro interno**	✓

Supuesto de hecho	Medidas preventivas y análisis de riesgos	Medidas mitigadoras y correctoras	Acciones	
Los datos personales afectados se refieren a clientes y empleados de la empresa, (en total pocas docenas de interesados afectados).	servidor central, incluso después de una investigación exhaustiva que determine que no se filtraron los datos personales, no se puede descartar por completo la probabilidad de una violación de la confidencialidad. · Brecha que afecta a la disponibilidad y confidencialidad de los datos afectados. · El restablecimiento de los datos llevó 5 días laborables y provocó pequeños retrasos en la entrega de pedidos a los clientes, así como una cantidad considerable de metadatos (p.ej., logs, fechas) que podrían no ser recuperables.	· Actualizar y subsanar las medidas organizativas y técnicas de tratamiento de datos personales y medidas y procedimientos de mitigación de riesgos.	**Notificar AC**	✓
			Notificar afectados	X
N.º 03: Ransomware con copia de seguridad adecuada y sin filtración, en un hospital. El sistema de información de un hospital fue expuesto a un ataque de ransomware y una parte importante de sus datos fue cifrada por el atacante. Los datos personales afectados se refieren a pacientes y empleados (en total miles de interesados afectados).	· Disponer de copia de seguridad. Sin embargo, dada la naturaleza de la brecha, el grado de severidad de las consecuencias, así como el número de afectados suponen un riesgo elevado. · No se encuentran evidencias de que se haya filtrado la información. · Disponer de registros que rastrean todos los flujos de datos que salen de la empresa (incluido el correo electrónico saliente).	· Investigar la infracción e identificar las causas y los métodos utilizados por el atacante para prevenir ataques similares. · Actualizar y subsanar las medidas organizativas y técnicas de tratamiento de datos personales y medidas y procedimientos de mitigación de riesgos.	**Registro interno**	✓
			Notificar AC	✓

Supuesto de hecho	Medidas preventivas y análisis de riesgos	Medidas mitigadoras y correctoras	Acciones	
Provocó retrasos importantes en el tratamiento de los pacientes, con cirugías canceladas/pospuestas, y una disminución del nivel de servicio debido a la indisponibilidad de los sistemas.	· Brecha que afecta a la confidencialidad y disponibilidad.	· Aunque los datos relativos a todos los pacientes tratados en el hospital durante los últimos años han sido encriptados, sólo se vieron afectados los pacientes que tenían previsto ser tratados en el hospital durante el tiempo en que el sistema informático no estuvo disponible. Se debe comunicar la brecha a esos pacientes directamente.	**Notificar afectados**	✓
N.º 04: Ransomware sin copia de seguridad y con filtración El servidor de una empresa de transporte público estuvo expuesto a un ataque de ransomware y sus datos fueron cifrados por el atacante. Según las conclusiones de la investigación interna, el agresor no solo cifró los datos, sino que también los filtró. El tipo de datos eran los datos personales de clientes y empleados, y de los varios miles de usuarios que utilizaban los servicios de la empresa (datos identificativos, números de identificación y los datos financieros, como datos de tarjetas de crédito).	· En un régimen de copias de seguridad bien diseñado, las múltiples copias de seguridad deben almacenarse de forma segura sin acceso desde el sistema principal, para no verse comprometidas en el mismo ataque. · Las copias de seguridad deberían realizarse periódicamente y estar aisladas, lo que aumentaría la probabilidad de recuperación. · La naturaleza, sensibilidad y volumen de los datos personales aumenta el riesgo. · La brecha de seguridad presenta un alto riesgo para los derechos y libertades de los interesados, ya que podría dar lugar a daños materiales (p.ej., pérdidas financieras) y no materiales (p.ej., robo de identidad o fraude). · Mantener actualizados el firmware, el sistema operativo y el software de aplicación de los	· Investigar la infracción e identificar las causas y los métodos utilizados por el atacante para prevenir ataques similares. · Importancia de una evaluación global del sistema de seguridad de los datos, con especial énfasis en la seguridad IT. · Los puntos débiles y los fallos de seguridad identificados deben documentarse y abordarse sin demora.	**Registro interno**	✓
			Notificar AC	✓

Supuesto de hecho	Medidas preventivas y análisis de riesgos	Medidas mitigadoras y correctoras	Acciones	
Existía una base de datos de respaldo, pero también fue encriptada por el atacante.	servidores, los componentes activos de la red y cualquier otro equipo de la misma LAN (incluidos los dispositivos Wi-Fi). · Garantizar que se aplican las medidas de seguridad informática adecuadas, asegurarse de que son eficaces y mantenerlas actualizadas periódicamente, incluyendo llevar un registro detallado de los parches aplicados y de la fecha de aplicación.		**Notificar afectados**	✓
Ataques que provocan fugas de información				
N.º 05: Filtración de datos de solicitudes de empleo de un sitio web A través de la instalación de un código malicioso, un ciberdelincuente atacó la web de una agencia de empleo. Este código malicioso hizo que la información personal enviada a través de los formularios de solicitud de empleo establecidos en la web y almacenada en el servidor web, fuera accesible. Se descubrió al mes de su instalación El malware instalado en particular tenía funcionalidades que permitían al atacante eliminar cualquier historial de filtración y	· Las auditorías periódicas de seguridad informática, las evaluaciones de seguridad informática, evaluaciones de vulnerabilidad y pruebas de penetración para detectar este tipo de vulnerabilidades hechas con antelación y solucionarlas y corregirlas. · Las herramientas de supervisión de la integridad de los archivos en el entorno de producción podrían haber ayudado a detectar la instalación del código malicioso. · Brecha de confidencialidad e integridad. · Investigar la brecha identificando el tipo de ataque y sus métodos, con el fin de evaluar las medidas que se deben adoptar.	· Comparar la base de datos con la almacenada en una copia de seguridad (cuanto más actualizada mejor). · Actualizar la infraestructura de TI. · Devolver todos los sistemas informáticos afectados a un estado limpio conocido, solucionar la vulnerabilidad y aplicar nuevas medidas de seguridad para evitar futuras brechas (p.ej., auditorías de seguridad o controles de integridad de archivos). · Adoptar medidas sistemáticas para recuperar los datos	**Registro interno** **Notificar AC**	✓ ✓

Supuesto de hecho	Medidas preventivas y análisis de riesgos	Medidas mitigadoras y correctoras	Acciones	
también permitía monitorear el tratamiento en el servidor y recoger datos personales. Los datos personales afectados se refieren a candidatos, (en total 213 formularios).	· Contar con un plan de respuesta a incidentes que especifique los pasos rápidos y necesarios para controlar el incidente. · No se vieron afectadas categorías especiales de datos personales. · Los datos a los que se accedió contienen información sobre los candidatos que podrían utilizarse de forma indebida de diversas maneras, por lo que afecta al riesgo de los derechos y libertades.	personales en el estado en que se encontraban antes de la brecha (copias de seguridad completas e incrementales). Ello implica disponer de un método robusto de almacenamiento y una política de retención adecuada.	**Notificar afectados**	✓
N.º 06: Filtración de la contraseña cifrada de un sitio web Una vulnerabilidad de inyección SQL fue explotada para obtener acceso a una base de datos del servidor de un de un sitio web de cocina. Los datos personales afectados se refieren a usuarios (en total contraseñas cifradas de 1.200 usuarios).	· Las contraseñas estaban almacenadas de forma cifrada con un algoritmo de última generación y la clave de acceso no estaba comprometida. · Brecha de confidencialidad. · No presenta riesgos para los derechos y libertades de los interesados y al no verse comprometidos datos personales de contacto, no existe un riesgo significativo para los interesados de ser objeto de acciones fraudulentas. · Por el tipo de página no se puede entender que afecta a datos de categorías especiales.	· No es obligatorio, pero se considera de buena fe, informar a los interesados de la violación por correo electrónico y solicitar el cambio de sus contraseñas, especialmente si la misma contraseña se utilizaba para otros servicios. · Corregir la vulnerabilidad y aplicar nuevas medidas de seguridad (p.ej. auditorías de seguridad de los sitios web).	**Registro interno**	✓
			Notificar AC	X
			Notificar afectados	X

Supuesto de hecho	Medidas preventivas y análisis de riesgos	Medidas mitigadoras y correctoras	Acciones	
N.º 07: Ataque con robo de credenciales en un sitio web bancario Debido a una vulnerabilidad del sitio web, en algunos casos se filtraron al atacante datos personales. El banco tuvo conocimiento de la violación de los datos porque su centro de operaciones de seguridad detectó un elevado número de solicitudes de inicio de sesión. Los datos personales afectados se refieren a unos 100.000 clientes (nombre, apellidos, sexo, fecha y lugar de nacimiento, código fiscal, códigos de identificación de usuario). De entre las cuentas de dichos afectados, el atacante consiguió entrar en unas 2.000 cuentas.	· Se dispone de un centro de operaciones de seguridad operativo y efectivo de cara a prevenir, detectar y responder ante vulnerabilidades y ataques de similares características. · La brecha afecta a un número elevado de usuarios y a categorías de datos identificativos (incluido el nombre de usuario) y financieros, lo que la hace especialmente grave. · Brecha de confidencialidad y disponibilidad.	· Realizar comprobaciones antifraude, de las cuentas afectadas con el fin de comprobar usos y accesos indebidos/no autorizados. · Exigir a los usuarios restablecer las contraseñas de sus cuentas. · Actualizar las medidas de seguridad en entorno web y añadir la autenticación de doble factor.	**Registro interno**	✓
			Notificar AC	✓
			Notificar afectados	✓
Brechas de origen interno derivadas de errores humanos				
N.º 08: Fuga de datos de contacto profesionales por parte de un empleado Durante su periodo de preaviso, un empleado copia datos comerciales de la base de datos. Después de dejar el trabajo, utiliza los datos obtenidos (datos básicos de contacto) para	· No se han tomado medidas previas para prevenir la copia de información. · Brecha de confidencialidad. · No se han filtrado datos sensibles. · No se puede controlar el uso posterior por parte del exempleado.	· Acciones legales inmediatas contra el exempleado para prevenir usos posteriores. · Aplicación de medidas de seguridad que impidan la extracción de información y copia a dispositivos extraíbles.	**Registro interno**	✓

Supuesto de hecho	Medidas preventivas y análisis de riesgos	Medidas mitigadoras y correctoras	Acciones	
contactar con los clientes y atraerlos a su nuevo negocio.		· Retirar determinadas opciones de acceso a los empleados que han manifestado su intención de abandonar la empresa. · Implantar registros de acceso para poder registrar y controlar los accesos no deseados. · El contrato firmado con los empleados debe incluir cláusulas que prohíban estas acciones. · Informar a los interesados puede ser beneficioso también para el responsable, ya que los clientes tendrán conocimiento de la brecha a través de la propia empresa y no del exempleado.	**Notificar AC**	✓
			Notificar afectados	X
N.º 09: Comunicación accidental de datos a un encargado del tratamiento Un agente de seguros se dio cuenta de que, debido a la configuración defectuosa de un archivo Excel recibido por email, tenía acceso a información relacionada con dos docenas de clientes que no pertenecían a su área (datos de contacto y datos sobre el propio seguro). El agente señaló inmediatamente el error al responsable del tratamiento, que corrigió el fichero y lo volvió a enviar, pidiendo al agente que borrara el mensaje anterior. El agente confirmó la supresión en una declaración escrita.	· Brecha de confidencialidad. · Cantidad baja de datos de interesados. · No se han filtrado datos sensibles. · Las circunstancias anteriores hacen que el caso concreto no suponga ningún riesgo.	· El hecho de que el encargado del tratamiento notificara inmediatamente es considerado una medida mitigadora. · Reducir el intercambio de archivos a través del correo electrónico, y utilizando en su lugar sistemas específicos para el tratamiento de los datos de los clientes. · Comprobar dos veces los archivos antes de enviarlos. · Separar la creación y el envío de ficheros.	**Registro interno**	✓
			Notificar AC	X
			Notificar afectados	X

Supuesto de hecho	Medidas preventivas y análisis de riesgos	Medidas mitigadoras y correctoras	Acciones	
Pérdida o robo de dispositivos y documentos				
N.º 10: Material robado con datos personales cifrados Robo de dos tabletas en una guardería que contenían una app con datos personales de los alumnos (nombres, fechas de nacimiento y datos personales sobre educación). Tanto las tabletas encriptadas, que estaban apagadas en el momento del robo, como la app, estaban protegidas por una contraseña robusta. Existía copia de seguridad y tras darse cuenta del robo, se emitió una orden de borrado a distancia.	· Se tomaron medidas adecuadas: encriptado de dispositivos, contraseñas y copias de seguridad. · La contraseña se configura de tal forma que aplica también a los datos personales contenidos en la tableta. · Debido a las medidas adoptadas, no se compromete la confidencialidad, disponibilidad ni la integridad de los datos.	· N/A	**Registro interno**	✓
			Notificar AC	X
			Notificar afectados	X
N.º 11: Material robado que almacena datos personales no cifrados Robo del portátil de un empleado que contenía nombres, apellidos, sexo, direcciones y fecha de nacimiento de más de 100.000 clientes, sin posibilidad de identificar si otras categorías de datos personales también estaban afectadas. El acceso al disco duro del portátil no estaba protegido por ninguna contraseña. Los datos personales pudieron restaurarse a partir de las copias de seguridad diarias disponibles.	· No se tomaron medidas preventivas. · Brecha de confidencialidad. · Potencial fraude de identidad de los interesados. · Número elevado de interesados que aumenta el riesgo.	· Establecer encriptación y contraseñas robustas.	**Registro interno**	✓
			Notificar AC	✓
			Notificar afectados	✓

Supuesto de hecho	Medidas preventivas y análisis de riesgos	Medidas mitigadoras y correctoras	Acciones	
N.º 12: Robo de archivos en papel con datos sensibles Robo de un libro de registro de un centro de rehabilitación de adicción a drogas con datos identificativos y de salud de los pacientes. Los datos sólo estaban almacenados en papel y no se disponía de copia de seguridad. El libro no estaba guardado en un cajón o una sala cerrada con llave y no se disponía de un sistema de control de acceso.	· Brecha con riesgo alto ya que no se han tomado medidas preventivas. · La naturaleza de los datos robados hace que el hecho de no existir copia de seguridad sea un factor de riesgo grave. · Brecha de confidencialidad, integridad y disponibilidad. · Se incumple con el secreto profesional y se pone en riesgo el tratamiento de los pacientes. · Los datos corren el riesgo de ser modificados o eliminados.	· Seudonimización de los nombres de los pacientes. · Almacenamiento en un lugar seguro y en un cajón o sala cerrada con llave. · Control de acceso adecuado con autentificación al acceder.	**Registro interno**	✓
			Notificar AC	✓
			Notificar afectados	✓
Errores en el envío de correo postal				
N.º 13: Error en el envío de correo postal Debido a un error humano, se enviaron productos (zapatos) y sus facturas de forma equivocada, por lo que dos clientes recibieron el producto y factura de otra persona. Tras darse cuenta de la infracción, se recogieron los pedidos y se enviaron a los destinatarios correctos.	· Riesgo bajo debido a la cantidad reducida de afectados.	· Revisar por qué ocurre el error y cómo se puede evitar en el futuro. · Proporcionar devolución gratuita a los clientes y solicitarles que eliminen/destruyan posibles copias. · La comunicación a los afectados es inevitable ya que la cooperación de los clientes es fundamental para mitigar el riesgo.	**Registro interno**	✓
			Notificar AC	X
			Notificar afectados	X
N.º 14: Datos de desempleados enviados por correo por error El departamento de empleo de una administración pública envió un correo	· Se deberían haber implantado medidas más estrictas. · Riesgo alto debido al número de datos afectados, así como su categoría.	· Los medios para mitigar eficazmente los riesgos de una violación similar, son limitados. · Aunque se haya solicitado el borrado del mensaje, no se puede	**Registro interno**	✓

Supuesto de hecho	Medidas preventivas y análisis de riesgos	Medidas mitigadoras y correctoras	Acciones	
electrónico a las personas registradas en su sistema como demandantes de empleo. Por error, se adjuntó a este correo electrónico un documento con todos los datos personales de más de 6000 demandantes de empleo (nombre, dirección de correo electrónico, dirección postal, número de la seguridad social). Posteriormente, la oficina se puso en contacto con todos los destinatarios y les pidió que borraran el mensaje anterior y que no utilizaran la información.	· Imposibilidad de controlar el uso posterior al robo.	obligar a los destinatarios a hacerlo y, en consecuencia, tampoco se puede tener la certeza de que cumplan con la solicitud.	**Notificar AC**	✓
			Notificar afectados	✓
N.º 15: Datos enviados por correo por error Una lista de participantes en un curso de inglés que tiene lugar en un hotel se envía por error a 15 antiguos participantes del curso en lugar de al hotel. La lista contiene los nombres, las direcciones de email y las preferencias alimentarias de los 15 participantes. Sólo dos participantes han indicado que son intolerantes a la lactosa. Cuando se descubre el error, inmediatamente después de enviar la lista, se informa a los destinatarios se solicita la eliminación.	· A pesar de que la información sobre intolerancias es un dato de salud, el riesgo de que se utilicen de forma perjudicial se considera relativamente bajo. En términos generales, no puede relacionarse con datos que revelen creencias religiosas o filosóficas.	· Se deben considerar medios de control adicionales. · Contacto con receptores del correo, incluyendo una disculpa, solicitando el borrado de la información e indicando que no pueden hacer uso de la misma.	**Registro interno**	✓
			Notificar AC	X
			Notificar afectados	X
N.º 16: Error en envío de correo postal Entidad aseguradora envía por correo postal pólizas que incluyen el nombre y la dirección	· La probabilidad de uso indebido de estos datos es entre baja y media. · Es probable que muchos destinatarios tiren a la basura la carta recibida erróneamente.	· Se debe facilitar la devolución de la carta a expensas del responsable.	**Registro interno**	✓

Supuesto de hecho	Medidas preventivas y análisis de riesgos	Medidas mitigadoras y correctoras	Acciones	
del titular de la póliza, así como el número de matrícula del vehículo, las tarifas del seguro del año actual y del siguiente, el kilometraje anual aproximado y la fecha de nacimiento del titular.	· No se puede descartar por completo que la carta se publique en las redes sociales o que se contacte con el asegurado.	· Informar al destinatario de no hacer un mal uso de la información. · Probablemente no será posible evitar por completo un error de entrega postal en un envío masivo automatizado. · Si aumente la frecuencia de errores, es necesario comprobar el funcionamiento de las máquinas de ensobrado.	**Notificar AC**	✓
			Notificar afectados	X
Otros casos - Ingeniería social				
N.º 17: Robo de identidad El call center de una empresa de telecomunicaciones recibe una llamada telefónica de alguien que se hace pasar por un cliente. El supuesto cliente exige a la empresa que cambie la dirección de correo electrónico a la que deben enviarse los datos de facturación. El trabajador del centro de contacto valida la identidad del cliente pidiéndole determinados datos personales (número de identificación y la dirección postal), según los procedimientos de la empresa. El procedimiento no prevé ninguna	· Riesgo alto ya que los datos de facturación pueden dar información sobre la vida privada (p.ej., hábitos, contactos) y podrían provocar daños materiales (p.ej., acoso, riesgo para la integridad física). · La medida de autenticación no es suficiente y debe de redefinirse función de los datos personales que puedan tratarse como resultado de la autenticación.	· No se recomienda el uso de medios de autenticación estática (donde la respuesta no cambia, y donde la información no es "secreta", como sería el caso de una contraseña). · La introducción de un método de autenticación multifactorial resolvería el problema.	**Registro interno**	✓
			Notificar AC	✓

Supuesto de hecho	Medidas preventivas y análisis de riesgos	Medidas mitigadoras y correctoras	Acciones	
notificación al antiguo contacto de correo electrónico. El cliente legítimo se pone en contacto con la empresa, reclamando no recibir la facturación a su dirección de correo electrónico, y niega cualquier llamada suya exigiendo el cambio del contacto de correo electrónico.			**Notificar afectados**	✓
N.º 18: Filtración del correo electrónico Una cadena de hipermercados detectó, 3 meses después de su configuración, que algunas cuentas de correo electrónico habían sido alteradas y se habían creado reglas para que todo correo electrónico que contuviera determinadas expresiones (p.ej., "factura", "pago", "transferencia bancaria", "autentificación de tarjeta de crédito", "datos de cuenta bancaria") fuera trasladado a una carpeta y reenviado a una dirección de correo electrónico externa.	· Se forzó un cambio de contraseña para las cuentas comprometidas. · Se bloqueó el envío de correos electrónicos a la cuenta de correo electrónico del atacante. · Se notificó al proveedor de servicios del correo electrónico utilizado por el atacante. · Se eliminaron las reglas establecidas por el atacante. · Se refinaron las alertas del sistema de monitorización para que las mismas se produjeran en el momento de crearse una regla automática.	· La brecha se debe comunicar a las 99 personas afectadas, y no solo a los 10 empleados cuyos salarios fueron filtrados. · Ampliar las revisiones de la automatización y los controles de los cambios, la detección de incidentes y las medidas de respuesta. · Los responsables que tratan datos sensibles, información financiera, etc., tienen una mayor responsabilidad en cuanto a	**Registro interno**	✓

Supuesto de hecho	Medidas preventivas y análisis de riesgos	Medidas mitigadoras y correctoras	Acciones	
Además, el atacante, haciéndose pasar por un proveedor, había hecho que los datos de la cuenta bancaria de ese proveedor fueran alterados para convertirlos en los suyos propios. Por último, se habían enviado varias facturas falsas que incluían los nuevos datos de la cuenta bancaria. El sistema de monitorización de la plataforma de correo electrónico acabó dando una alerta sobre las carpetas. La empresa no pudo detectar cómo el atacante accedió a las cuentas de correo electrónico, pero supuso que un correo electrónico infectado fue el culpable de dar acceso al grupo de usuarios. El atacante recibió información sobre 99 empleados (nombre y salario de un mes concreto en relación con 89 interesados; nombre, estado civil, número de hijos, salario, horas de trabajo y resto de información sobre la percepción de salarios de 10 empleados cuyos contratos habían finalizado). El responsable del tratamiento sólo notificó a los 10 empleados pertenecientes a este último grupo.		proporcionar una seguridad de datos adecuada.	**Notificar AC**	✓
			Notificar afectados	✓