cyber zaintza

Datuak Babesteko Euskal Agintaritza
Autoridad Vasca de Protección de Datos

Guía básica para

Entidades del sector público vasco sobre la gestión de incidentes de ciberseguridad

2024-2029

EUSKO JAURLARITZA
GOBIERNO VASCO

Índice

1.1 Sobre la Autoridad Vasca de Protección de Datos

La Autoridad Vasca de Protección de Datos (AVPD) es una autoridad de control independiente, con personalidad jurídica propia y plena capacidad pública y privada. Actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones, velando por que se garantice un tratamiento adecuado de los datos personales por parte de las Administraciones e Instituciones que conforman el sector público vasco.

Además, controla y supervisa el uso que de los datos personales hacen las personas físicas o jurídicas cuando el tratamiento se lleva a cabo para el ejercicio de funciones públicas en materias que son competencia de las administraciones públicas o las entidades de derecho privado que prestan servicios públicos mediante cualquier forma para las mismas.

La AVPD atiende consultas relacionadas con la protección de datos personales y participa en acciones de difusión y formación para dar a conocer los derechos reconocidos en la normativa que rige esta materia y aumentar la conciencia pública acerca del valor de la privacidad.

Corresponde también a la AVPD tutelar los derechos que a las personas les reconoce la normativa de protección de datos personales.

Para garantizar la protección efectiva de los derechos y libertades de los ciudadanos, la AVPD, en cumplimiento de sus funciones como autoridad de control, pone a disposición de las entidades del sector público vasco el procedimiento electrónico para la notificación de brechas de seguridad de datos personales.

Se puede obtener información más detallada y extensa en:
https://www.avpd.eus

1.2 Sobre Cyberzaintza

Cyberzaintza, la Agencia Vasca de Ciberseguridad, es un organismo público, con personalidad jurídica propia, creado para combatir, de una manera integral y transversal, las amenazas derivadas del uso de internet y las nuevas tecnologías en Euskadi y su creación se recoge en la Ley 7/2023, de 29 de junio, de creación de la Agencia Vasca de Ciberseguridad.

La Agencia tiene como objeto promover y coordinar la ciberseguridad en el sector público vasco delimitado en la Ley 3/2022, de 12 de mayo, del Sector Público Vasco, en el ámbito de la seguridad de los sistemas de información y de las redes electrónicas de competencia de dicho sector, y apoyar e impulsar la capacitación en ciberseguridad y el desarrollo digital seguro de la Comunidad Autónoma Vasca, de su Administración pública, de su ciudadanía y de su tejido empresarial. Las funciones de la Agencia están recogidas en la propia Ley.

Se puede obtener información más detallada y extensa en:
https://www.ciberseguridad.eus

2. Glosario

Amenaza
Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Brecha de seguridad de datos personales
Toda violación (en adelante, brecha) de la seguridad que ocasione 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.

Ciberataque
Cualquier tipo de maniobra ofensiva hecha por individuos u organizaciones que atacan a sistemas de información como lo son infraestructuras, redes computacionales, bases de datos que están albergadas en servidores remotos, por medio de actos maliciosos usualmente originados de fuentes anónimas que también roban, alteran o destruyen un blanco específico mediante hackeo de un sistema vulnerable.

Datos personales
Toda información sobre una persona física identificada o identificable («la interesada»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Encargado de tratamiento
La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Incidencia
Posible problema que podría afectar de manera negativa a los servicios de tecnologías de la información en el entorno de la organización.

Incidente
Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

Persona Delegada de Protección de Datos (DPD)
Informa al Responsable y/o al Encargado de tratamiento de las obligaciones y responsabilidades en relación con las brechas de seguridad de datos de carácter personal. Coopera con la AVPD en la gestión de las brechas de seguridad.

Plan de respuesta a incidentes
Es un conjunto de instrucciones dirigidas a ayudar a una organización a detectar, responder y recuperarse de los incidentes de ciberseguridad que sufran.

Registro de actividades de Tratamiento
Inventario de tratamientos que la entidad debe publicar de forma accesible por medios electrónicos. Se deben especificar las actividades de tratamiento según sus finalidades.

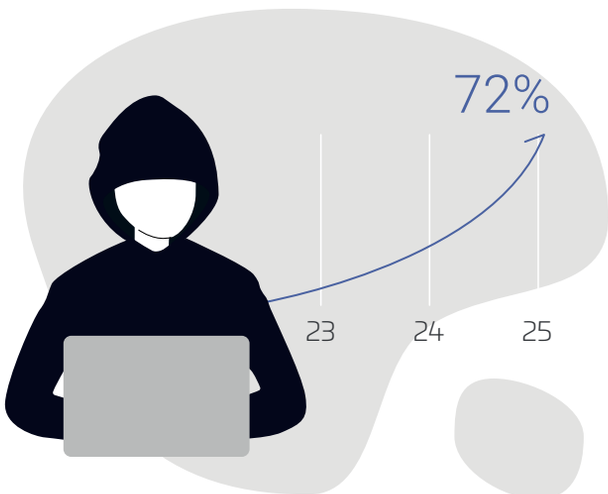
Responsable de tratamiento
La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

Tratamiento
Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Vulnerabilidad
Toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

3. Contexto

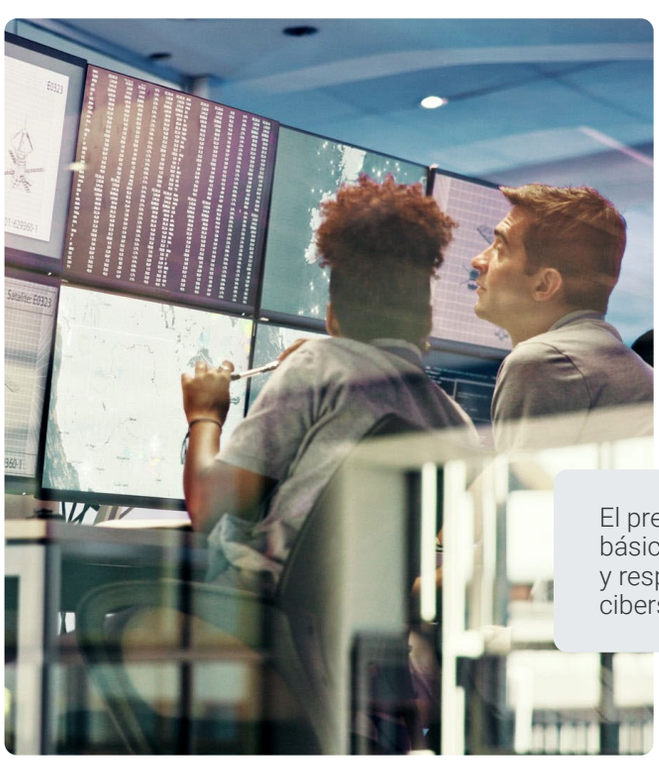
En los últimos años ha habido un incremento muy significativo en cuanto a los ciberataques y a los incidentes de ciberseguridad sufridos en Euskadi. Según los datos de la «Memoria Delincuencial de la Euskal Polizia», en los últimos 3 años ha habido un incremento del 72% en las denuncias relacionadas con delitos informáticos. Las brechas de seguridad notificadas a la AVPD también han crecido en comparación con años anteriores.



Instituciones públicas, entidades privadas y ciudadanía han visto incrementado el riesgo de sufrir un incidente como consecuencia de diferentes factores como la profesionalización de los cibercriminales, el aumento descontrolado de la superficie de exposición, la adopción de nuevas tecnologías como la inteligencia artificial sin tener en cuenta la perspectiva de seguridad y privacidad, los errores de configuración o la asunción de que los sistemas vienen por defecto configurados para ser seguros, las vulnerabilidades, la falta de concienciación y la consecuente falta de medidas de protección, la falta de especialización y la difícil colaboración en la persecución del delito.

En el caso de la administración pública vasca, para obtener mayor detalle de los principales riesgos de ciberseguridad y aprender a hacer frente a los mismos para reducirlos y mitigarlos en caso de que se materialicen, se recomienda la lectura del informe "Principales riesgos de ciberseguridad en la Administración Pública Vasca".

Llegados a este punto, ya se han normalizado noticias como que nuestros datos personales se han visto comprometidos y expuestos como consecuencia de un incidente de ciberseguridad sufrido por algún proveedor de servicios de internet, alguna red social, alguna empresa tecnológica, etc. O noticias de fraudes con las consecuentes pérdidas económicas, y que pueden impactar directamente en la continuidad de las entidades, así como en su nivel reputacional.

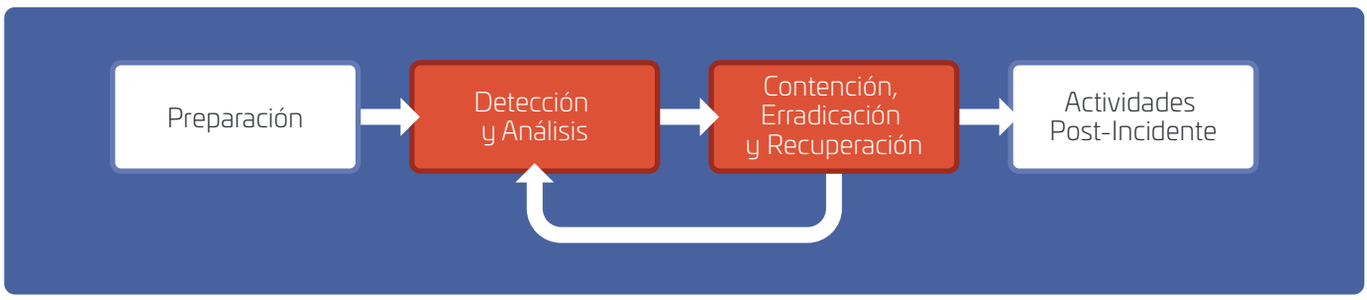


Cabe destacar que conforme al artículo 33 del Reglamento General de Protección de Datos (RGPD), tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido un ciberincidente asociado a una brecha de seguridad que pueda afectar a datos personales, debe efectuar la correspondiente notificación a la AVPD. Dicha notificación debe realizarse sin dilación, y a más tardar en las 72 horas siguientes, computando también las horas transcurridas durante fines de semana y festivos. Se dispone de más información en la guía "Notificación de brechas de seguridad". Así mismo, en el Esquema Nacional de Seguridad se establece la obligatoriedad de notificación de aquellos incidentes categorizados con nivel alto, muy alto o crítico.

El presente documento surge con el objetivo de servir de ayuda básica a las entidades del sector público vasco para prepararse y responder de manera adecuada a los incidentes de ciberseguridad cuando estos se produzcan.

4. Ciclo de vida de la respuesta a incidentes

El ciclo de vida de la respuesta a incidentes de ciberseguridad se compone de varias fases, cada una de las cuales juega un papel crucial para responder de manera adecuada limitando el potencial impacto. A continuación, se detalla cada una de estas fases.



4.1 Preparación

La primera fase del ciclo de vida de la respuesta a un incidente de ciberseguridad es la preparación. En esta etapa, las organizaciones desarrollan y mejoran sus capacidades para gestionar incidentes mediante la adecuación a la legislación de protección de datos de carácter personal, la creación de políticas, procedimientos y despliegue y configuración de herramientas de protección adecuadas.

Esto incluye tareas tales como:

- Realizar una evaluación y gestión adecuada de los riesgos, identificando y priorizando la protección de los activos / sistemas críticos para la organización.
- Identificar las tipologías de incidentes habituales. Para ello, en el anexo I está disponible la Guía CCN-STIC 817, la cual establece una taxonomía estandarizada que recoge las categorías principales, así como una serie de tipos de incidentes para cada una de ellas.
- Más allá de la tipología de incidentes, conviene establecer una serie de criterios a partir de los cuales se establece el umbral de impacto del incidente: Crítico, Muy Alto, Alto, Medio y Bajo. Los criterios pueden ser ámbito de afección, porcentaje de sistemas afectados, tiempo de inactividad provocado por el incidente, tipología de daños: económicos, reputacionales, etc., y especialmente, el menoscabo respecto a los derechos y libertades de las personas afectadas por dicho ciberincidente.
- Asignar roles y responsabilidades ante un incidente, así como recopilar todos los datos de contacto y establecimiento de canales de comunicación.
- Identificar puntos de contacto adicionales: proveedores, grupos de interés, etc.
- Identificar y cumplir los requisitos normativos en materia de ciberseguridad para la organización.
- Desarrollar y documentar políticas y procedimientos de alerta y de respuesta a incidentes, como, por ejemplo, planes de continuidad de negocio o planes de recuperación ante desastres, estableciendo plazos de revisión periódica.
- Imprimir la información de los procedimientos.
- Implementar y operar herramientas y tecnologías de protección y monitorización frente a amenazas.
- Capacitar al personal en las mejores prácticas de ciberseguridad y respuesta a incidentes, haciendo hincapié en el ámbito de la Protección de Datos de carácter personal.
- Realizar simulacros y ejercicios para evaluar la preparación del equipo.

En lo referente al cumplimiento del RGPD, se contemplan las siguientes tareas:

- Publicar el registro de actividades de tratamiento de la entidad con el contenido mínimo que exige la normativa de Protección de Datos.
- Designar una persona como DPD de la entidad de acuerdo con los requisitos que exige el RGPD.
- Publicar los datos de contacto de la persona DPD en un lugar visible del sitio web de la entidad, y comunicarlos a la AVPD a través del procedimiento disponible en la web de la Autoridad.
- Realizar evaluaciones de impacto de los tratamientos que lo requieran.

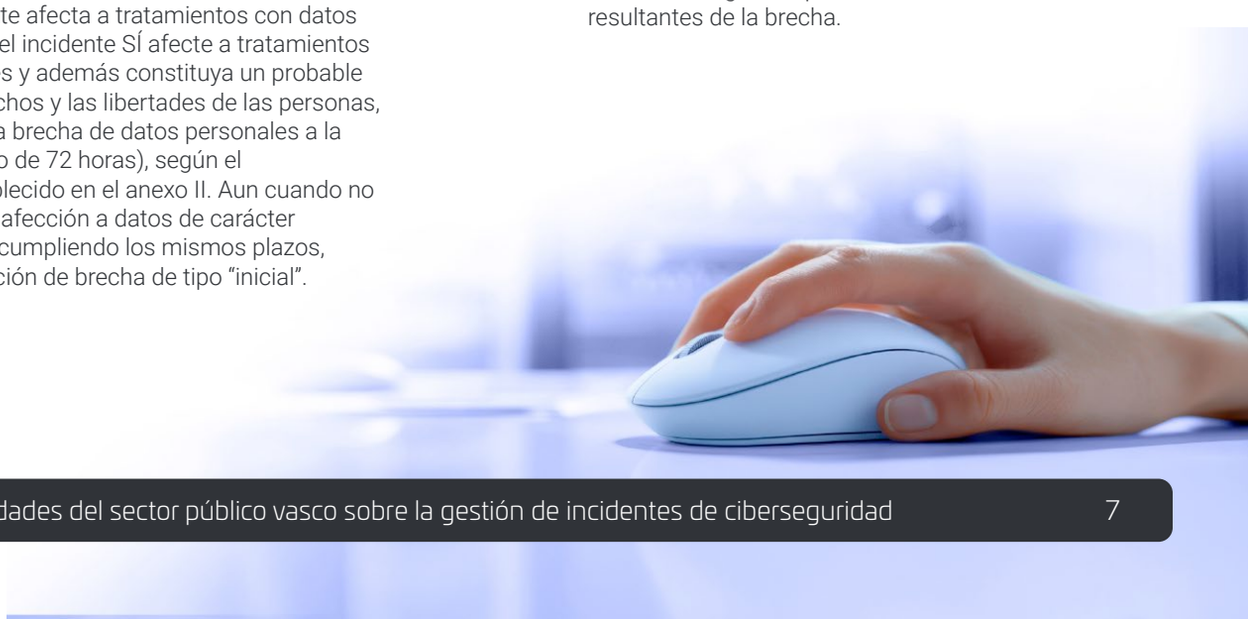
En lo referente al cumplimiento del ENS, se contemplan las siguientes tareas relacionadas con la preparación para la respuesta a incidentes:

- Definir roles y responsabilidades específicas en la gestión de la seguridad: responsable de seguridad, responsable del sistema, responsable de la información, etc.
- Disponer de un procedimiento formal actualizado de gestión de incidentes que vaya alineado con la guía CCN-STIC 817.
- Evaluar periódicamente la eficacia del plan a partir de simulacros y situaciones de incidentes reales cuando se produzcan.
- Disponer de mecanismos de detección, registro y análisis de eventos.

4.2 Detección y Análisis

La siguiente fase es la detección y análisis, donde se identifican y comprenden los incidentes de ciberseguridad. Esto suele involucrar la monitorización de sistemas y redes para detectar actividades sospechosas, el uso de software de detección de amenazas y la correlación de eventos para determinar la naturaleza y el alcance del incidente. Una rápida identificación y análisis son esenciales para contener y mitigar los efectos del incidente.

- Utilizar herramientas de detección de amenazas para identificar posibles incidentes.
- Monitorizar continuamente sistemas y redes para detectar actividades inusuales.
- Almacenar logs para tener trazabilidad de lo que sucede en los sistemas.
- Correlacionar eventos de seguridad para determinar el origen y la naturaleza del incidente.
- En el caso de identificar un incidente, es fundamental actuar con diligencia y notificar con inmediatez a las personas / entidades con capacidad de actuación para gestionarlo.
- Realizar un análisis en profundidad para comprender el alcance y el impacto del incidente.
- Analizar si el incidente afecta a tratamientos con datos personales: cuando el incidente SÍ afecte a tratamientos con datos personales y además constituya un probable riesgo para los derechos y las libertades de las personas, se deberá notificar la brecha de datos personales a la AVPD (plazo máximo de 72 horas), según el procedimiento establecido en el anexo II. Aun cuando no haya fehaciencia de afección a datos de carácter personal se deberá, cumpliendo los mismos plazos, realizar una notificación de brecha de tipo “inicial”.
- Los responsables de tratamiento deben anotar la brecha en el registro de incidentes de la entidad, así como la información relativa a las decisiones tomadas sobre la notificación a la AVPD y la comunicación a las personas afectadas.
- Cuando sea probable que la brecha entrañe un alto riesgo para los derechos y libertades de las personas físicas, se deberá notificar a estas cumpliendo lo siguiente:
  - Plazo: El RGPD obliga a que la notificación a los afectados se haga sin dilación indebida con el fin de que puedan tomar las precauciones necesarias.
  - La comunicación debe, en un lenguaje claro y sencillo, describir la naturaleza de la brecha de seguridad de datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la brecha.



4.3 Contención, Erradicación y Recuperación

Esta fase consta de tres subfases relacionadas:

Contención

El objetivo principal de la contención es limitar el alcance del incidente y evitar que se propague. Existen estrategias de contención a corto plazo, como aislar sistemas comprometidos, y a largo plazo, como la implementación de actualizaciones de seguridad. Esto incluye tareas tales como:

- Determinar el alcance del incidente, no sólo para la propia entidad, sino también para la ciudadanía, clientes, proveedores, etc., especialmente en el caso de que se hayan visto afectados datos personales.
- Implementar medidas de contención para controlar el incidente, lo que puede incluir:
  - Reforzar medidas de protección perimetral: aplicar reglas en los firewalls para bloquear el acceso a ciertas direcciones IP o dominios.
  - Aplicar segmentación adicional a la red.
  - En caso necesario, aislar por completo los sistemas afectados.
  - Cambiar el nivel de privilegios de usuarios afectados.
  - Bloqueo de cuentas de usuario o rotación de contraseñas.

Erradicación

Una vez contenida la amenaza, la erradicación se centra en eliminar por completo el código malicioso que ha provocado el incidente, en aquellos casos que sean de esta tipología. Esto incluye tareas tales como:

- Implementar mecanismos para proteger los sistemas, como por ejemplo EDR.
- Eliminar el malware y otros artefactos maliciosos como scripts, etc.
- Eliminar tareas automatizadas, entradas de registro, etc., relacionadas con el incidente.
- Aplicar actualizaciones de seguridad.

Recuperación

La fase de recuperación tiene como objetivo restaurar y validar la funcionalidad normal de los sistemas. Esto incluye tareas tales como:

- Diseñar una estrategia de recuperación, estableciendo prioridades.
- Restaurar sistemas y servicios afectados a su estado normal.
- Verificar que todas las medidas correctivas se han implementado adecuadamente, validando la integridad de los sistemas restaurados.
- Monitorizar los sistemas recuperados para asegurar que no haya recurrencias.

Las actuaciones a realizar en el caso de las NOTIFICACIONES de brechas de seguridad de datos personales ante la AVPD son las siguientes:

- Cuando se disponga de toda la información relevante de la brecha de seguridad se realizará una notificación a la AVPD de tipo "completa"; si no es el caso, se deberá realizar una notificación del tipo "inicial" (implica una notificación posterior del tipo "complementaria"). Para cualquier aclaración sobre el proceso se puede contactar con la AVPD escribiendo un email a evaluación.tecnologia@avpd.eus o llamando al 945 016 230.
- La notificación complementaria se debe realizar antes de que transcurra 1 mes desde la notificación inicial.
- El responsable de tratamiento deberá incluir la decisión tomada sobre la comunicación de la brecha de datos personales a las personas afectadas.

4.4 Actividades Post-Incidente

La fase final del ciclo de vida de la respuesta a un incidente es la de actividades post-incidente. En esta etapa, se lleva a cabo una revisión exhaustiva del incidente para identificar lecciones aprendidas y oportunidades de mejora. Esto incluye tareas como:

- Realizar una revisión detallada del incidente y de la respuesta al mismo.
- Identificar lecciones aprendidas y áreas de mejora.
- Actualizar políticas y procedimientos basados en las lecciones aprendidas.
- Implementar tecnología y herramientas que contribuyan a elevar el nivel de protección: MFA, segmentación, etc.
- Elaborar informes detallados para la alta dirección, CSIRT, autoridades de control, entidades interesadas, etc.
- Comunicar a partes externas sobre el incidente y las medidas adoptadas.
- Recepción del informe de cierre de brecha de datos personales enviado por parte de la AVPD, atendiendo a las recomendaciones emitidas.

Es fundamental que las lecciones aprendidas se conviertan en un plan de acción, en el que se identifiquen las acciones de mejora, se fijen hitos y se realice un seguimiento de consecución de estos.

4.5 Tareas comunes durante toda la gestión del incidente

- Recolectar y preservar evidencias digitales, preservando la cadena de custodia por si fuera necesaria la judicialización del incidente.
- Documentar todos los hallazgos y acciones tomadas a efectos justificativos de una debida diligencia y con el fin de realizar una gestión adecuada del incidente.
- Cumplir con las obligaciones de notificación, notificando al CSIRT que corresponda y autoridades de control que establezca la normativa que aplique a la organización.
- Interponer la correspondiente denuncia en una comisaría de la Ertzaintza.
- Notificar a Cyberzaintza, para que puedan tomar medidas para proteger al resto de entidades del sector público (900 104 891 – incidencias@cyberzaintza.eus), siendo obligatorio en los casos en los que afecte la Norma Vasca de Autoprotección.
- Gestionar la brecha de seguridad de datos personales cumpliendo el RGPD y atendiendo a los requerimientos de la AVPD no implica la imposición de una sanción; al contrario, una notificación, y en su caso comunicación a las personas afectadas, realizada en tiempo y forma, es una evidencia de la diligencia de la organización a la hora de ejecutar eficazmente la obligación de responsabilidad proactiva del RGPD. Sin embargo, el no cumplir con las obligaciones de notificación y comunicación a las interesadas sí está tipificado como infracción.

5. Errores comunes

A continuación, se indican los errores más destacados que se han extraído del análisis de incidentes de ciberseguridad:

- Pensar que los incidentes de ciberseguridad les pasan a otros y no a nosotros / nuestra organización, lo que deriva en una falta de planificación y preparación.
- No tener impresa la documentación, lo cual es especialmente crítico en los casos de ransomware ya que cifran la información de los sistemas imposibilitando el acceso a la misma.
- Creer que la gestión de los incidentes de ciberseguridad es únicamente responsabilidad del área de informática. Los incidentes involucran a otras áreas como la dirección general, el área legal, el de cumplimiento normativo, comunicación, control económico, recursos humanos, y en general a todo el personal de la organización.
- No conocer las obligaciones normativas y legales en caso de sufrir un incidente.
- Comunicación deficiente entre las personas que participan en la gestión del incidente.
- Aceptar explicaciones simplistas de lo sucedido o no intentar identificar la causa de lo sucedido, lo que conlleva en muchas ocasiones restaurar los sistemas sin haber determinado la causa del incidente, lo que implica que puede volver a suceder.
- La ausencia de logs imposibilita analizar las causas del incidente y dificulta la gestión de este.
- La ausencia de documentación dificulta significativamente el cumplimiento normativo y el aprendizaje.
- Pensar que, porque ya nos ha sucedido, no nos va a volver a suceder.
- Ignorar las lecciones aprendidas, lo que conlleva en muchas ocasiones a no invertir lo suficiente en implementar medidas para evitar que vuelva a suceder, en no invertir en formación continua y entrenamiento, etc.
- No tener en cuenta que el incidente de seguridad puede afectar a tratamientos con datos personales y por lo tanto existe la obligación de notificar a la AVPD la brecha de seguridad. No notificar las brechas de seguridad de datos personales supone la infracción del artículo 33 del RGPD, y se trata de una infracción GRAVE de acuerdo con el artículo 73.r de la LOPDGDD. Así mismo, aun cuando el responsable no tiene fehaciencia de si existe o no afección de los datos personales, se deberá notificar una brecha de tipo “inicial”.
- No comunicar la brecha de seguridad a las personas afectadas, cuando la autoridad de control así lo ha solicitado, está calificado como infracción GRAVE según el artículo 73.s de la LOPDGDD.
- Incumplir la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento es una infracción GRAVE conforme al artículo 73.v de la LOPDGDD.

6. Referencias normativas

- Orden de 7 de junio de 2024, del Vicelehendakari Primero y Consejero de Seguridad regula la elaboración de planes de continuidad informática en materia de ciberseguridad para ciertas actividades sujetas a la Norma Vasca de Autoprotección.
- Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G.
- Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos.
- Ley 7/2023, de 29 de junio, de creación de la Agencia Vasca de Ciberseguridad.
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

ANEXO I: Taxonomía de ciberincidentes

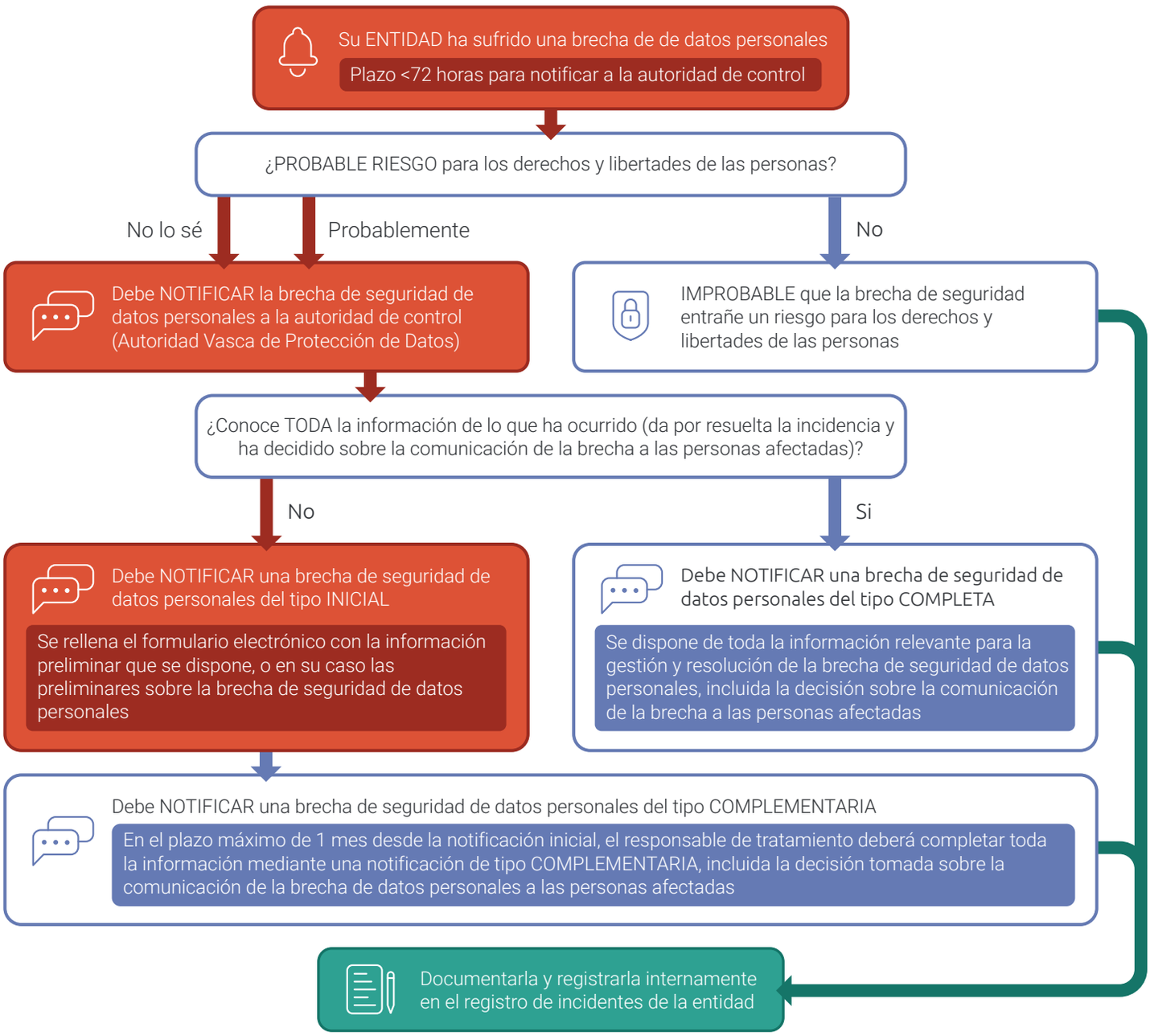
Clasificación/Taxonomía de ciberincidentes		
Clasificación	**Tipo de incidente**	**Descripción y ejemplos prácticos**
Contenido abusivo	Spam	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delito de odio	Contenido 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.
Contenido dañino	Sistema infectado	Sistema infectado con malware. Ej: Sistema, computadora o teléfono móvil infectado con un rootkit.
	Servidor C&C (Mando y Control)	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Distribución de malware	Recurso usado para 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.
Obtención de información	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.
Intento de intrusión	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.
Intrusión	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.

Clasificación/Taxonomía de ciberincidentes

Clasificación	Tipo de incidente	Descripción y ejemplos prácticos
Disponibilidad	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.
	Mala configuración	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
	Sabotaje	Sabotaje físico. Ej: cortes de cableados de equipos o incendios provocados.
	Interrupciones	Interrupciones por causas ajenas. Ej: desastre natural.
Compromiso de la información	Acceso no autorizado a información	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	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	Pérdida de información. Ej: pérdida por fallo de disco duro o robo físico.
Fraude	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.
Vulnerable	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.
Otros	Otros	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
	APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

ANEXO II: Procedimiento de notificación de brechas

Notificaciones de brechas de seguridad a la autoridad de control (AVPD).



Sarean ere, auzolana.
Por ti hacemos red.

cyber zaintza

Incidentes de ciberseguridad

900 104 891

incidencias@cyberzaintza.eus

Planes de autoprotección

jarraipena@cyberzaintza.eus

Información general

945 236 636

info@cyberzaintza.eus

Datuak Babesteko Euskal Agintaritza
Autoridad Vasca de Protección de Datos

Brechas de Seguridad / Comunicación de persona DPD

Buzón para dudas: **evaluacion.tecnologia@avpd.eus**

Notificaciones: **Sede electrónica de la AVPD**

Información general

945 016 230

avpd@avpd.eus

Datuak Babesteko Euskal Agintaritza
Autoridad Vasca de Protección de Datos

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza

www.ciberseguridad.euskadi.eus

www.avpd.eus