POLÍTICAS DE PROTECCIÓN DE DATOS DE Athento Europa, S.L.

Política de privacidad general

1. Objeto y ámbito de aplicación

Esta política:

- Establece el compromiso de Athento Europa, S.L. de confidencialidad de la información personal y sus responsabilidades con respecto a la divulgación de dicha información;
- Tiene por objeto garantizar que todo el personal, ya sea empleado directamente o contratado, sea consciente de sus responsabilidades en relación con la confidencialidad de la información personal; y
- Se aplica a todo el personal de Athento Europa, S.L. incluyendo personal temporal y de agencia, contratistas y voluntarios y a la información personal registrada en cualquier formato, incluyendo papel, electrónico y cualquier otro medio.

2. Responsabilidades

Todos los empleados, contratistas y asociados comparten la responsabilidad de asegurar que los activos de información se manejen de acuerdo con esta política.

3. Definiciones

Datos: Información tal y como se define en la ley de protección de datos, es decir:

- Procesada electrónicamente, es decir, sistemas de información, bases de datos, microfichas, sistemas de audio y vídeo (CCTV) y sistemas de registro telefónico;
- Registrada con la intención de que sea procesado por el equipo; o
- Registrada como parte de un sistema de archivo pertinente, es decir, estructurada, ya sea por referencia a personas físicas o por referencia a criterios relativos a personas físicas a los que se puede acceder fácilmente.

Responsable del tratamiento: La persona, empresa u organización que determina la finalidad y la forma en que pueden tratarse los datos personales.

Encargado del tratamiento : Cualquier persona que trate datos personales por cuenta del responsable del tratamiento;

Interesado: Toda persona titular de los datos que sean objeto del tratamiento.

Divulgación: La divulgación o provisión de acceso a los datos.

Datos personales confidenciales: Información personal sobre individuos identificados o identificables, que debe mantenerse privada o secreta . Información personal incluye la definición de datos personales del Reglamento General de Protección de Datos (RGPD), pero está adaptada para incluir tanto a las personas muertas como a las vivas y "confidencial" incluye tanto la información "entregada con carácter confidencial" como "lo que se le debe como un deber de confianza", y está adaptada para incluir la información "sensible" tal como se define en la ley de protección de datos.

Información personal: Información que se refiere a una persona viva que puede ser identificada a partir de la información que esté en posesión del responsable del tratamiento o que pueda llegar a estarlo.

Tratamiento: Usar la información de las siguientes maneras:

- Obtención
- Grabación
- Recuperación
- Alteración
- Revelación de información
- Destrucción
- Uso
- Transmisión
- Eliminación

Datos personales de categoría especial (formalmente conocidos como datos personales sensibles): es cualquier información sobre una persona relativa a su persona:

- Raza
- Origen étnico
- Política
- Religión
- Afiliación sindical
- Genética
- Biometría (cuando se utiliza para fines de identificación)
- Salud
- Vida sexual
- Orientación sexual

Terceros: Cualquier persona que no sea:

- El interesado;
- El responsable del tratamiento; y
- Cualquier encargado del tratamiento u otra persona autorizada para el tratamiento por cuenta del responsable del tratamiento.

4 . Protección de datos

Los principios de la protección de datos

La ley de protección de datos establece los siguientes principios para apoyar las buenas prácticas y la imparcialidad en el tratamiento de la información personal. Estos principios estipulan que:

- Los datos personales deben tratarse de forma legal, justa y transparente;
- Los datos personales sólo pueden ser recogidos para fines específicos, explícitos y legítimos;
- Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para su tratamiento;
- Los datos personales deben ser exactos y mantenerse actualizados con todos los esfuerzos para borrar o rectificar sin demora;
- Los datos personales deberán conservarse en una forma que permita identificar al interesado sólo durante el tiempo necesario para su tratamiento;
- Los datos personales deben ser tratados de manera que se garantice la seguridad adecuada; y
- El responsable del tratamiento debe poder demostrar el cumplimiento de los demás principios de protección de datos (responsabilidad proactiva).

Seguridad de la información

Con el fin de garantizar la confidencialidad de la información personal, se requieren sistemas y procedimientos para controlar el acceso a dicha información. Dichos controles son esenciales para garantizar que sólo lo han hecho las

personas autorizadas:
Acceso físico al hardware y al equipo informático;
Acceso a utilidades del sistema informático capaces de anular el sistema y los controles de acceso, por ejemplo, los derechos de administrador; y
Acceso a registros electrónicos o en papel que contengan información confidencial sobre las personas.

Las responsabilidades de confidencialidad y tratamiento adecuado de Athento Europa, S.L. de los datos personales se mantienen incluso si el tratamiento es realizado por un tercero.

Acceso a la información personal

Las personas que actúen en su nombre con su consentimiento tienen derecho de acceso a los datos que obren en su poder. Esto incluye el acceso a los registros de auditoría que indican quién ha accedido a sus datos personales o confidenciales.

5. Confidencialidad

Deber de confidencialidad

Todo el personal y los contratistas deben reconocer que la confidencialidad es una obligación. Cualquier abuso de confianza, uso inapropiado de los registros o abuso de los sistemas informáticos puede dar lugar a procedimientos disciplinarios y procedimientos judiciales.

El personal temporal y voluntario de la agencia también está sujeto a dichas obligaciones y debe firmar un acuerdo de confidencialidad cuando trabaje para o en nombre de Athento Europa, S.L..

El personal debe tener la seguridad de que existe una base legal antes de compartir la información. Cualquier pregunta sobre la legitimidad de compartir información debe dirigirse al Gerente de Seguridad de la Información.

Cualquier intercambio ilegal de datos personales o confidenciales que se lleve a cabo debe ser reportado como un incidente e investigado de acuerdo con el Procedimiento de Gestión de Incidentes de Seguridad.

Objeciones al tratamiento de datos confidenciales

Cualquier duda u objeción sobre el tratamiento de los datos personales será remitida inmediatamente al Responsable de Seguridad de la Información. Cuando Athento Europa, S.L. actúe como procesador de datos bajo contrato, la consulta se remitirá al responsable del tratamiento.

6. Evaluaciones de impacto de la protección de datos (PIA)

Las nuevas iniciativas que impliquen un tratamiento de alto riesgo de los datos personales se someterán a una PIA para garantizar el mantenimiento de la privacidad y la seguridad de los datos personales confidenciales.

7. Mapeo de flujo de información

Los flujos de información personal que entran y salen de Athento Europa, S.L. se mapearán en los informes de PIA.

8. Transferencias internacionales

La información de identificación personal no debe transferirse fuera de los EEE a menos que se haya llevado a cabo una evaluación adecuada del riesgo y se hayan establecido controles atenuantes.

Athento Europa, S.L. debe revisar los flujos de información personal identificable para entender si la información transferida a organizaciones externas fluye fuera del Reino Unido y del EEE.

Las decisiones sobre la transferencia de información de identificación personal sólo deben ser tomadas por un alto directivo que haya sido autorizado para tomar esa decisión.

Las organizaciones necesitarán obtener una declaración de garantía de terceros que procesen los datos personales de sus usuarios o personal en el extranjero. Esta garantía puede estar dentro del contrato entre las dos organizaciones o dentro de otros términos de procesamiento.

9. Implementación

El Gerente de Seguridad de la Información es responsable de asegurar que el personal relevante dentro de Athento Europa, S.L. haya leído y entendido este documento.

Propietario y aprobación del documento

El Director de Seguridad de la Información es el propietario de este documento y es responsable de asegurar que este procedimiento se revise de acuerdo con los requisitos de revisión establecidos en esta política.

Firma:

Plan de contingencia interno

El objetivo del plan de contingencia es garantizar la continuidad de las actividades y facilitar el aseguramiento, la confidencialidad y la integridad de los datos personales y de la información, así como de los equipos y activos que la procesan.

Ámbito de aplicación

El plan de contingencia hace referencia al conjunto de activos de Athento Europa, S.L., en especial a los sistemas informáticos (*hardware* y *software*), soportes documentales, infraestructura y personal.

El plan de contingencia debe aplicarse con anterioridad a la materialización de un incidente de seguridad, durante el propio incidente y posteriormente, a fin de recuperar el funcionamiento normal de la organización.

Este plan se complementa con la evaluación de riesgos y el registro de equipos e inventarios, los cuales se han tenido en cuenta para la elaboración del mismo, así como con el resto de las políticas internas de la organización.

Medidas preventivas

Athento Europa, S.L. ha diseñado e implementado las siguientes medidas de seguridad para mitigar los riesgos y evitar un incidente de seguridad en materia de protección de datos:

- Política de almacenamiento seguro de los datos personales
- Política de cifrado de la información
- Política de control de acceso a los datos personales
- Política de actualización de software y hardware
- Política de denuncias internas
- Política de destrucción y reutilización de equipos y soportes
- Política de formación en protección de datos
- Política de traslado de soportes
- Política de respaldo
- Política de uso adecuado de internet y redes wifi
- Política uso de contraseñas

Medidas de contención

En caso de producirse un incidente de seguridad, Athento Europa, S.L. ha establecido las siguientes medidas para contener el incidente y evitar mayores consecuencias:

- **Impedir el acceso al origen de la brecha de seguridad:** Siempre que sea posible debe impedirse al acceso al dominio, conexión, equipo, puerto, actualización u origen del incidente de seguridad para bloquear el ataque.
- **Cambiar todas las credenciales de acceso a información privilegiada:** Deben suspenderse las credenciales y, en caso de ser necesario, cambiarlas o hacer que los usuarios lo hagan de manera segura.
- **Copia del sistema (clonado):** Realizar copias bit a bit del disco duro y analizar la copia por medio de herramientas forenses a fin de determinar el origen y alcance de la incidencia.
- **Aislar el sistema:** Aislar el sistema para revelar los datos con la finalidad de realizar el pertinente análisis.
- **Eliminación de los datos divulgados:** En caso de que los datos personales se hayan divulgado, solicitar que se eliminen estos datos personales.
- **Control de la difusión de los datos filtrados:** Especialmente cuando los datos personales sean sensibles se deberá realizar una vigilancia de su difusión en sitios web y redes sociales.

Medidas de erradicación

Finalmente, una vez contenido el incidente, deben tomarse las medidas necesarias para la erradicación completa del mismo. Athento Europa, S.L. ha establecido las siguientes medidas:

- **Definición de un proceso de desinfección:** Este proceso se debe basar en firmas, herramientas, nuevas versiones/revisiones de software, etc. Antes de implementarse se debe probar que el proceso funciona adecuadamente y asegurar que no se van a producir daños en los servicios y en los datos personales.
- **Comprobación de la integridad de todos los datos personales almacenados en el sistema:** Se debe realizar mediante un sistema que garantice que los datos personales no han sido modificados, prestando especial atención a los archivos del sistema ejecutables.
- **Revisión de las actualizaciones y antivirus.**
- **Análisis con antivirus de todo el sistema.**
- **Restaurar las conexione s y los permisos:** Debe realizarse de forma paulatina, especialmente debe asegurarse la integridad de los accesos remotos.

Informe y notificación del incidente

El incidente y todo el proceso de recuperación debe quedar documentado a fin de poder comunicarlo a las personas interesadas así como poder elaborar un informe que analice la situación y permita obtener conclusiones para revisar el plan de prevención.

Es importante obtener evidencias de todo lo acontecido que pueden ser utilizadas como prueba en procedimientos sancionadores y judiciales.

Durante el transcurso del incidente y su posterior solución debe mantenerse la comunicación entre el responsable de seguridad y la gerencia de la organización. Es recomendable realizar un informe que contenga los siguientes puntos:

- Descripción del incidente: alcance e impacto
- Controles preventivos existentes
- Medidas de respuesta tomadas y su impacto en la resolución del incidente
- Acciones para la prevención de futuros incidentes
- Probabilidad de que el incidente se repita ante una casuística igual
- Medidas de detección aplicadas
- Registro de comunicaciones durante la respuesta al incidente

Debe recordarse que, al margen de la implementación de estas medidas y de la documentación del proceso, debe notificarse el incidente a la autoridad de control competente.

El artículo 33 del RGPD establece que la notificación de las brechas de seguridad que afecten a datos personales debe realizarse sin dilación indebida y, de ser posible, a más tardar 72 horas después de su detección, a menos que sea improbable que constituya un riesgo para los derechos y libertades de las personas físicas.

Lo más recomendable es comunicar el incidente a la autoridad de control durante las 72 horas siguientes a su detección ya que, posteriormente, se podrán realizar notificaciones complementarias que aclaren todo aquello que no se hubiera podido comunicar en la notificación inicial.

Asimismo, en caso de que el incidente pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas, se deberá comunicar a los afectados el incidente sin delación indebida, tal y como establece el artículo 34 del RGPD.

Política de control de acceso a datos personales

La presente política se ha redactado en atención a la normativa de protección de datos y a la norma ISO 27002:2005 de buenas prácticas para la gestión de la seguridad de la información.

El objetivo de esta política es impedir el acceso no autorizado a los datos personales, garantizando así la seguridad y confidencialidad de estos.

Medidas implementadas

Athento Europa, S.L. ha establecido las siguientes medidas de seguridad:

- Los empleados solo tendrán acceso a aquellos recursos y datos que precisen para el desarrollo y cumplimiento de sus funciones.
- Se determinará la relación de usuarios y los accesos autorizados para cada uno de ellos en un registro de personal.
- Se han establecido mecanismos para evitar que una persona acceda a datos distintos de los autorizados mediante procedimientos de identificación y autentificación como un sistema de usuarios y contraseñas.
- Queda expresamente prohibido compartir contraseñas y/o escribir las contraseñas en un lugar visible.
- Únicamente las personas autorizadas para ello podrán conceder, alterar o anular las autorizaciones de acceso a los datos personales de los demás empleados.
- En línea con la Política de almacenamiento seguro de los datos, el acceso a documentos físicos se realizará mediante uso de llaves u otras medidas de seguridad.

Política de información de los interesados

En el capítulo III, sección 2 del 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 señala la importancia de la de la información, concretamente en los artículos 13 y 14.

Para realizar la presente política se ha tomado como referencia, además de la normativa en protección de datos, la norma ISO/IEC 27001 en materia de seguridad de la información. La citada norma, menciona la adecuada comunicación y seguimiento de la información. Además, implementa un sistema de reconocimiento de riesgos basado en los controles de la norma ISO/IEC 27002 que identifica las amenazas de la seguridad de los datos personales y de la información que se trata en la empresa.

Athento Europa, S.L., ha adecuado una política o protocolo para dar cumplimiento a la obligación de informar a los interesados sobre las circunstancias relativas al tratamiento de sus datos en el momento en que se solicite, en virtud del principio de transparencia. En el supuesto de que los datos no se obtengan del propio interesado, por obtenerse de alguna cesión legítima, o de fuentes de acceso público, el Responsable informará a las personas interesadas dentro de un plazo conveniente, pero en cualquier caso:

- Antes de un mes desde que recibieron los datos personales.
- Antes o en la primera notificación con el interesado
- Antes de que los datos personales, se hayan notificado a otros destinatarios.

Esta información se debe llevar a cabo sin obligación de requerimiento, con un lenguaje claro y sencillo, de forma concisa, transparente, inteligible y de fácil acceso. El responsable deberá poder autentificar con posterioridad que la información ha sido realizada.

La empresa procederá a la recogida de datos mediante los siguientes modos:

- Formularios en papel.
- Navegación o formularios Web
- Datos de actividad personal
- Entrevista telefónica
- Registro de aplicaciones móviles

Por otra parte, las comunicaciones al interesado sobre datos ya disponibles, o tratamientos adicionales, pueden hacerse llegar mediante los siguientes métodos:

- Correo postal
- Notificaciones emergentes en servicios y aplicaciones
- Mensajería electrónica

Política de ejercicios de derechos

De acuerdo con la normativa aplicable en materia de protección de datos, los interesados podrán solicitar, al responsable o corresponsables si hubiera, los siguientes derechos:

- Derecho de acceso.
- Derecho de supresión, - conocido como derecho al olvido.
- Derecho de rectificación.
- Derecho a la limitación en el tratamiento.
- Derecho a la portabilidad.
- Derecho de oposición.
- Derecho a no ser objeto de decisiones individuales automatizadas, en la cual se incluye la elaboración de perfiles.

El responsable del tratamiento o DPO, deberá actuar de forma diligente en la resolución del ejercicio de los derechos descritos anteriormente, en la forma y el plazo que se determinan para hacerlo. La omisión en la respuesta a los derechos conlleva graves sanciones para quien esté obligado a hacerlo.

En la presente política general se regulan los aspectos a tener en cuenta en el procedimiento del ejercicio de derechos por parte del Responsable o Delegado de protección de datos.

Solicitantes de los derechos

De acuerdo con el artículo 12 de la Ley Orgánica de Protección de Datos, los derechos descritos se podrán ejercer directamente por el interesado, o por medio de un representante legal o voluntario designado debidamente por el interesado.

La solicitud de los derechos siempre deberá ser atendida por el responsable o delegado de protección de datos, sin embargo podrá ser denegada, debidamente justificada, cuando en la misma no se acredite quién es la persona que lo solicitan.

Procedimiento en el ejercicio de los derechos

El coste del procedimiento para el ejercicio de los derechos será en principio gratuito, a excepción de que comporte manifestaciones infundadas o excesivas, y con un componente reiterado, donde el responsable, de acuerdo con los artículos 12 y ss del RGPD, podrá obrar un canon razonable en función de los costes afrontados para dar respuesta a la referida solicitud.

El responsable del tratamiento adquiere la carga de la prueba para demostrar y justificar el carácter infundado o excesivo de la solicitud.

El procedimiento que ha adoptado la empresa es el siguiente:

Se deberá dirigir la comunicación al responsable a través de cualquier medio puesto a disposición de los interesados y que previamente ha sido informado.

A título informativo, la referida comunicación por parte de los interesados debe contener como mínimo los siguientes datos: nombre y apellidos del interesado, fotocopia del D.N.I. o N.I.E., y en su caso, si se realizara a través de representante, el D.N.I. del mismo y el documento que acredite la representación, descripción de la petición detallada en que se concreta la solicitud, dirección electrónica a efectos de notificaciones, fecha y firma del solicitante.

El plazo para responder a las consultas de los afectados debe ser el menor tiempo posible desde la recepción de la solicitud, con un máximo de un mes y la posibilidad de prorrogarse dos meses más en el caso de ser necesario, teniendo en cuenta la complejidad de la misma y el número de solicitudes recibidas.

Política de formación en protección de datos

El 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 señala la importancia de la formación a sus trabajadores y colaboradores externos en diferentes artículos (en adelante, RGPD). En concreto el artículo 28 en las funciones del Encargado del Tratamiento, asimismo el artículo 39 señala que una de las funciones del Delegado de Protección de Datos es la relevancia y formación de los trabajadores y colaboradores externos y el artículo 47 relacionado al contenido de las normas vinculantes sobre la formación de datos.

Athento Europa, S.L., ha adecuado una política para que sus trabajadores tengan una formación en protección de datos con el fin de garantizar el cumplimiento normativo del programa implementado en la empresa.

De este modo, se formará a los trabajadores de manera continua en la referida materia con el fin de evitar posibles brechas de seguridad y una posterior sanción económica por incumplimientos por parte de los trabajadores en la gestión de los datos.

Athento Europa, S.L., Empresa quien realiza la adecuación o el DPO es el encargado de realizar la formación de la siguiente forma:

- Se enviará una circular informativa mediante correo electrónico a todos los trabajadores donde se recogerá el día, hora y lugar donde se realizará la formación en protección de datos.
- Las sesiones formativas se impartirán de forma bimensual para actualizar e informar de los diferentes conceptos a los trabajadores y posibles colaboradores en materia de seguridad de datos, así como de las novedades e información de interés para el sector en que opere la empresa.
- La formación puede ser presencial u online. En las sesiones formativas, los trabajadores pueden preguntar sobre las dudas o cuestiones que les interesen, así como contar con ejemplos prácticos.
- Una vez concluida la formación, los participantes de la misma firmarán el acta de acuerdo han recibido la formación impartida, la cual será una evidencia de la responsabilidad proactiva en materia de protección de datos.
- La formación se personaliza de acuerdo con los diferentes departamentos de la empresa, así como del acceso a los datos por cada trabajador y el nivel de los mismos, en cuanto sean sensibles o no.

El cumplimiento de la referida política es obligatoria para todos los integrantes de la empresa. Y por ello, todos los trabajadores han sido informados de las medidas a seguir para dar cumplimiento a la misma. Se evidencia así, la existencia de un protocolo para ejercer la formación por parte del interesado, y resolver las solicitudes recibidas sin dilaciones indebidas.

Así mismo, Athento Europa, S.L., ha adoptado todas las medidas de seguridad establecidas en la legislación actual sobre protección de datos, en el caso de vulnerarse las referidas medidas, el afectado debe poner en conocimiento al responsable de seguridad.

Política de desconexión digital

De acuerdo con el artículo 88 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales (en adelante, LOPDGDD) la empresa quiere resaltar la importancia de garantizar el derecho a la desconexión digital y por ello, reconoce a todos sus trabajadores la referida desconexión digital fuera de su jornada laboral, con la máxima de garantizar el derecho a intimidad de los mismos.

Athento Europa, S.L. ha adoptado una política o protocolo que regula el derecho a la desconexión digital en el contexto del derecho a la intimidad por el uso de los dispositivos electrónicos en el ámbito laboral de acuerdo con la LOPDGDD. Más concretamente se han diseñado e implementado las siguientes medidas:

- Los empleados tienen el derecho de dejar los dispositivos digitales, como pueden ser móviles, tablets u ordenadores portátiles en el puesto de trabajo, sin que en ningún caso se les pueda exigir que hagan uso de los mismos fuera de su jornada laboral.
- Los empleados tienen derecho a no acceder a su correo electrónico de empresa cuando no se encuentren en su lugar y horario de trabajo.
- En ningún caso los empleados podrán ser sancionados por el hecho de no responder a llamadas o correos electrónicos fuera de su horario de trabajo.
- Se fomentará el derecho a la desconexión digital, en los casos de aquellos trabajadores que realicen funciones laborales desde el domicilio particular de los mismos, tomando todas las medidas necesarias para ello.

El cumplimiento de la referida política es obligatoria para todos los integrantes de la empresa. Y por ello, todos los trabajadores han sido informados del procedimiento a seguir para dar cumplimiento a la misma. Se evidencia así, la existencia de un protocolo para ejercer el referido derecho por parte del interesado, y resolver las solicitudes recibidas sin dilaciones indebidas.

Así mismo, Athento Europa, S.L. ha adoptado todas las medidas de seguridad establecidas en la legislación actual sobre protección datos, en el caso de vulnerarse el referido derecho, el afectado podrá ejercer el mismo, mediante escrito dirigido a:

Responsable del tratamiento: Athento Europa, S.L.

N .I.F: B92688365

Dirección: Iván Pavlov 2, Planta 2, Oficina 3, Edificio Hevimar II, Parque Tecnológico de Andalucía, 29590, Campanillas, Málaga

DPO/Responsable de Seguridad: athento@athento.com

Política de denuncias internas

Athento Europa, S.L., en virtud del artículo 24 de la LOPDGDD ha implementado un canal de denuncias internas o whistleblowing a fin de facilitar la posibilidad de que los empleados o terceros pongan en conocimiento de la empresa la comisión de actos contrarios a la normativa general o sectorial de protección de datos aplicable cometidos por parte de empleados de la organización o por parte de terceros que contratan con Athento Europa, S.L..

Las denuncias internas se podrán realizar incluso de forma anónima, preservando la identidad del denunciante. En caso de que la persona denunciante se hubiera identificado deberán adoptarse las medidas necesarias para preservar su identidad y garantizar la confidencialidad de sus datos, así como los de las personas afectadas.

Plazo de conservación de los datos

Los datos de la persona que formula la comunicación, de los empleados y terceros se conservarán en el sistema de denuncias internas durante el tiempo imprescindible para la decisión sobre la procedencia o improcedencia de la iniciación de una investigación sobre los hechos objeto de la denuncia.

El plazo de conservación general de dichos datos es de tres meses desde la introducción de los mismos, transcurrido dicho plazo se procederá a la supresión de los mismos, excepto que su conservación tenga como finalidad dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica (compliance penal).

Sin perjuicio de su conservación por un plazo superior a los tres meses establecidos, los datos de las denuncias se podrán conservar de forma anonimizada, sin necesidad de proceder al bloqueo de los datos.

Asimismo, los datos podrán tratarse por un plazo superior a los tres meses para la investigación de los hechos denunciados, siempre que no se conserven en el sistema de información de denuncias internas.

Acceso a los datos del sistema de información de denuncias internas

Únicamente podrán acceder a los datos contenidos en el canal de denuncias internas quienes tengan encomendadas las funciones de control interno y de cumplimiento o compliance, pudiendo tratarse de personas que formen o no parte de la organización o los encargados del tratamiento designados para la realización de estas funciones. Asimismo, podrán acceder otras personas cuando ello resulte necesario para la adopción de medidas disciplinarias o para la tramitación de procedimientos judiciales.

Se notificará a la autoridad competente los hechos que se incardinen como ilícitos penales o administrativos, pudiendo permitir el acceso al personal encargado de la gestión y control de recursos humanos únicamente cuando proceda adoptar medidas disciplinarias contra un trabajador.

Política de almacenamiento seguro de datos

Para realizar la presente política se ha tomado como referencia, además de la normativa en protección de datos, la norma ISO/IEC 27040:2015, que alude al almacenamiento seguro de datos, teniendo como objetivo prestar atención a los riesgos, ayudar a las organizaciones en un mejor aseguramiento de sus datos almacenados y proporciona una base para la auditoría, el diseño y la revisión de los controles de seguridad de almacenamiento.

Athento Europa, S.L. ha establecido una política de almacenamiento seguro de los datos personales con la finalidad de garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales almacenados por la organización.

La información de la organización puede ser almacenada en los siguientes sistemas:

- Documentación en soporte papel
- Almacenamiento local
- Servidores de almacenamiento en red
- Sistemas de copias de seguridad
- Dispositivos externos
- Servicios de almacenamiento en la nube

Documentación en soporte papel

Para la documentación en papel deben tomarse las siguientes medidas de seguridad:

- Los documentos deben ser almacenados en lugares cerrados por medio de llave u otros sistemas que obstaculicen su apertura.
- Cuando los documentos se encuentren fuera de la zona de archivo por ser necesaria su utilización, la persona que se encuentre a cargo de los documentos debe velar por que las personas no autorizadas no tengan acceso a los documentos.
- Queda expresamente prohibido mantener los documentos de forma desordenada en el escritorio o lugar de trabajo. Se seguirá una política de mesas limpias.

Almacenamiento local

Para el almacenamiento local de datos personales se ha establecido lo siguiente:

- Uso de contraseñas seguras.
- En los equipos locales únicamente se almacenarán los datos de forma temporal.
- Cifrado de la información en caso de ser necesario.
- Queda prohibido expresamente el almacenamiento de documentos personales, archivos de música o fotografías en el equipo de trabajo.

Servidores de almacenamiento en red

Para el almacenamiento en la red corporativa se tomarán las siguientes medidas:

- Uso de contraseñas seguras o llaves criptográficas.
- Utilización de cortafuegos.
- Utilización de sistemas IDS (Intrusion Detection System).
- Red Privada Virtual (o VPN).
- Encriptación SSL/TLS.

Sistemas de copias de seguridad

Las copias de seguridad se regirán por lo dispuesto en la Política de copias de seguridad de Athento Europa, S.L..

Dispositivos externos

Respecto a los dispositivos externos como pueden ser USBs o CDs, no se permite almacenar en ellos datos personales en los mismos debido a que son especialmente susceptibles a la pérdida de información.

Servicios de almacenamiento en la nube

El servicio de almacenamiento en la nube debe ser elegido en atención a sus medidas de seguridad. En la medida de lo posible, los datos personales se encriptaran o anonimizarán a fin de evitar que la información se desvele a terceros.

Asimismo, se deberá controlar el acceso a la nube mediante usuario y contraseña. Queda prohibido expresamente que los trabajadores den acceso al almacenamiento de la nube a personas ajenas a la organización.

Política de cifrado de la información

El 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 (RGPD) establece que el Responsable o Encargado debe determinar las medidas técnicas y organizativas más apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Por ello, Athento Europa, S.L. ha adoptado una política de cifrado de la información con el objetivo de salvaguardar la confidencialidad, integridad y autenticidad de los datos personales tratados por la organización.

Medidas implementadas

Athento Europa, S.L. ha adoptado las siguientes medidas:

- **Uso de firma electrónica**: Se utilizará la firma electrónica en los intercambios comerciales y en los trámites con las Administraciones Públicas.
- **Certificados web SSL:** La empresa deberá adquirir un certificado web para garantizar la seguridad de la información en un sitio web.
- **Cifrado de datos sensible s cuando se contratan servicios externos:** Se debe comprobar que el servicio externo contratado utiliza canales cifrados para las comunicaciones y herramientas de cifrado en el tratamiento de la información sensible.
- **Cifrado de datos sensibles cuando se solicitan desarrollos de aplicaciones:** Se debe comprobar que se cifran las credenciales de acceso cuando se solicitan desarrollos web o apps que impliquen el login de usuarios.
- **Acceso desde el exterior con VPN**: La empresa deberá habilitar canales VPN cifrados que garanticen la confidencialidad e integridad de las comunicaciones de la política de uso de wifis y conexiones externas cuando tengan trabajadores o autoricen el acceso desde el exterior a los servidores de las instalaciones de la empresa.
- **Algoritmos de cifrado autorizados:** La empresa deberá aplicar y revisar los algoritmos de cifrado para evitar el uso de sistemas de cifrado obsoletos.
- **Aplicaciones autorizadas para usos criptográficos**: Se deberá tener una lista de las aplicaciones autorizadas para fines criptográficos.
- **Uso de protocolos seguros de comunicación:** La empresa deberá proporcionar a los trabajadores los protocolos criptográficos actualizados para el uso de su actividad y formación.

Política de actualización de software y hardware

En cumplimiento de las políticas de seguridad de la información y de protección de datos, Athento Europa, S.L. informa a los trabajadores/as que deberán actualizar los equipos de sistemas de la información con una periodicidad, como mínimo, semestral.

Los sistemas deben estar actualizados a la última versión disponible y las actualizaciones siempre deben ser entregadas por los fabricantes por motivos de seguridad. De este modo, Athento Europa, S.L., asegura a sus trabajadores que sus equipos informáticos no estarán expuestos a riesgos. Más concretamente se han implementado las siguientes medidas:

- Determinar el software qué debe ser actualizado.
- Determinar cuándo y qué actualizaciones se deben instalar.
- Probar las actualizaciones y realizar un registro.
- Configurar un sistema de alertas.
- Recomendable aplicar actualizaciones automáticas.
- En la actualización manual las fuentes dónde se obtiene el software debe ser de confianza.
- Los Servicios contratados a terceros, deben estar actualizados.
- En el momento que el software quede obsoleto y sin soporte oficial por parte del fabricante, dejaremos de utilizarlo.
- Revisar la existencia de actualizaciones y parches de seguridad para nuestro software y realizar procedimientos que admitan que dichas actualizaciones y parches se instalen en los equipos de forma segura.

Política de destrucción y reutilización de equipos y soportes

En cumplimiento de las políticas de seguridad de la información y de protección de datos, Athento Europa, S.L. informa a los trabajadores/as como deberán destruir tanto los documentos físicos y soportes digitales, así como la reutilización de los equipos de sistemas de la información.

Asimismo, la empresa informa a sus trabajadores en cuanto a la destrucción de datos las siguientes medidas:

- La destrucción de información propiedad de la empresa debe realizarse de un modo que haga imposible la recuperación de la misma en los ordenadores, portátiles, memoria externa, etc.
- La destrucción física de soportes digitales como el formateo del mismo se realizará por el departamento o personal autorizado de la empresa.
- Para la destrucción de información confidencial en papel se debe realizar siguiendo los procedimientos vigentes (aquéllos que implementa la empresa) y siempre de modo seguro.

Uso de la Destructora de Papel.

Athento Europa, S.L. señala que ha implementado los medios necesarios para la eliminación de los datos que se encuentren en soporte de papel y en soporte digital, bien a través de destructoras de papel o empresas homologadas de destrucción. Asimismo la forma y los plazos de eliminación de los soportes dependerá del tipo de datos y de las normas internas de la empresa.

En cuanto a la reutilización de equipos y soportes propiedad de la Empresa, se implementan las siguientes medidas:

- Formatear los equipos con el fin de restablecer los discos duros, una memoria USB o cualquier dispositivo que instale datos, a su estado original, borrando, de forma definitiva, los datos que este contiene.