NORMATIVA

COMUNICACIÓN Y GESTIÓN DE INCIDENTES

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.17	DOCUMENTO:	NORMATIVA DE COMUNICACIÓN Y GESTIÓN DE INCIDENTES

REVISIÓN NÚMERO:	1.0	FECHA DE ENTRADA EN VIGOR:	31 – Octubre - 2019

ES ORIGINAL:	☒	ES COPIA CONTROLADA:	☐	ES COPIA NO CONTROLADA:	☐

ELABORADOR POR:	REVISADO POR:	APROBADO POR:
[ÁREA]	[ÁREA]	Comité de Seguridad de la Información
[NOMBRE – INICIALES]	[NOMBRE – INICIALES]	[NOMBRE – INICIALES]
FECHA:	FECHA:	FECHA:
FIRMA:	FIRMA:	FIRMA:

CONTROL DE CAMBIOS:

REVISIÓN Nº:	FECHA:	APARTADO MODIFICADO:	CAUSA DEL CAMBIO:	ENTRADA EN VIGOR:

DOCUMENTACIÓN OBSOLETA:	☐	FECHA:	

CLASIFICACIÓN DE LA INFORMACIÓN:

SEGURIDAD

PÚBLICA:	☐	PUBLICABLE	☐	USO INTERNO	☒	CONFIDENCIAL:	☐	SECRETA:	☐

PRIVACIDAD

NO IP	☐	IP A	☒	IP B	☐	IP C	☐

Confidencialidad Acerca de este documento

AVISO: Este documento está protegido por la legislación referente a propiedad intelectual e industrial y por tratados internacionales. La utilización permitida de esta documentación queda limitada exclusivamente en relación con el Ayto. de Baeza, y todo uso no autorizado será perseguido de acuerdo con la legislación aplicable. Se prohíbe su copia, modificación, reproducción o distribución sin permiso del titular.

Excmo. Ayuntamiento de Baeza

Pje. Cardenal Benavides, 10
23440 Baeza, Jaén
ESPAÑA
http://www.baeza.es/baeza/extranet/

1) OBJETO

El objeto de la presente normativa es el de establecer la sistemática que el Excmo. Ayuntamiento de Baeza (en adelante Ayuntamiento) implantará para la detección, notificación, contención, recuperación e investigación de incidentes de seguridad, y la posterior puesta en marcha de la fase de aprendizaje frente a futuros incidentes que pudieran producirse.

2) ALCANCE

Esta normativa se aplicará a todo el personal del Ayuntamiento, que deberá notificar de manera inminente las incidencias detectadas a su responsable más inmediato. En caso de terceros, igualmente deberán notificar las incidencias detectadas al responsable más inmediato del Ayuntamiento.

Esta normativa ha sido aprobada por el Comité de Seguridad, atendiendo a las recomendaciones del Responsable de la Información, Responsable de Seguridad, Responsable del Sistema y de todos los actores intervinientes en la misma.

Cualquier modificación posterior entrará en vigor al día siguiente de su aprobación y publicación por parte del Comité de Seguridad. En este caso, la versión anterior quedará anulada por la última versión de esta normativa.

3) RESPONSABILIDADES

Será responsabilidad del Responsable del Sistema, poner en marcha las medidas definidas en esta normativa. De cada incidente de seguridad y de las medidas a adoptar será informado el responsable de seguridad de la entidad.

4) DESARROLLO NORMATIVO

4.1) INTRODUCCIÓN

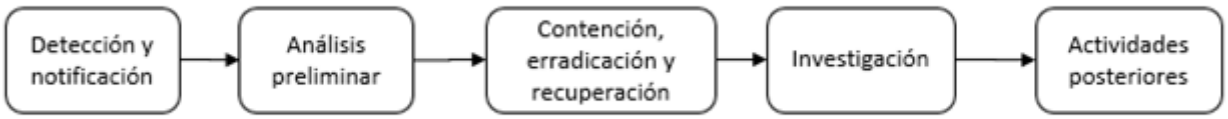
Un incidente de seguridad es cualquier evento adverso, real o potencial, vinculado a la seguridad de los sistemas informáticos o a las redes de computadoras.

Los problemas derivados de incidentes de seguridad deben ser solventados lo antes posible. La notificación de dichos problemas puede provenir de medios automatizados como sistemas de monitorización o de estadísticas de uso o informes sobre ficheros de registro de uso, así como de la notificación por parte de los propios empleados y/o usuarios del sistema.

Para garantizar una eficiente resolución de los problemas detectados es necesario definir un procedimiento ágil, eficiente y de fácil acceso para los usuarios de notificación de eventos de seguridad de la información. Es el objetivo de este procedimiento el detallar el procedimiento designado para que los usuarios reporten los puntos débiles de seguridad detectados, el procedimiento de tratamiento y escalamiento de dichas notificaciones y acciones a tomar en la resolución de los mismos.

4.2) DESCRIPCIÓN DEL PROCEDIMIENTO

Dentro de la metodología de gestión de incidentes de seguridad se abarca en este punto la detección y notificación de los eventos de seguridad.



Detección del incidente o punto débil en la seguridad de la información

Un incidente o punto en la seguridad puede ser de varias formas:

- De forma activa mediante una alarma proveniente de alguno de los sistemas de monitorización utilizados.
- De forma activa por un usuario mientras realiza su trabajo diario.

No copiar ni divulgar sin autorización previa del Ayto. de Baeza
Este documento es para uso exclusivo interno del Ayto. de Baeza

- De forma proactiva mediante la revisión de los equipos y sistemas que dan soporte al Ayuntamiento, por parte del Responsable del Sistema.

Si el incidente/punto débil es detectado por cualquier usuario del Ayuntamiento, este será reportado en el sistema de gestión de incidencias del Ayuntamiento por el propio usuario o por el responsable del departamento que reciba la incidencia.

Cualquier usuario de los sistemas del Ayuntamiento, sea empleado o un tercero subcontratado, debe notificar por medio del sistema de gestión de incidencias cualquier incidente o punto débil de seguridad detectado lo más rápidamente posible. Para ello es necesaria la publicación y lectura de este documento por parte de todos los usuarios.

Notificación del incidente o punto débil en la seguridad de la información

La notificación inicial de un incidente o punto débil de seguridad se puede producir por aviso de un usuario, del Responsable del Sistema o por alguna herramienta que envíe una alerta.

Todas las incidencias que se crean y las operaciones realizadas sobre las mismas provocan el envío de un mensaje de email hacia las personas involucradas en el incidente/punto débil de seguridad.

Al realizar esta tarea se debe contar con la información necesaria para poder iniciar el proceso de resolución del incidente reportado.

En cada notificación de un incidente/punto débil se debe disponer de los siguientes datos:

- Número de Identificación (ticket).
- Fecha y hora.
- Clasificación.
- Breve descripción.
- Efectos producidos.
- Descripción detallada.

También pueden encontrarse datos del notificador tales como:

- Nombre.
- Cargo.
- Área.
- Teléfono / Extensión interna.
- Dirección de email.

5) APRENDIZAJE DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

E.1) INTRODUCCIÓN

Mediante el procedimiento detallado en este documento se establecen las pautas y criterios que deben seguirse en la revisión de los incidentes de seguridad que se dan en el Ayuntamiento para poder implementar o mejorar controles sobre dichos incidentes que ayuden a minimizar el impacto de los mismos.

Estos controles deben buscar incidentes recurrentes de seguridad, incidentes de alta importancia cuya resolución debe ser documentada, realizar una mejora del control y resolución de los incidentes, etc.

Este proceso de aprendizaje es la última fase en el procedimiento de notificación y resolución de incidentes de seguridad.

5.2) OBJETIVO

El objetivo del procedimiento de aprendizaje de incidentes de seguridad es establecer las medidas a tomar para mejorar la calidad de resolución de incidentes de seguridad producidos en los equipos.

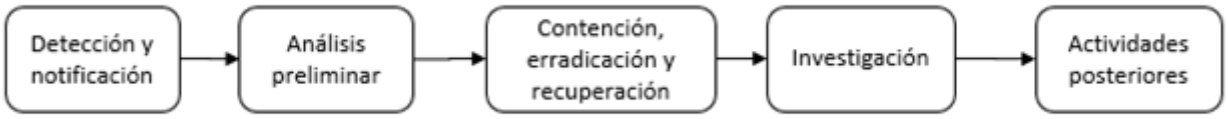
En cualquiera de los pasos que se realizan para la resolución de incidentes pueden darse situaciones o problemas que impidan una resolución ágil y eficaz de los mismos. Es objetivo de este procedimiento establecer las pautas a seguir para mejorar dicha resolución.

No copiar ni divulgar sin autorización previa del Ayto. de Baeza
Este documento es para uso exclusivo interno del Ayto. de Baeza

Es también objetivo de este procedimiento establecer las normas para realizar un estudio de los incidentes de seguridad detectados y diseñar un procedimiento para implementar o establecer controles adicionales para reducir la frecuencia de los mismos e identificar aquellos incidentes recurrentes o que supongan un gran impacto.

5.3) DESCRIPCIÓN DEL PROCEDIMIENTO

Dentro de la metodología de gestión de incidentes de seguridad se abarca en este punto la fase de actividades posteriores.



Para realizar el aprendizaje de los incidentes de seguridad detectados se establecen controles de revisión de los mismos en distintas etapas.

Durante la resolución de los incidentes de seguridad y tras el cierre de los mismos, el personal asignado a la resolución debe estar concienciado para:

- Detectar aquellos problemas que dificulten la resolución de incidentes de seguridad.
- Detectar y reportar aquellos eventos que requieran una modificación de cualquiera de las políticas de seguridad.
- Detectar y reportar aquellos incidentes de seguridad recurrentes.
- Detectar aquellas medidas de prevención que han fallado o que no existen.
- Detectar aquellas medidas de detección que han fallado o que no existen.
- Detectar aquellas medidas de notificación que han fallado o que no existen.
- Detectar aquellas medidas de contención, erradicación y recuperación que han fallado o que no existen.
- Detectar aquellas medidas correctivas que han fallado o que no existen.
- Detectar aquellas herramientas que puedan ser de utilidad para mejorar cualquier medida que haya fallado o que no exista.
- Generar y modificar la documentación necesaria en la Base de Conocimientos que permita solucionar posteriores incidentes recurrentes.

Todos estos controles y medidas mejorarán no solo la resolución de incidentes en curso, sino también futuros incidentes de seguridad, colaborando a mejorar la estabilidad y seguridad de los servicios ofrecidos.

Estos controles y medidas deben ser dados a conocer al personal encargado de la resolución de incidencias de seguridad.

Al finalizar el incidente, se pueden desarrollar los siguientes aspectos de forma detallada:

- Investigación sobre las causas y las consecuencias del incidente:
    - Estudio de la documentación generada por el equipo de respuesta a incidentes.
    - Revisión detallada de los registros de actividad (“logs”) de los equipos y dispositivos afectados por el incidente.
    - Evaluación del coste del incidente de seguridad para la organización: equipos dañados, software que se haya visto afectado, datos destruidos, horas de personal dedicado a la recuperación de los equipos y los datos, información confidencial comprometida, necesidad de soporte técnico externo, etc.
    - Análisis de las consecuencias que haya podido tener para terceros.
    - Revisión del intercambio de información sobre el incidente con otras empresas e instituciones, así como con los medios de comunicación.
    - Seguimiento de las posibles acciones legales emprendidas contra los responsables del incidente.
- Revisión de las decisiones y actuaciones del equipo de respuesta a incidentes:
    - Composición y organización del equipo.
    - Formación y nivel de desempeño de los miembros.

Excmo. Ayuntamiento de Baeza
No copiar ni divulgar sin autorización previa del Ayto. de Baeza
Este documento es para uso exclusivo interno del Ayto. de Baeza

    - Rapidez en las actuaciones y decisiones: ¿cómo respondió el personal involucrado en el incidente?, ¿qué tipo de información se obtuvo para gestionar el incidente?, ¿qué decisiones se adoptaron?.
- Análisis de los procedimientos y de los medios técnicos empleados en la respuesta al incidente:
    - Redefinición, actualización y mejora de aquellos procedimientos que no hayan resultado adecuados basándose en la experiencia obtenida en la resolución del incidente de seguridad. Esta revisión puede conllevar la modificación no solo de documentos en la Base de Conocimientos, sino también de procedimientos, políticas y cualquier otra documentación generada alrededor del sistema y de las medidas de seguridad implantadas en el mismo.
    - Organización, en caso necesario, de reuniones con los usuarios y/o técnicos involucrados en la incidencia para discutir las causas y soluciones adoptadas.
    - Adopción de las medidas correctivas que se consideren necesarias para mejorar la respuesta ante futuros incidentes de seguridad.
    - Revisión de las medidas de control existentes e implementación de medidas de control preventivas adicionales que no estén ya siendo aplicadas según se hayan detectado y analizado en la fase de resolución del incidente de seguridad.
    - Adquisición de herramientas y recursos para reforzar la seguridad del sistema y la respuesta ante futuros incidentes de seguridad.
- Revisión de las Políticas de Seguridad de la organización:
    - Definición de nuevas directrices y revisión de las actualmente previstas por la organización para reforzar la seguridad de su sistema informático.

De forma periódica se realizará una auditoría de los incidentes de seguridad reportados para aplicar los controles detallados anteriormente, detectando los problemas que no se han identificado en el momento de su resolución y aplicando las medidas necesarias para evitarlos en un futuro.

Esta revisión podría tener en cuenta:

- Costes de resolución de incidentes.
- Incidentes que se dan de forma recurrente.
- Impacto de los distintos tipos de incidentes que se producen.
- Otros daños producidos por los incidentes.

6) RECOPILACIÓN DE EVIDENCIAS

6.1) INTRODUCCIÓN

Mediante el procedimiento detallado en este documento se establecen las pautas y criterios que deben seguirse en la recopilación de datos y evidencias cuando se dan incidentes de seguridad en el Ayuntamiento para implementar una recogida de evidencias que pueda ser presentada como prueba en procesos disciplinarios contra empleados de la entidad o en acciones legales contra personas o entidades externas.

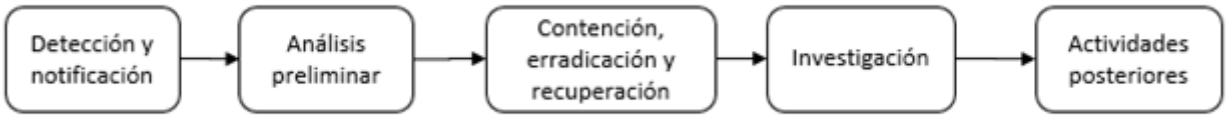
6.2) OBJETIVO

El objetivo del procedimiento de recopilación de evidencias es especificar los procedimientos y normas internas que deben observarse cuando se recogen y almacenan las evidencias necesarias para la realización de una acción disciplinaria dentro de la entidad o cuando se realiza una acción legal (civil o criminal) contra terceros después de un incidente de seguridad.

6.3) DESCRIPCIÓN DEL PROCEDIMIENTO

Dentro de la metodología de gestión de incidentes de seguridad se abarca en este punto la fase de Investigación.

No copiar ni divulgar sin autorización previa del Ayto. de Baeza
Este documento es para uso exclusivo interno del Ayto. de Baeza



Una vez que se ha contenido, erradicado y recuperado de las consecuencias del incidente de seguridad se debe proceder a realizar la investigación de las causas que han originado el mismo. Este proceso podría ser necesario para tomar acciones legales contra terceros ajenos al departamento o para tomar acciones disciplinarias contra empleados de la entidad que hayan puesto en riesgo la seguridad de la información que esta maneja.

¿Qué tipo de evidencias deben recopilarse cuando nos enfrentamos con un incidente de seguridad? Debe recopilarse la siguiente información:

- Información de los equipos y/o aplicaciones tales como fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la red, backups, archivos copiados recientemente, etc.
- Información basada en equipos de red tales como ficheros de log de IDSs, logs de los sistemas de monitorización, información recolectada mediante sniffers, logs de routers, logs de firewalls, información de servidores de autenticación, etc.
- Información recopilada mediante conversaciones con las personas involucradas en cualquiera de las fases por las que pasa el incidente de seguridad.

Para realizar la investigación de un incidente deben recolectarse las evidencias que confirmen la existencia del incidente. Para ello deben cumplirse las siguientes propiedades en la recolección de evidencias:

- **Autenticidad.** Quien haya recolectado la evidencia debe poder probar que es auténtica y que no ha sido modificada, almacenándola en un lugar seguro y restringiendo el acceso a la misma.
- **Cadena de custodia.** Registro detallado del tratamiento de la evidencia, incluyendo quienes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.
- **Validación.** Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

Como se consigue cumplir las propiedades anteriormente descritas:

- **Autenticidad.** Para garantizar la autenticidad de las evidencias recopiladas estas serán tratadas tomando las siguientes medidas:
    - Se almacenarán en un lugar seguro con acceso restringido. La información en formato electrónico se almacenará en el sistema de gestión de incidencias. Las evidencias que no estén disponibles en formato electrónico se almacenarán en lugar seguro en las instalaciones del Ayuntamiento.
- **Cadena de custodia.** Se registrarán todas las actividades realizadas con las evidencias recopiladas tomando las siguientes medidas:
    - Se registrará en el sistema de incidencias todo acceso a las evidencias, incluyendo donde han sido conseguidas (equipo, rutas, aplicaciones), quiénes, cuándo y de qué forma se han realizado los accesos a dichas evidencias.
    - El acceso al sistema de gestión de incidencias se realiza de forma segura, estando restringido el acceso a estas incidencias al número mínimo de personas para gestionarlo y tratarlo.
    - Las evidencias recopiladas deben ser preservadas para evitar su alteración. En caso de pruebas físicas estas serán almacenadas en lugar seguro en las instalaciones del Ayuntamiento.
- **Validación.** Toda la información que se recopila se almacena de forma segura en el sistema definido en el Ayuntamiento. Para ello se tomas las siguientes medidas:
    - Se restringe el acceso a la información solo a personal autorizado
    - El ticket abierto en el sistema de gestión de incidencias no puede ser eliminado ni alteradas las notas registradas en el mismo para cada incidente detectado y reportado.

Excmo. Ayuntamiento de Baeza
No copiar ni divulgar sin autorización previa del Ayto. de Baeza
Este documento es para uso exclusivo interno del Ayto. de Baeza

- Las evidencias en formato electrónico serán incorporadas al sistema de gestión de incidencias.
- Las evidencias en otro formato serán almacenadas en un sitio seguro (archivo del departamento legal) y, a ser posible, serán digitalizadas e incorporadas al sistema de gestión de incidencias.

Durante el proceso de recolección de evidencias deben seguirse estos pasos:

- Registrar toda la información que rodea a la evidencia. Debe realizarse siempre en el sistema de gestión de incidencias descrito en el documento *"Procedimiento de Notificación y Gestión de eventos de seguridad".* Aquella información no disponible en el registro de incidencias puede estar ubicada en el servidor de registro donde se almacenan los registros de eventos y sucesos de los equipos monitorizados. Se debe indicar las configuraciones de los equipos que han sufrido la incidencia, fecha y hora del sistema y de los distintos eventos registrados, nombres de ficheros utilizados y en general todos los hallazgos recopilados que puedan aportar luz en el proceso de análisis de las incidencias de seguridad.
- Tomar fotografías del entorno de la evidencia en caso de ser necesario.
- Recopilar las evidencias generadas por los distintos sistemas y servicios durante el incidente de seguridad reportado para su análisis y utilización durante todo el proceso de gestión de la incidencia.
- Registrar la evidencia en el sistema de gestión de incidentes dentro del ticket abierto para la incidencia reportada, indicando donde ha sido almacenada y qué personas están autorizadas a acceder a las evidencias.
- Rotular todos los medios que serán tomados como evidencia para poder ser catalogados y referenciados en la documentación generada acerca de la incidencia de seguridad.
- Almacenar toda la evidencia en forma segura. Todas las evidencias de incidentes de seguridad deben almacenarse de forma segura. Para ello se dispone de medidas de seguridad implementadas en el sistema de gestión de incidencias, el cual es el principal repositorio de información en el que se almacenan las evidencias de dichas incidencias. El acceso a la información está restringido al Responsable del Sistema o la/s persona/s en quien delegue, y a los usuarios que hayan detectado y reportado la incidencia. En ningún caso se permite la modificación o eliminación de información en la incidencia reportada.
- Realizar las investigaciones en "duplicados de trabajo" de la evidencia original. Nunca debe trabajarse con los ficheros originales, realizándose copias de los mismos. Esta copia de ficheros debe realizarse únicamente por personal autorizado. Se debe registrar el proceso realizado para la copia de dichos ficheros, mediante qué herramientas se ha realizado, qué personas han realizado la copia de los datos y cuando ha sido realizada. Esta misma información debe registrarse cuando se destruya la información copiada después de su utilización.
- Generar copias de seguridad de las evidencias originales. Se realizan copias de seguridad de los ficheros de registro que se generan como parte del sistema de generación de copias de seguridad especificado en el documento "*Política de Copias de seguridad, restauración y verificación".* Se generan así mismo copias de seguridad de las evidencias de los incidentes de seguridad reportados, bien a través del método descrito anteriormente o a través de la realización de copias de seguridad adicionales de los sistemas donde se almacenan dichas evidencias, así como del sistema de gestión de incidencias donde se reportan todos los incidentes y su ciclo de vida.
- Realizar revisiones periódicas para garantizar que la evidencia se encuentra correctamente conservada. Cada semana se realiza una revisión del almacenamiento y acceso a las evidencias almacenadas necesarias para la realización de acciones legales o procedimientos disciplinarios.

En caso de ser necesario se solicitará la asistencia del Secretario de la entidad que ofrezca el asesoramiento y se encargue el proceso que pueda abrirse de forma legal contra terceros debidos a incidentes de seguridad detectados y reportados.

6.4) HERRAMIENTAS Y REGISTROS QUE PUEDEN USARSE PARA RECOPILAR EVIDENCIAS

Para la recopilación de evidencias pueden utilizarse los siguientes registros (que pueden estar localizados bien en los propios equipos o en el servidor donde se almacenan los registro):

- Registros de Eventos de Aplicación, Seguridad y Sistema de los equipos Windows.
- Registros de acceso y errores de servidores web.
- Registros de las aplicaciones de correo.
- Registros de los antivirus.
- Registros de los firewalls.
- Registros de auditoría y seguridad de las aplicaciones instaladas.

Excmo. Ayuntamiento de Baeza
No copiar ni divulgar sin autorización previa del Ayto. de Baeza
Este documento es para uso exclusivo interno del Ayto. de Baeza

- Registros de auditoría del gestor de base de datos.

Pueden utilizarse herramientas de análisis de sistemas para la recopilación de evidencias y pruebas de los incidentes de seguridad. Estas herramientas pueden ser herramientas incorporadas dentro del propio sistema operativo o herramientas de terceros de auditorÍa de los sistemas y aplicaciones.

Las evidencias tomadas a través de todas estas fuentes se recopilarán e incluirán en el sistema de gestión de incidencias.

7) RESPONSABLE DEL CUMPLIMIENTO

Será responsabilidad del Responsable de Seguridad velar por el cumplimiento de la presente normativa, con el consenso del Responsable del Sistema.

8) REFERENCIAS

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Guía de Seguridad CCN-STIC 821: Normas de Seguridad.
- Guía de Seguridad de las TIC CCN-STIC 883: Guía de Implantación del ENS para Entidades Locales.
- Guía de Seguridad CCN-STIC 804: Guía de Implantación.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- RGPD (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.
- Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de derechos digitales.
- Política de Copias de seguridad, restauración y verificación.
- Procedimiento de Notificación y Gestión de eventos de seguridad.
- Procedimiento de Gestión de Vulnerabilidades Técnicas.
- Procedimiento de Gestión de Cambios y Versiones.

9) REGISTROS/ANEXOS

Excmo. Ayuntamiento de Baeza
No copiar ni divulgar sin autorización previa del Ayto. de Baeza
Este documento es para uso exclusivo interno del Ayto. de Baeza