POLÍTICA DE SEGURIDAD

CENTRO ASOCIADO DE LA UNED EN MADRID

Este documento debe ser entregado a todas las personas que tratan datos personales en la entidad. Las sucesivas versiones deben ser notificadas a dichas personas a través de correo electrónico con acuse de recibo.

Los usuarios deben verificar periódicamente que disponen de la versión más actualizada del documento, según la numeración que consta al pie del mismo.

CONTROL DE VERSIONES		
EDICION	**FECHA**	**DESCRIPCIÓN**
Quinta	Enero 2022	Se actualizan los registros de actividades del Tratamiento (RAT´s) Se actualiza la relación de encargados del tratamiento. En el procedimiento de gestion de brechas de seguridad, se recogen recomendaciones de la última guía publicada al efecto por la AEPD. Se modifican/suprimen determinados apartados

PICÓN & ASOCIADOS
ABOGADOS

Política de Seguridad:

PARTE GENERAL

Esta Parte General de la Política de Seguridad debe ser entregada a todas las personas que tratan datos personales en la entidad, así como al personal de empresas externas que tengan acceso a datos y presten sus servicios presencialmente en las instalaciones de la Entidad o mediante conexión remota.

No obstante, el Capítulo 7 sólo deberá entregarse a aquellos empleados que traten datos personales en régimen de movilidad o teletrabajo.

Capítulo 1.- Conceptos básicos

1.1. Objeto

La presente Política de Seguridad describe las medidas que deben aplicarse en CENTRO ASOCIADO DE LA UNED EN MADRID (en adelante, la Entidad) para evitar la alteración o pérdida de los datos personales o su tratamiento o acceso no autorizados.

El cumplimiento de esta Política de Seguridad es obligatorio para todas las personas que tratan datos personales en la Entidad, así como para el personal de empresas externas que tengan acceso a datos y presten sus servicios presencialmente en las instalaciones de la Entidad o mediante conexión remota.

Las medidas de seguridad definidas en este documento son resultado del Análisis de Riesgos efectuado al efecto.

1.2. Definición de datos personales

Dato personal es cualquier información concerniente a personas físicas, identificadas o identificables. Por tanto, no son datos personales los datos de personas jurídicas (sociedades mercantiles, instituciones, etc.).

1.3. Relación del Personal

Responsable del Tratamiento de los Datos:

Es quien decide sobre los fines y los medios del tratamiento de los datos. A efectos de esta Política, es Responsable del Tratamiento:

Identificación		NIF
CENTRO ASOCIADO DE LA UNED DE MADRID		Q-2802102-J
Domicilio	C/ Tribulete 14 28012-Madrid (España)	

Asimismo, existen las siguientes sedes CAMA:

- Madrid Capital

  Gregorio Marañón

  Jacinto Verdaguer

  Las Tablas

- Madrid Periferia

  Las Rozas

  Arganda del Rey

  Rivas Vaciamadrid

  San Martín de Valdeiglesias

  San Sebastián de los Reyes

  Coslada

  Torrejón de Ardoz

  Collado Villaba

  Pozuelo de Alarcón

Contacto de Seguridad:

Es la persona que, dentro de la entidad, tiene la función de coordinar y controlar la aplicación y efectividad de las medidas técnicas y organizativas establecidas para el cumplimiento de la normativa sobre protección de datos personales. El Contacto de Seguridad es:

Identificación del Contacto de Seguridad
D. Antonio Crespo León
E-mail del Contacto de Seguridad
subdirector.cyt@madrid.uned.es

Usuarios:

Personas autorizadas para acceder a datos personales de la Entidad o responsabilidad de sus clientes.

La relación de usuarios y los permisos de acceso concedidos a cada uno de ellos figuran en el Directorio Activo de Windows, pudiendo extraerse de este el listado.

Delegado de Protección de Datos (DPD):

Es la persona que tiene la función de supervisar el cumplimiento de la normativa sobre protección de datos personales y actuar como punto de contacto entre la Entidad y los interesados y entre aquella y la autoridad de control (Agencia Española de Protección de Datos).

Todos los usuarios deben contactar con el DPD para atender los asuntos que surjan en relación con la privacidad, así como consultarle antes de realizar cualquier nuevo tratamiento de datos personales o desarrollar productos o servicios nuevos que impliquen dicho tratamiento.

Se incluyen a continuación los datos del Delegado de Protección de Datos de la Entidad:

Identificación del Delegado de Protección de Datos
Picón y Asociados Derecho y Nuevas Tecnologías, S.L.
E-mail de contacto del Delegado de Protección de Datos
dpd@piconyasociados.es

1.4. Tratamientos de datos a los que se aplica la Política de Seguridad

La presente Política de Seguridad se aplica a los tratamientos de datos personales que se realizan en la Entidad, ya informáticamente, ya en papel.

Las medidas de seguridad deben también cumplirse con respecto a los ficheros temporales o copias de documentos creados exclusivamente para realizar trabajos temporales. Los ficheros o documentos temporales han de ser destruidos por el usuario cuando hayan dejado de ser necesarios para los fines que motivaron su creación.

La Entidad realiza, como responsable, los tratamientos de datos personales que constan en el Registro de Actividades del Tratamiento que figura en el **ANEXO** a la **Política de Protección de Datos Personales**.

Adicionalmente, la Entidad, realiza, como encargada del tratamiento de sus clientes (Uned Central), los tratamientos de datos personales que constan en dicho **ANEXO**.

1.5. Descripción del software utilizado en el tratamiento de datos

Se utilizan los siguientes programas:

- **Genéricas de UNED Central**:
  - "Akademos" (aplicación informática de gestión de los datos académicos de estudiantes y de los profesores tutores).
  - "Alma"" (aplicación informática de datos de estudiantes para control de préstamos de libros en bibliotecas).
  - "Valija Virtual" (aplicación informática de gestión de exámenes de alumnos).
  - "Quid" (aplicación informática de desarrollo de actividades relacionadas con el COIE).
  - Webex (aplicación informática destinada a la llevanza de los diversos trámites relativos a la extensión universitaria, los cursos de verano y UNED Senior).
- **Propias del CAMA**:
  - "Biblex": (aplicación de gestión de los usuarios externos de bibliotecas).
  - "Apliman" (aplicación informática en desarrollo - Contabilidad y datos de filiación de Tutores y PAS).
  - "Verisure" (aplicación informática destinada a la gestión y al tratamiento de las imágenes captadas por el sistema de videovigilancia.

- “Microsoft OFFICE 365”: Paquetes de aplicaciones ofimáticas, integrados por procesador de textos (Word), hoja de cálculo (Excel), base de datos (Access) y PowerPoint (Presentaciones) y entorno Cloud.

1.6. Nuevas actividades de tratamiento de datos

Los usuarios deben **consultar previamente al DPD** cuando, en el desempeño de sus funciones, necesiten realizar las siguientes actividades:

- Tratar datos personales distintos de los que figuran en el Registro de Actividades del Tratamiento de la entidad o para finalidades diferentes de las indicadas en él.

- Tratar datos personales en el disco duro del propio ordenador personal del usuario, en un disco duro de un ordenador distinto de los destinados a ello, en otro dispositivo electrónico o mediante computación en nube.

- Instalar una nueva aplicación informática que utilice datos personales o desinstalar o alterar una ya existente.

Capítulo 2.- Controles de Acceso a la Información y Confidencialidad

2.1. Objeto

Este Apartado describe los controles existentes para que cada usuario acceda únicamente a los datos y recursos que necesite para el desempeño de sus funciones.

2.2. Reglas generales

Se debe evitar el acceso de personas no autorizadas a los datos personales.

A tal fin, se evitará dejar los datos expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), incluyendo las pantallas que se utilicen para la visualización de imágenes captadas por las cámaras.

No se comunicarán datos personales a terceros, prestando especial atención en no divulgar datos personales durante las conversaciones telefónicas, en correos electrónicos, etc.

Los deberes de confidencialidad y secreto subsisten aún después de finalizada la relación entre el usuario y la empresa.

2.3. Contraseñas

El mecanismo de identificación y autenticación utilizado en el tratamiento automatizado de los datos personales es el de usuario y contraseña.

La generación inicial de una contraseña la hará el Contacto de Seguridad, quien la comunicará confidencialmente a cada usuario. El cambio de contraseñas será realizado por el propio usuario, cada vez que el sistema lo exija.

Las contraseñas tendrán un mínimo de 10 caracteres y estarán integradas por números, letras (mayúsculas y minúsculas) y símbolos.

Cada identificador y contraseña debe ser tratado por los usuarios como información **confidencial, personal e intransferible** y no podrán ser revelados a terceros, ni siquiera a compañeros de trabajo.

Si un usuario necesita acceder a datos o correos electrónicos a los que no tenga acceso, debe comunicarlo al Contacto de Seguridad, quien, si lo considera justificado, podrá facilitarle el acceso. En ningún caso dos usuarios podrán compartir sus contraseñas para acceder de manera conjunta a los datos personales.

En caso de que la confidencialidad de una contraseña pudiera verse comprometida, se deberá poner inmediatamente en conocimiento del Contacto de Seguridad.

No está permitido apuntar los identificadores y contraseñas, ni en papel, ni en soporte electrónico.

Cuando un usuario se ausente del puesto de trabajo, procederá al bloqueo de la pantalla o al cierre de la sesión.

No está permitido utilizar los ordenadores del trabajo para fines personales. En caso de que, excepcionalmente, sea necesario, se deberá disponer de perfiles de usuario distintos para cada una de las finalidades.

2.4. Accesos en remoto

En caso de que existan accesos al sistema de tratamiento de datos a través de redes de comunicaciones electrónicas o en remoto, se deberán aplicar en ellos las mismas medidas de seguridad que en los accesos locales.

2.5. Controles de acceso a la información en papel

A los documentos en papel que contengan datos personales únicamente podrán acceder los usuarios que lo necesiten para desempeñar sus funciones, de conformidad con los permisos que cada uno tenga autorizados. El resto de usuarios tienen prohibido el acceso a estos documentos.

Si un usuario necesita tratar documentos con datos personales, pero no tiene permiso para ello, debe solicitar la autorización previa del Contacto de Seguridad.

2.6. Control de acceso físico

Las medidas de seguridad físicas juegan un papel tan importante como las medidas técnicas, en tanto que protegen los sistemas de un acceso físico no autorizado.

En este sentido, la empresa valorará la conveniencia de establecer sistemas de identificación del personal, definición de áreas de acceso restringido, sistemas de detección de intrusos o la instalación de barreras perimetrales, debiendo los usuarios respetar dichas medidas, en su caso.

Sólo el personal de informática podrá acceder a los lugares donde se encuentren ubicados los equipos físicos que dan soporte al sistema informático con el que se tratan dichos datos. El acceso a dicho lugar se encuentra limitado mediante llave, huella dactilar o mecanismo equivalente. El acceso a dichos locales por personas distintas debe efectuarse siempre bajo el control del Contacto de Seguridad.

Capítulo 3: Gestión de soportes informáticos y documentos

3.1. Objeto

Este Apartado describe las condiciones en las que pueden utilizarse soportes informáticos portátiles – CDs, memorias portátiles, discos duros externos, ordenadores portátiles, etc. – y documentos en papel que contengan datos personales.

3.2. Medidas aplicables a todos los soportes y documentos

Las medidas de seguridad contenidas en este apartado deben aplicarse tanto a soportes informáticos como a documentos en papel, siempre que contengan datos personales.

3.2.1. Almacenamiento de soportes y documentos

Mientras no se esté trabajando con ellos, los usuarios deben guardar los soportes y documentos con datos personales en estancias, armarios, cajones u otros dispositivos que dispongan de cerradura con llave o mecanismo equivalente, de modo que sólo él o, en su caso, el resto de personas autorizadas, puedan acceder a ellos.

3.2.2. Borrado de datos. Desechado de documentos y soportes

El fin último en la destrucción o retirada de los dispositivos y soportes que contienen datos personales debe ser un borrado irreversible de los datos, para que no puedan ser recuperados.

Quien vaya a desechar documentos o soportes que contengan datos personales, debe, previamente, destruirlos o borrarlos, cumpliendo las siguientes premisas:

1. El usuario guardará reservadamente el documento o soporte hasta que lleve a cabo el borrado o destrucción.

2. La destrucción o borrado deben tener como resultado necesario la imposibilidad de acceder o reconstruir, siquiera parcialmente, la información.

3. Siempre que se cumpla el objetivo anterior, la destrucción se podrá hacer por medios manuales o, en su caso, por los medios mecánicos que la Entidad ponga a disposición de los usuarios.

4. Queda terminantemente prohibido depositar soportes o documentos no destruidos o borrados en la vía pública o lugares accesibles a personas no autorizadas.

Se recomienda seguir los siguientes procedimientos de destrucción o borrado, conforme a los estándares internacionales generalmente reconocidos:

SOPORTE	PROCEDIMIENTO	
Papel o microfilm	Destruir	Trituradora en tiras o cuadrados de 2mm
Móviles y PDAs	Borrar manualmente	Agenda, mensajes, llamadas y resetear a la configuración de fábrica
Routers	Borrar manualmente	Tablas de encaminamiento, registros de actividad, cuentas de administración y resetear a la configuración de fábrica
Impresoras y faxes	Borrar manualmente	Resetear a la configuración de fábrica
Discos reescribibles	Formatear	Formateo de bajo nivel
Discos de solo lectura	Destruir	Trituradora: 5mm
Discos virtuales cifrados	Además de lo anterior	Destruir las claves

El usuario que tenga conocimiento de la existencia de soportes o documentos que, debiendo ser destruidos o borrados, no lo hayan sido, lo comunicará de inmediato al Contacto de Seguridad, para que adopte las medidas oportunas para la destrucción.

3.3. Medidas especiales aplicables a documentos en papel

Además de las medidas previstas en el Apartado 3.2 anterior, cuando se traten documentos en papel que contengan datos personales, deben cumplirse las siguientes:

3.3.1. Documentos en tramitación o revisión

Durante el tiempo en que, por estar en revisión o tramitación, anterior o posterior a su archivo, los documentos con datos personales no se encuentren almacenados en las condiciones previstas en el Apartado 3.2.1, la persona que esté a su cargo los mantendrá permanentemente en su poder y bajo su vigilancia y control, impidiendo a terceros no autorizados acceder a ellos. El resto del tiempo, los documentos permanecerán guardados en los lugares mencionados en el apartado 3.2.1

Siempre que un usuario haya de imprimir documentos que incluyan datos personales, debe tener en cuenta las siguientes medidas:

- Supervisará el proceso, con el fin de impedir que personas no autorizadas puedan visualizar los datos mientras se realiza la impresión.
- Retirará los documentos de la impresora en cuanto sea posible y los guardará en un lugar seguro.

3.3.2. Ubicación de archivadores con datos de riesgo elevado

Los archivadores en los que se almacenen los documentos con datos cuyo tratamiento implique un riesgo elevado (conforme a lo previsto en el Registro de Actividades de Tratamiento) deben ubicarse en un área que disponga de puerta con llave propia o sistema equivalente. Dicha área debe permanecer cerrada mientras no sea necesario acceder a los documentos.

3.3.3. Copias o reproducciones de documentos con datos de riesgo elevado

Las copias o reproducciones de los documentos con datos cuyo tratamiento implique un riesgo elevado (conforme a lo previsto en el Registro de Actividades de Tratamiento) deben realizarse siempre con autorización del Contacto de Seguridad.

Cuando este tipo de documentos se trasladen, deben adoptarse las medidas necesarias para impedir el acceso indebido o la manipulación de la información.

En todo caso, si un usuario tuviera conocimiento de la existencia de documentos en papel con datos personales con respecto a los que no se cumplan las medidas de seguridad previstas en este Apartado 3.3 lo comunicará de inmediato al Contacto de Seguridad, para que adopte las medidas oportunas.

3.4. Medidas especiales aplicables a soportes informáticos

3.4.1. Usos permitidos de soportes informáticos

Como regla general, no está permitida a los usuarios la grabación de datos personales en soportes físicos o informáticos portátiles – CDs, memorias portátiles, discos duros externos, ordenadores portátiles, etc. –. Únicamente podrán tratar dichos datos en soporte papel y sólo si ello es necesario para el desempeño de sus funciones.

Excepcionalmente, se permite la grabación o utilización de datos personales en soportes informáticos portátiles cuando el usuario, necesitándolo para desempeñar sus funciones, solicite y obtenga una autorización del Contacto de Seguridad.

Adicionalmente, se podrán grabar datos personales en soportes informáticos portátiles en los siguientes supuestos:

a) Para la realización de copias de seguridad, por las personas encargadas de hacerlo.
b) Los usuarios que hayan sido autorizados para utilizar ordenadores portátiles, agendas electrónicas, tablets o dispositivos análogos.

3.4.2. Cifrado de los datos

La salida de soportes – CDs, memorias portátiles, discos duros externos, ordenadores portátiles, etc. – que contengan datos cuyo tratamiento implique un riesgo elevado (conforme a lo previsto en el Registro de Actividades de Tratamiento) se realizará cifrando dichos datos o utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada.

El tratamiento de datos cuyo tratamiento implique un riesgo elevado mediante soportes portátiles fuera de las instalaciones de la Entidad debe hacerse también cifrando los datos.

No se podrán enviar datos cuyo tratamiento implique un riesgo elevado por medios telemáticos (e-mail, Internet, etc.) sin autorización expresa del Contacto de Seguridad. Además, antes de efectuar cualquier comunicación de dichos datos mediante redes de telecomunicaciones, también deberá cifrarse la información.

En todo caso, se valorará la posibilidad de proceder al cifrado de datos personales con carácter previo a que salgan de las instalaciones de la entidad en soporte informático, aun cuando, por la naturaleza de los datos personales enviados y resto de circunstancias concurrentes, no exista un riesgo elevado.

Capítulo 4: Gestión de brechas de seguridad

4.1. Objeto

Este apartado describe la forma de actuar en caso de que se produzca una brecha de la seguridad que afecte o pueda afectar a los datos personales.

Una brecha de seguridad es todo quebranto de la seguridad que ocasione o pueda ocasionar la destrucción, pérdida o alteración accidental o ilícita de datos personales tratados o la comunicación o acceso no autorizados a dichos datos. Por ejemplo, si se produjese una incidencia informática (virus, hacker, etc.) que pusiese en peligro la confidencialidad, integridad o disponibilidad de los datos personales.

4.2. Desarrollo

Todos los usuarios tienen la obligación de comunicar al Contacto de Seguridad, lo antes posible, cualquier anomalía o evento que observen y que en su ejecución o desarrollo pueda afectar a la

seguridad de la información tratada por la entidad, cualquiera que sea el soporte en que se encuentre, informático o en papel.

A tal fin, cuando un usuario detecte una brecha de seguridad (potencial o consumada), debe comunicarlo de modo inmediato al Contacto de Seguridad, con toda la información que conozca hasta ese momento.

Salvo que, excepcionalmente, las circunstancias lo impidan, la comunicación al Contacto de Seguridad se efectuará al correo electrónico subdirector.cyt@madrid.uned.es , incluyendo, al menos, la siguiente información:

- Nombre, apellidos y puesto de la persona que efectúa la notificación.
- En qué ha consistido la posible brecha de seguridad.
- Fecha y hora en la que fue detectada.
- Cuáles han sido sus efectos, potenciales o consumados.
- Toda la información complementaria que se considere de interés.

El e-mail se remitirá con acuse de recibo, que deberá ser confirmado por el destinatario y conservado por el remitente como prueba del envío.

Capítulo 5: Protección de las comunicaciones

5.1. Uso del correo electrónico

El uso del correo electrónico queda limitado, estrictamente, al cumplimiento de las tareas laborales o profesionales que el usuario tenga asignadas, no pudiendo utilizarse para fines privados.

Se utilizará el correo electrónico corporativo, evitando, salvo que resulte imprescindible, el uso de otras cuentas de correo distintas.

5.2. Confidencialidad de los destinatarios del correo electrónico

Cuando se envíe un e-mail a varios destinatarios simultáneamente, para evitar que las direcciones de correo electrónico de cada uno de ellos sean visibles para los demás, dichas direcciones se incluirán siempre en el campo “CCO” (con copia oculta) del programa gestor de correo y nunca en el campo “Para”, ni en el campo “CC” (con copia).

5.3. Limpieza de los documentos

Cuando un documento electrónico deba ser enviado fuera de las instalaciones de la empresa, previamente, se debe retirar de él toda la información contenida en campos ocultos, meta-datos, comentarios, revisiones anteriores, etc. salvo cuando dicha información sea pertinente para el receptor del documento. En los siguientes links se explica cómo eliminar esta información:

- Documentos Office: https://support.office.com/es-es/article/quitar-datos-ocultos-e-informaci%C3%B3n-personal-mediante-la-inspecci%C3%B3n-de-documentos-presentaciones-o-libros-356b7b5d-77af-44fe-a07f-9aa4d085966f

- Documentos Adobe: https://helpx.adobe.com/es/acrobat/using/pdf-properties-metadata.html#edit_document_metadata

Esta medida es especialmente relevante cuando el documento vaya a difundirse ampliamente o entre varias personas.

5.4. Cifrado de datos

Cuando se envíen datos personales a través de redes de telecomunicaciones (por ejemplo, a través del correo electrónico), el usuario deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información. En caso de que valore que es conveniente cifrar los datos, procederá al cifrado por sí mismo o con la asistencia del Contacto de Seguridad.

El servidor en el que se aloja la página web debe tener instalado un certificado SSL (Secure Sockets Layer). Ello asegura que la comunicación de datos personales a través de la web se hace de forma fiable, garantizando a los usuarios la identidad del sitio web y cifrando la información transmitida.

En todo caso, será obligatorio el previo cifrado de los datos cuyo tratamiento implique un riesgo elevado (conforme a lo previsto en el Registro de Actividades de Tratamiento).

Capítulo 6. Protección frente a código dañino y phishing

Se considera **código dañino** los virus, los gusanos, los troyanos, los programas espías, «spyware» y, en general, todo lo conocido como «**malware**».

El **phishing** es una técnica engañosa utilizada por los delincuentes para obtener información confidencial, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, haciéndose pasar por una comunicación confiable y legítima.

Para prevenir estos ataques, antes de abrir correos electrónicos, ejecutar archivos informáticos o pulsar hipervínculos, los usuarios se asegurarán de los siguientes extremos:

- Que dichas acciones estén relacionadas con el ejercicio de sus funciones laborales.
- Que se identifique correctamente al remitente.

Los usuarios deben estar atentos a cualquier indicio de que en el sistema informático haya podido instalarse código dañino. Ante dicha sospecha, el usuario, como primera medida de prevención, desconectará el equipo de la red y lo apagará, comunicando inmediatamente la situación al Contacto de Seguridad para que se adopten las actuaciones oportunas.

Capítulo 7: Tratamiento de datos personales en régimen de movilidad o teletrabajo

Los Usuarios que traten datos personales fuera de la oficina, en situación de movilidad o teletrabajo,[1] además de observar las medidas generales descritas en esta Política de Seguridad, deberán cumplir las siguientes:

a) Protección de los dispositivos y del acceso a ellos:

- Se deben utilizar contraseñas de acceso diferentes a las utilizadas para acceder a cuentas de correo personal, redes sociales y otro tipo de aplicaciones utilizadas por el Usuario en su vida personal.
- No se deben descargar ni instalar aplicaciones que no hayan sido previamente autorizadas por la Entidad.
- Se debe evitar la conexión de los dispositivos a la red corporativa desde lugares públicos, así como la conexión a redes WI-FI abiertas no seguras.
- Si se dispone de un equipo corporativo, no se debe utilizar con fines particulares evitando el acceso a redes sociales, correo electrónico personal, páginas web con reclamos y publicidad impactante, así como otros sitios susceptibles de contener virus o favorecer la ejecución de código dañino.
- Si el equipo utilizado es personal, debe evitarse simultanear la actividad personal con la profesional y definir perfiles independientes para desarrollar cada tipo de tarea.
- El antivirus instalado en el equipo debe estar operativo y actualizado.
- Siempre ha de verificarse la legitimidad de los correos electrónicos recibidos, comprobando que el dominio electrónico del que procede es válido y conocido, y desconfiando de la descarga de ficheros adjuntos con extensiones inusuales o el establecimiento de conexiones a través de enlaces incluidos en el cuerpo del correo que presenten cualquier patrón fuera de lo normal.
- Si pueden ser gestionadas por el Usuario, conviene desactivar las conexiones WI-FI, bluetooth y similares que no estén siendo utilizadas.
- Una vez concluida la jornada de trabajo, debe desconectarse la sesión de acceso remoto y apagar o bloquear el acceso al dispositivo.

b) Protección de la información

[1] Algunos de los riesgos derivados de dicha situación son la pérdida o deterioro de los datos por catástrofes físicas (incendio, inundación, derrumbe del edificio, etc.), robo o extravío del dispositivo, limitaciones en la posibilidad de acceder a los datos por la caída de Internet, la falta de sincronización con la plataforma matriz en la que se alojan los datos, los daños en el dispositivo de acceso por la intervención de otras personas que residan con el Usuario o por descuidos (como la caída de bebidas o alimentos), el robo de credenciales o el conocimiento indebido de ellas por terceros, el empleo del dispositivo por personas no autorizadas, el uso de conexiones a internet no seguras (redes wi-fi públicas), la visualización de los datos por personas no autorizadas (otras personas que convivan con el Usuario o terceros, en estaciones de tren o aeropuertos), hacking/cracking o instalación de aplicaciones maliciosas por falta de actualización del sistema operativo o de las aplicaciones, por no instalación o actualización de antivirus o por ausencia de firewall, conexión mediante equipos no autorizados por la compañía, etc. Todos estos riesgos pueden materializarse en incidencias que afecten a la confidencialidad, integridad o disponibilidad de los datos personales, por lo que deben ser prevenidos.

- Tanto en lugares públicos como en el entorno doméstico, deben adoptarse las precauciones necesarias para garantizar la confidencialidad de los datos personales.
- Si se genera y trabaja con papel durante situaciones de movilidad, es importante minimizar o evitar la entrada y salida de documentación y extremar las precauciones para evitar accesos no autorizados por parte de terceros.
- La información en soporte papel, incluyendo borradores, no se puede desechar sin garantizar que es adecuadamente destruida. No arrojar papeles con datos personales, enteros o en trozos, en papeleras de hoteles, lugares públicos o en la basura doméstica.
- Hay que extremar las precauciones para evitar el acceso no autorizado a los datos personales, no dejando a la vista ningún soporte que los contenga en el lugar donde se desarrolle el teletrabajo y bloqueando las sesiones de los dispositivos cuando estos estén desatendidos.
- Se debe evitar exponer la pantalla a la mirada de terceros. Si se trabaja habitualmente desde lugares públicos, es recomendable utilizar un filtro de privacidad para la pantalla.
- En la medida de lo posible, se debe prevenir que se puedan escuchar conversaciones por parte de terceros, utilizando, por ejemplo, auriculares o retirándose a un espacio en el que el Usuario no esté acompañado.

c) Almacenamiento de la información

- Se evitará almacenar los datos personales de forma local en el dispositivo utilizado, salvo situaciones excepcionales. Se deben utilizar los recursos de almacenamiento compartidos o en la nube proporcionados por la Entidad, que son los siguientes: One Drive.
- No se debe bloquear o deshabilitar la política de copia de seguridad corporativa definida para cada dispositivo.
- Es recomendable revisar y eliminar periódicamente la información residual que pueda quedar almacenada en el dispositivo, como archivos temporales del navegador o descargas de documentos.

Se informa a los Usuarios de que se encuentra instalado un sistema de monitorización de la actividad para identificar patrones anormales de comportamiento en el tráfico de red, con el objetivo de evitar la propagación de malware por la red corporativa y el acceso y uso no autorizado de recursos. Asimismo, dicho sistema es utilizado por la Entidad para supervisar el correcto desempeño por el Usuario de sus tareas y obligaciones, en el marco de las funciones de control previstas en el Estatuto de los Trabajadores, que se ejercerán dentro de las condiciones legales y con los límites inherentes a ellas.

Política de Seguridad:

PARTE ESPECIAL

Esta Parte Especial debe ser entregada únicamente al **Contacto de Seguridad y personal de informática**, pero, como regla general, no al resto de usuarios de la entidad.

Sin embargo, excepcionalmente, también deben entregarse los siguientes Capítulos:

- Capítulo 2. Controles de acceso a la información (Parte Especial): Debe entregarse a los usuarios con acceso a los ordenadores, cuando sean ellos mismos quienes elijan y cambien las contraseñas.

- Capítulo 5. Copias de Seguridad: Debe entregarse a los usuarios encargados de hacer las copias de seguridad, cuando aquellos no coincidan con el Contacto de Seguridad o personal de informática.

También debe entregarse al Contacto de Seguridad el Anexo de este Documento, en el que consta en procedimiento que debe seguirse en caso de que se produzcan brechas de seguridad que pudieran afectar a los datos personales.

Capítulo 1: Sistema de tratamiento

1.1. Objeto

Este Apartado describe el sistema mediante el cual se llevan a cabo los tratamientos de datos.

El software utilizado se describe en el apartado 1.5 de la "Parte General".

1.2. Nuevos tratamientos y modificaciones en el sistema

El Contacto de Seguridad consultará previamente a **Picón & Asociados Abogados** cuando los usuarios deseen llevar a cabo tratamientos de datos personales distintos de los del **ANEXO** de la **Política de Protección de Datos Personales** o utilizar plataformas de tratamiento de datos mediante computación en la nube.

El personal de informática, incluidas las compañías subcontratadas de servicios informáticos, deben informar al Contacto de Seguridad de los cambios que realicen en el sistema informático.

En todos los casos mencionados**, Picón & Asociados Abogados** informará sobre la legalidad de los nuevos tratamientos o sistemas de tratamiento de datos y asesorará sobre las medidas a adoptar.

La adecuada gestión de los medios del tratamiento, ya sean activos de hardware, software o recursos de red, es clave para garantizar la seguridad de los datos personales, al igual que todo cambio producido en estos y que debe estar perfectamente sincronizado, controlado y supervisado, para que, de modo accidental, no derive en una revelación, modificación o pérdida no autorizada de los datos personales tratados.

1.3. Pruebas con datos reales

Las pruebas anteriores a la implantación o modificación de los sistemas de tratamiento no se realizarán con datos reales, salvo que se asegure la aplicación de todas las medidas de seguridad correspondientes al tipo de datos tratados.

Capítulo 2: Controles de Acceso a la información (Parte especial)

2.1. Objeto

Este Apartado describe los controles existentes para que cada usuario acceda, únicamente, a los datos y recursos que necesite para el desempeño de sus funciones.

2.2. Controles de acceso a la información automatizada

Cada usuario dispone de un nombre de usuario y una contraseña que le identifican de forma inequívoca y personalizada en el acceso al sistema y verifican que se encuentra autorizado. Este sistema de identificación y autenticación se encuentra:

- En las aplicaciones informáticas.
- En el acceso al dominio.

Cada usuario tiene asignado un perfil o protocolo de acceso a datos, de forma tal que únicamente puede acceder a aquellos que necesita para ejercer sus funciones.

Se habilitarán perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a datos personales.

2.3. Generación y distribución de contraseñas

La generación de contraseñas la realiza UNED CENTRAL.

Las contraseñas tendrán, al menos, 10 caracteres, incluyendo números, letras (mayúsculas y minúsculas) y símbolos.

La distribución de contraseñas la realiza UNED CENTRAL, quien las comunica verbalmente y de modo confidencial a cada usuario.

Los sistemas que realicen la identificación del usuario garantizarán que la introducción de la contraseña y su representación en pantalla, en el momento de la autenticación, se efectúan en un formato no legible para el resto de los usuarios.

2.4. Almacenamiento de las contraseñas

Las contraseñas se almacenan en formato ininteligible en el sistema informático donde se realiza la autenticación de usuarios, en cada caso. Sólo el Contacto de Seguridad podrá conocer y almacenar las contraseñas de los demás usuarios.

En caso de que dicho almacenamiento se produzca en soporte papel, el documento que las contenga deberá guardarse en un lugar sólo accesible al Contacto de Seguridad. En caso de que el almacenamiento se efectúe en archivo informático, dicho archivo deberá guardarse, a su vez, bajo contraseña sólo conocida por el Contacto de Seguridad.

2.5. Renovación periódica de contraseñas

Las contraseñas son renovadas por el propio usuario, al menos una vez al año y, además, toda vez que se sospeche que su confidencialidad ha sido comprometida.

2.6. Otros controles de acceso

Cuando el personal de la Entidad tenga que realizar trabajos que no impliquen acceso a datos personales, el Contacto de Seguridad debe adoptar las medidas adecuadas para limitar el acceso a dichos datos, a los soportes que los contengan o a los recursos del sistema de información.

2.7. Limitación de intentos reiterados de acceso al sistema

El sistema de usuario y contraseñas debe bloquearse cada vez que alguien intente reiteradamente el acceso no autorizado al sistema de información.

Se considera que existe un intento reiterado de acceso no autorizado cuando alguien introduzca 3 ó más veces un nombre de usuario o contraseña erróneos o falsos para acceder al sistema.

2.8. Monitorización y registro de accesos

Si es posible, se activará un registro de logs en los sistemas de información, para permitir la identificación y seguimiento de las acciones realizadas por los usuarios cuando acceden a los equipos en los que se realiza el tratamiento de datos personales, con el fin de identificar potenciales intentos de acceso no autorizado, tanto internos como externos, y como medida de responsabilidad proactiva en el caso de que se produzca un incidente de seguridad. De cada acceso que se produzca, se guardará, al menos, la identificación del usuario que haya accedido, la fecha y hora en que se realizó el acceso, el registro accedido y el tipo de acceso.

El registro de accesos informáticos será obligatorio en relación con los datos cuyo tratamiento implique un riesgo elevado.

El Contacto de Seguridad supervisará directamente el correcto funcionamiento del registro de accesos, no permitiendo su desactivación o manipulación.

Capítulo 3: Tratamientos de datos por terceras personas o empresas

3.1. Objeto

El objeto de este apartado es la identificación de los tratamientos de datos personales efectuados por terceros encargados del tratamiento y la indicación de las normas que han de cumplirse en estos casos.

3.2. Personal ajeno a la Entidad con acceso a datos

Las personas o entidades que acceden a los datos tratados en los sistemas de la Entidad en la prestación de sus servicios como proveedores externos (encargados del tratamiento) son:

Picón & Asociados Derecho y Nuevas Tecnologías, S.L.	
Descripción de los servicios.	Asesoramiento legal para el cumplimiento de la normativa sobre protección de datos personales.
Datos a que accede.	Cualesquiera, en la medida en que sea necesario para la prestación del servicio.

Compañía de asesores técnicos y económicos, S.A.P	
Descripción de los servicios.	Asesoramiento para el cumplimiento de la normativa laboral.
Datos a que accede.	Empleados (PAS).

D. Juan Carlos Lopez-Amor García	
Descripción de los servicios.	Asesoramiento jurídico general
Datos a que accede.	Cualesquiera, en la medida en que sea necesario para la prestación del servicio.

Securitas Direct, S.A.U.	
Descripción de los servicios.	Videovigilancia.
Datos a que accede.	Imágenes captadas por el sistema instalado.

Dña. Yolanda Dominguez Torreadrado	
Descripción de los servicios.	Comunicación social
Datos a que accede.	Cualesquiera, en la medida en que sea necesario para la prestación del servicio.

Audit, S.L.	
Descripción de los servicios.	Soporte aplicación “Aplined”
Datos a que accede.	Cualesquiera, en la medida en que sea necesario para la prestación del servicio.

Apliman, S.L.	
Descripción de los servicios.	Mantenimiento aplicación “Apliman”
Datos a que accede.	Cualesquiera, en la medida en que sea necesario para la prestación del servicio.

Dña. Teresa Zurita Ramón	
Descripción de los servicios.	Coordinadora COIE.
Datos a que accede.	Cualesquiera, en la medida en que sea necesario para la prestación del servicio.

Medios de prevención externos Centro Levante, S.L.	
Descripción de los servicios.	Servicios PRL.
Datos a que accede.	Empleados (PAS).

Ayuntamiento de Pozuelo de Alarcón	
Descripción de los servicios.	Cesión de instalaciones.
Datos a que accede.	Empleados (PAS).

Ayuntamiento de Pozuelo de Alarcón	
Descripción de los servicios.	Cesión de instalaciones.
Datos a que accede.	Cualesquiera, en la medida en que sea necesario para la prestación del servicio

Ibermática, S.L.	
Descripción de los servicios.	Mantenimiento y soporte técnico informático.
Datos a que accede.	Cualesquiera, en la medida en que sea necesario para la prestación del servicio

Cada encargado del tratamiento tiene las facultades de acceso y tratamiento de datos personales que son estrictamente necesarias para la prestación de los servicios contratados. Las obligaciones que deben cumplir se encuentran recogidas en el contrato de prestación de servicios suscrito con cada uno de ellos en las condiciones exigidas por el artículo 28 RGPD. Se debe velar por que los encargados del tratamiento elegidos reúnan las condiciones necesarias para cumplir el RGPD, tanto en su elección como durante la prestación de sus servicios.

3.3. Personal ajeno a la Entidad sin acceso a datos personales

Cuando personal ajeno a la Entidad tenga que realizar trabajos que no impliquen acceso a datos personales, la Entidad debe solicitar a la empresa para la que trabajen que les exija que no accederán a los datos y, en su caso, que guardarán secreto respecto de los que hubieran podido conocer en la prestación de los servicios.

Capítulo 4: Gestión y notificación de brechas de seguridad (Parte especial)

4.1. Objeto

Este Apartado describe la forma de actuar ante las brechas de seguridad que afecten o puedan afectar a datos personales.

4.2. Desarrollo

Las brechas de seguridad que sean notificadas al Contacto de Seguridad se gestionarán conforme al procedimiento que consta al efecto en el **ANEXO** de este Documento.

Capítulo 5: Copias de Seguridad

5.1. Objeto

Describir la forma en que se deben realizar las copias de seguridad.

5.2. Procedimiento de copias de seguridad

El procedimiento para realizar copias de seguridad es el siguiente:

Las copias se llevan a cabo con la autorización de Contacto de Seguridad.:

Las copias de seguridad están programadas cronológicamente de la siguiente manera:

SERVER56: 23:30 hrs de lunes a domingo
Partición del sistema EFI: Completa
C: Incremental

SERVER57: 22:30 hrs. de lunes a domingo
Partición del sistema EFI: Completa
C: Incremental

SERVER58: Suspendidas por falta de actividad en el servidor.

También hay una copia completa de carácter mensual en cada uno de los servidores.

Todas ellas se encuentran debidamente etiquetadas, siendo identificables en forma clara y precisa.

Las copias antiguas o caducas se sobrescriben.

Una vez efectuadas, las copias se almacenan bajo acceso restringido por llave a los usuarios autorizados.

Por otra parte, el procedimiento para realizar las copias de seguridad de las imágenes captadas por las cámaras es el siguiente:

Las realiza la entidad Securitas Direct, S.A., con la autorización del Contacto de Seguridad.

Se almacenan en los servidores habilitados al efecto de la entidad referida.

Todas ellas se encuentran debidamente etiquetadas, siendo identificables en forma clara y precisa.

Las copias antiguas o caducas se sobrescriben.

Una vez efectuadas, las copias se almacenan bajo acceso restringido por llave a los usuarios autorizados.

En cualquier caso, los datos personales grabados por las cámaras son cancelados en el plazo máximo de un mes desde su captación.

Las copias de seguridad se deben guardar en un lugar diferente de aquél en que se encuentran los equipos informáticos con los ficheros originales, con el fin de permitir la recuperación de los datos en caso de pérdida de la información. Además, aquellas copias que alberguen datos de "riesgo alto", deberán verse sometidas a un proceso de cifrado previo al traslado referido, que garantice la debida confidencialidad, integridad, disponibilidad y resiliencia de la información contenida en las mismas.

Periódicamente, el Contacto de Seguridad verificará el correcto funcionamiento de las copias de seguridad.

Como complemento a lo anterior, es recomendable que la entidad desarrolle un plan de continuidad de negocio, que describa los procedimientos que debe seguir si se produjese un incidente o brecha de seguridad que afectase a los datos personales, con objeto de que se pueda restaurar la disponibilidad y el acceso a ellos de forma rápida.

Capítulo 6: Otras salvaguardas

6.1. Objeto

Describir una serie de medidas técnicas complementarias que permitan la salvaguarda de los datos personales.

6.2. Relación de salvaguardas complementarias

Se exponen a continuación el resto de salvaguardas que la Entidad debe implementar en su sistema informático, para garantizar la seguridad de los datos personales que se traten en él.

6.2.1. Actualización de ordenadores, dispositivos y aplicaciones

Los dispositivos, ordenadores y aplicaciones utilizados para el almacenamiento y tratamiento de los datos personales deberán mantenerse actualizados.

Si es posible, se impedirá que los usuarios puedan instalar nuevas aplicaciones o desinstalar o alterar las existentes.

6.2.2. Antivirus

En los ordenadores y dispositivos en los que se realicen tratamientos de datos personales se instalará un sistema antivirus que garantice, en la medida de lo posible, el robo y destrucción de la información. El antivirus se actualizará periódicamente y, si es posible, a diario. Los usuarios no podrán desactivar el antivirus.

6.2.3. Seguridad de las comunicaciones y cortafuegos

Debe valorarse la necesidad de asegurar las comunicaciones, tanto hacia Internet como en la interconexión con otros sistemas internos o externos, mediante la instalación de sistemas de detección de intrusión y segregación de redes.

Para evitar accesos remotos indebidos a los datos, se instalará un cortafuegos, que permanecerá activado, al menos, en los ordenadores y dispositivos en los que se realice el tratamiento o almacenamiento de datos personales.

6.2.4. Opción de seudonimización o cifrado de los datos

Cuando los datos vayan a salir fuera de las instalaciones en las que habitualmente se realice su tratamiento, se deberá valorar la posibilidad de seudonimizarlos o utilizar previamente un método de encriptación, para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

6.2.5. Borrado automático de los datos

Debe valorarse la implementación de políticas automáticas de borrado de la información para asegurar que los datos no se conservan más allá del tiempo necesario en relación con el propósito para el que fueron recabados.

6.3. Cumplimiento de las salvaguardas complementarias

El Contacto de Seguridad velará por que las salvaguardas complementarias mencionadas en este Capítulo 6 se implanten y se mantengan activas, solicitando, en caso necesario, auxilio de quienes estén encargados del mantenimiento del sistema informático.

Capítulo 7: Revisión/auditoría de las medidas de seguridad

7.1. Objeto

Este Apartado describe la forma y periodicidad con que deben hacerse revisiones o auditorías de las medidas y procedimientos establecidos en la presente Política de Seguridad.

7.2. Revisiones/auditorías puntuales

El Contacto de Seguridad deberá revisar y, en su caso, modificar las medidas de seguridad que figuran en este Documento cada vez que se produzca alguna de las circunstancias siguientes:

a) Cambios en la legislación vigente.
b) Evolución de las actividades de la entidad.
c) Resultados de las revisiones y análisis de riesgos efectuados.
d) Defectos encontrados en la aplicación de procedimientos y medidas existentes.

7.3. Revisiones/auditorías periódicas

El Contacto de Seguridad debe revisar y, en su caso, modificar las medidas de seguridad que figuran en este Documento, al menos, una vez al año y, además, cada vez que se produzcan cambios relevantes en el sistema de información o los recursos protegidos.

Las revisiones/auditorías tienen el objeto de comprobar el cumplimiento de las medidas y procedimientos de seguridad establecidos. Además, se realizará una revisión/auditoría cuando se produzcan modificaciones sustanciales en el sistema de tratamiento de datos que puedan repercutir en el cumplimiento de dichas medidas.

Si así se desea, en el marco de los servicios de un contrato de mantenimiento o puntualmente, **Picón & Asociados Abogados** podrá efectuar las revisiones/auditorías.

Los resultados de la revisión/auditoría se reflejarán en un Informe que se pronunciará sobre la adecuación de las medidas y controles, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias.

El Contacto de Seguridad analizará el Informe de Revisión/Auditoría y lo elevará a la Dirección de la Entidad para la adopción de las medidas correctoras adecuadas.

Capítulo 8: Entrega de la documentación de protección de datos. Formación

8.1. Objeto

Este Apartado describe el modo de entrega de la Política de Seguridad y de la Política de Protección de Datos a los empleados y demás personal al servicio de la entidad.

8.2. Entrega

El Contacto de Seguridad hará entrega a todos los usuarios con acceso a datos de la Política de Protección de Datos, de la Parte General de la Política de Seguridad y de los correspondientes ANEXOS. Asimismo, en su caso, entregará la Parte Especial de la Política de Seguridad a aquellos usuarios que deban conocerla, según lo indicado en la introducción de esta Parte Especial.

Cada usuario debe asumir un compromiso de cumplimiento de la Política de Protección de Datos y de la Política de Seguridad mediante la firma de un documento que le debe ser entregado al efecto por el Contacto de Seguridad o el responsable de recursos humanos de la Entidad.[2]

Cuando se elaboren nuevas versiones o actualizaciones de la Política de Protección de Datos y de la Política de Seguridad, el Contacto de Seguridad notificará su existencia a los usuarios, poniéndolas a su disposición a través de e-mail o de la intranet. En estos casos, los usuarios deberán firmar el correspondiente recibí de la notificación.[3]

8.3. Formación.

Para una efectiva implantación de las medidas técnicas y organizativas, el personal de la organización debe recibir formación periódica y actualizada en relación a los procedimientos de protección de datos personales y seguridad definidos y, en particular, los relativos a las restricciones en la comunicación y divulgación de datos personales, la protección del acceso a estos por parte de terceros no autorizados mediante medidas de almacenamiento seguro, bloqueo de sesiones, cierre de despachos, etc. así como la destrucción segura de documentos y soportes.

Capítulo 9: Medidas aplicables al tratamiento de datos en régimen de teletrabajo

Cuando los Usuarios traten datos personales en situaciones de movilidad o teletrabajo, el Contacto de Seguridad se debe asegurar de que las aplicaciones y soluciones de teletrabajo que implante ofrezcan garantías e impidan la exposición de los datos personales, en particular, a través de los servicios de correo y mensajería. A tal fin, sólo recurrirá a proveedores y encargados que ofrezcan soluciones probadas y garantías suficientes.

[2] El modelo de dicho documento se incluye en la letra c) del Libro Registro de Cláusulas y Contratos.
[3] El modelo de dicho documento se incluye en la letra e) del Libro Registro de Cláusulas y Contratos.

En estas situaciones, se deben adoptar las siguientes medidas de seguridad específicas, recabándose para ello el auxilio del Administrador del Sistema:

- Los perfiles o niveles de acceso a datos tienen que configurarse en función de los roles de cada Usuario de forma especialmente restrictiva y aplicar restricciones de acceso adicionales en función del tipo de dispositivo desde el que se acceda (equipos portátiles corporativos securizados, equipos personales externos y dispositivos móviles como smartphones o tablets) y también dependiendo de la ubicación desde la que se accede.

- Los recursos que pueden ser accedidos en remoto se han de limitar en función de la valoración del riesgo que represente una pérdida del dispositivo cliente y la exposición o acceso no autorizado a la información

- Los servidores de acceso remoto han de ser revisados y hay que asegurar que están correctamente actualizados y configurados para garantizar el cumplimiento del presente Apartado y el control de los perfiles de acceso definidos. Estas revisiones serán realizadas, al menos, cada tres meses.
- · Los equipos corporativos utilizados como clientes tienen que:

    - Estar actualizados a nivel de aplicación y sistema operativo,

    - Tener deshabilitados los servicios que no sean necesarios,

    - Tener una configuración por defecto de mínimos privilegios que no pueda ser desactivada ni modificada por el empleado,

    - Instalar únicamente las aplicaciones autorizadas,

    - Contar con software antivirus actualizado,

    - Disponer de un cortafuegos local activado,

    - Tener activados solo las comunicaciones (wifi, bluetooth, NFC, …) y puertos (USB u otros) necesarios para llevar a cabo las tareas encomendadas.

    - Incorporar mecanismos de cifrado de la información.

- · Si se permite el uso de dispositivos personales de los empleados, deberán contar con un sistema operativo y software original y actualizado, software antivirus actualizado y cortafuegos local activado. Además, en estos casos, debe valorarse la posibilidad de restringir la conexión a una red segregada que únicamente proporcione un acceso limitado a aquellos recursos que se hayan identificado como menos críticos y con menor nivel de riesgo.
- · Hay que establecer sistemas de monitorización para identificar patrones anormales de comportamiento en el tráfico de red, con el objetivo de evitar la propagación de

malware por la red corporativa y el acceso y uso no autorizado de recursos, respetando siempre los derechos digitales establecidos en la LOPDGDD y, en particular, el derecho a la intimidad y uso de dispositivos digitales y el derecho a la desconexión digital en el ámbito laboral.

La configuración definida para acceder a los recursos de forma remota debe ser revisada de forma periódica para garantizar que no ha sido alterada ni desactivada sin autorización, además de permanecer actualizada y adaptada a los cambios que pudieran producirse.

El Responsable de Seguridad debe solicitar al Administrador del Sistema que, periódicamente, revise que se están cumpliendo las medidas de seguridad definidas en este Documento para las situaciones de movilidad o teletrabajo.

ANEXO.- Procedimiento de gestión y notificación de brechas de seguridad

1.- ¿Cuál es el objeto de este documento?

Este documento describe el procedimiento que debe seguirse en la Entidad para detectar, gestionar y, en su caso, notificar las brechas de seguridad que se produzcan en relación con datos personales.

2.- ¿Qué es una brecha de seguridad?

Todo quebrantamiento de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de cualquier otra forma, o la comunicación o acceso no autorizados a dichos datos.

3.- ¿Cómo deben notificar los usuarios las brechas de seguridad que detecten?

Cualquier usuario que detecte una brecha de seguridad (potencial o consumada), la notificará al Contacto de Seguridad del modo establecido en el apartado 4.2 de la Política de Seguridad.

Conforme al criterio de la AEPD, es recomendable impartir a los usuarios formación específica sobre el modo de prevenir, detectar y gestionar brechas de seguridad

4.- ¿Cómo debe actuar el Contacto de Seguridad cuando se comunica una brecha de seguridad?

Cuando el Contacto de Seguridad tenga conocimiento de una posible brecha de seguridad o reciba de un usuario una comunicación de las descritas en el apartado anterior, deberá obtener la información necesaria, con el fin de verificar si la brecha de seguridad afecta a datos personales de personas físicas y las posibles consecuencias derivadas de ello.

A tal fin, obtendrá toda la información que sea posible sobre los siguientes aspectos:

i. Naturaleza y descripción de la brecha de seguridad.

ii. Las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

iii. Posibles consecuencias de la brecha de seguridad de los datos personales.

En caso de que el Contacto de Seguridad compruebe que la brecha de seguridad **NO** ha afectado ni puede afectar a datos personales, cumplimentará el documento que se incluye en la ADDENDA I y conservará el original, debidamente archivado, dando por cerrado el incidente a efectos de protección de datos.

En caso de que el Contacto de Seguridad compruebe que la brecha de seguridad **SÍ** ha afectado o puede afectar a datos personales, valorará si dicha brecha de la seguridad constituye o no un riesgo para los derechos y las libertades de las personas físicas. A tal efecto, antes de tomar una decisión, se recomienda que el Contacto de Seguridad lo consulte con Picón & Asociados Abogados.

a) Si se concluyese que la brecha de la seguridad **NO** constituye un riesgo para los derechos y las libertades de las personas físicas, el Contacto de Seguridad se limitará a cumplimentar y firmar el documento que se incluye en la ADDENDA I, debiendo archivarlo debidamente.

b) Si se concluyese que la brecha de la seguridad de los datos personales **SÍ** constituye un riesgo para los derechos y las libertades de las personas físicas:

    a. Valorará la decisión sobre la notificación del hecho a la Agencia Española de Protección de Datos o, en su caso, al interesado.

    b. Decidirá qué medidas han de adoptarse o proponerse para poner remedio a la brecha de seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

    c. Cumplimentará y firmará el documento que se incluye en la ADDENDA II, debiendo archivarlo debidamente

En caso de que la brecha de seguridad afecte a datos de los que sean responsables clientes de la entidad, se comunicará a estos el hecho por escrito y sin dilación, junto a toda la información de que se disponga, para que adopten la oportuna decisión sobre la comunicación del hecho.

5.- ¿Cómo debe actuar la Entidad una vez disponga de toda la información?

En caso de que se confirme que la brecha de seguridad ha afectado a datos personales, suponiendo un riesgo para los derechos y las libertades de las personas físicas, la Entidad, lo comunicará a la Agencia Española de Protección de Datos (AEPD).[4]

La comunicación la llevará a cabo el Contacto de Seguridad, previa obtención de la oportuna autorización escrita de la Dirección de la Entidad, bastando para ello un correo electrónico de esta que lo confirme y, en su caso, dé las oportunas instrucciones.

[4] Se podrá consultar a Picón & Asociados Abogados en estos casos, bien dentro del servicio de mantenimiento, bien, de no estar contratado, previa la aprobación del correspondiente presupuesto.

La comunicación a la AEPD se hará a través del siguiente link: https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf

Se exceptúa del deber de comunicar el caso de que sea improbable que la brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. En caso de duda sobre si se debe o no efectuar la comunicación a la AEPD, se llevará a cabo dicha comunicación.

La comunicación debe hacerse sin dilación indebida o, a más tardar y, de ser posible, antes de 72 horas después de que haya tenido constancia de la brecha de seguridad. No obstante, si la notificación a la autoridad de control no pudiera efectuarse en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

A la hora de practicar la notificación sin dilación indebida, deberán tenerse en cuenta, en particular, los siguientes factores:

a) La naturaleza y gravedad de la brecha de la seguridad de los datos personales.

b) Sus consecuencias y efectos adversos para el interesado.

c) Las restantes circunstancias de la brecha, inclusive si los datos personales se hallaban protegidos mediante las medidas técnicas adecuadas, limitando eficazmente la probabilidad de usurpación de identidad u otras formas de uso indebido

Si, por cualquier motivo justificado, no fuera posible facilitar toda la información simultáneamente, se facilitará de manera gradual sin dilación indebida.

6.- ¿La notificación de brechas de seguridad a la AEPD puede tener consecuencias para la entidad?

La notificación podría dar lugar a una intervención de la AEPD, de conformidad con las funciones y poderes que le reconoce la ley. No obstante, las consecuencias legales para la entidad siempre serán más graves si, debiendo haberse notificado a la AEPD una brecha de seguridad, no se ha hecho.

7.- ¿Deben notificarse las brechas de seguridad a los afectados?

Como regla general, no deben comunicarse a las personas afectadas.

No obstante, como excepción, la brecha de seguridad se debe comunicar a los interesados, sin dilación indebida, cuando sea probable que la brecha de seguridad de los datos personales entrañe un alto riesgo para sus derechos y libertades. Dicha decisión será adoptada, en su caso, por la Entidad, siendo recomendable que solicite la previa opinión de Picón & Asociados Abogados.

Asimismo, la AEPD, una vez considerada la probabilidad de que la brecha entrañe un alto riesgo, podrá exigirá la Entidad que comunique al interesado la brecha de seguridad de los datos personales, aunque se hubiese decidido lo contrario.

En caso de que se confirme que la brecha de seguridad entraña un alto riesgo para los derechos y libertades de los interesados, el Contacto de Seguridad será responsable de la comunicación a estos, previa obtención de la oportuna autorización escrita de la Dirección de la Entidad,

bastando para ello un correo electrónico de esta que lo confirme y, en su caso, dé las oportunas instrucciones sobre el modo en que la comunicación se debe llevar a cabo.

Para llevar a cabo la comunicación a los afectados, la Entidad utilizará preferentemente los datos de que disponga para ponerse en contacto directo con ellos (p.ej. e-mail o teléfono). A falta de datos de contacto directo, utilizará medios de difusión generales (publicación en su página web y en su perfil de redes sociales, en periódicos, etc.).

8.- ¿Cómo deben notificarse las brechas de seguridad a los afectados, en su caso?

La comunicación al interesado, en su caso se podrá efectuar a través de cualquier medio que permita acreditarla y contendrá en un lenguaje claro y sencillo la siguiente información:

a) La descripción de la naturaleza de la brecha de seguridad de los datos personales.

b) El nombre y los datos de contacto del Contacto de Seguridad o de otro punto de contacto en el que pueda obtenerse más información.

c) Describir las posibles consecuencias de la brecha de seguridad de los datos personales.

d) Describir las medidas adoptadas o propuestas para poner remedio a la brecha de seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. Se deben incluir aquí las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la brecha.

La comunicación a los interesados, en su caso, debe realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la AEPD, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir brechas de la seguridad de los datos personales continuas o similares.

9.- ¿Existen excepciones al deber de notificar las brechas de seguridad a los afectados?

La comunicación al interesado no será necesaria si se cumple alguna de las condiciones siguientes:

a) La Entidad ha adoptado medidas de protección técnicas y organizativas apropiadas, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado, y, además, estas medidas se hayan aplicado a los datos personales afectados por la brecha de seguridad.

b) La Entidad ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se materialice el alto riesgo para los derechos y libertades del interesado.

c) Suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante, por la que se informe de manera igualmente efectiva a los interesados.

ADDENDA I

REGISTRO DE INCIDENTE DE SEGURIDAD SIN AFECTACIÓN A DATOS PERSONALES

Fecha:	Hora:

Persona que notificó el incidente:

Fecha y hora en que se notificó el incidente:

Descripción del incidente:

Información que ha resultado afectada por el incidente (en su caso):

Medidas adoptadas para la subsanación del incidente:

Medidas adoptadas para prevenir futuros incidentes análogos:

Firma del Contacto de Seguridad:

ADDENDA II

REGISTRO DE BRECHA DE SEGURIDAD DE DATOS PERSONALES

Fecha del incidente: **Hora:**	**Fecha de detección**: **Hora**:
Persona que detectó el hecho: **Medios de detección:**	

Origen del incidente: Interno ☐; Externo ☐.

Tipología del incidente: Confidencialidad ☐; Integridad ☐; Disponibilidad ☐.

Descripción de la brecha de seguridad:

Categorías de datos personales afectados:

Identificativos ☐; Credenciales acceso/identificación ☐; DNI/NIE/Pasaporte ☐; De contacto ☐; Económico-financieros ☐; De localización ☐; Otros ☐ (especificar) _____.

Categorías especiales de datos:

Religión/creencias ☐; Salud ☐; Opinión política ☐; Origen racial ☐; Afiliación sindical ☐; Vida sexual ☐; Genéticos ☐; Biométricos ☐; Infracciones penales ☐; Otros ☐ (especificar) _____.

Categorías de personas afectadas:

Clientes ☐; Usuarios ☐; Empleados ☐; Proveedores ☐; Potenciales clientes ☐; Suscriptores ☐; Estudiantes ☐; Menores ☐; Pacientes ☐; Personas en riesgo de exclusión ☐; Otros ☐ (especificar): _____

Número aproximado de interesados afectados: _____.

Número aproximado de registros afectados: _____.

Posibles consecuencias derivadas de la brecha de la seguridad:

¿Se ha resuelto el incidente? SI ☐ NO ☐**. Fecha y hora de resolución**:

Medidas adoptadas para poner remedio a la brecha de seguridad y mitigar sus efectos:

Medidas propuestas para prevenir estos incidentes en el futuro:

¿Procede comunicar el hecho a la AEPD? SI ☐; NO ☐. Indicar motivos:

Fecha en que se notifica a la AEPD (en su caso): (adjuntar justificante de notificación).

¿Procede comunicar el hecho a los interesados? SI ☐; NO ☐. Indicar motivos:

Fecha y modo en que se notifica a los interesados (en su caso):

Firma del Contacto de Seguridad: