Política

Política de Seguridad de la Información aplicable a proveedores de EDP en España

Código	E_PL-SI-001
Versión	5.1
Fecha	16/02/2024
Clasificación	Información Pública

1. HISTÓRICO DE VERSIONES

Versión	Fecha de aprobación	Elaboración	Aprobación	Principales modificaciones
1	03/10/2016	Departamento de Tecnologías de la Información	Departamento de Tecnologías de la Información	Versión inicial
2	23/01/2020	Seguridad de la Información	Seguridad de la Información	Revisión y actualización
3	02/09/2021	Seguridad Lógica	Seguridad Lógica	Revisión y actualización
3.1	24/02/2022	Seguridad Lógica	Seguridad Lógica	Actualización plantilla
3.2	30/03/2022	Seguridad Lógica	Seguridad Lógica	Actualización apartado 5.2.15 herramientas conexión proveedores.
4.0	22/08/2022	Seguridad Lógica	Seguridad Lógica	Actualización plantilla
4.1	04/09/2023	Seguridad Lógica	Seguridad Lógica	Actualización plantilla
5.0	16/02/2024	Seguridad Lógica	Seguridad Lógica	Actualizacion procedimiento
5.1	21/03/2024	Seguridad Lógica	Seguridad Lógica	Actualizacion procedimiento

TABLA DE CONTENIDOS

2. OBJETIVO

En toda organización existe información confidencial, en mayor o menor grado, cuya pérdida o uso indebido puede dañar su reputación. Asimismo, el deterioro o indisponibilidad de los sistemas de información puede interrumpir el normal desarrollo de la operativa, produciendo efectos negativos en la calidad del servicio y los beneficios de la compañía.

El principal objetivo del presente documento es mitigar los riesgos asociados a los sistemas de información de EDP España describiendo lo que se espera de todo el personal que pertenece a otras empresas proveedoras que trabajan para EDP España y que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos de EDP España en general, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información y sistemas manejados por EDP España.

Asimismo, se pretende fomentar el uso de buenas prácticas en materia de seguridad de la información.

Para ello, las empresas proveedoras a las que se les remita este documento se responsabilizan de informar de las normas incluidas en el mismo a las personas que destinen a prestar sus servicios para EDP España, así como de obtener su compromiso de cumplir y respetar dichas normas. Esta Política de Seguridad refleja requerimientos legales y éticos aplicables a las actuaciones de los empleados pertenecientes a empresas proveedoras que trabajan para EDP España. Con dicho propósito, este documento traslada, en lo que es aplicable, lo establecido en la Política de Seguridad de EDP España y las Normas que lo desarrollan, las obligaciones a las que está sujeta por la legislación vigente, y en particular por:

- El Reglamento (EU) 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
- Las exigencias de separación de actividades establecidas en la Ley 24/2013, de 26 de diciembre, del Sector Eléctrico (LSE), en la Ley 34/1998, de 7 de octubre, del Sector de Hidrocarburos (LSH) y en sus normas de desarrollo.

3. AMBITO

El ámbito de aplicación de este documento son todas las actividades desarrolladas por personal que pertenece a otras empresas proveedoras que prestan servicios a EDP España, vinculadas a través del correspondiente contrato de provisión de servicios. Cualquier empresa o tercero que para la prestación de servicios a EDP España tenga que utilizar los sistemas de información o disponga de acceso a los recursos informáticos en general de EDP España, debe tener conocimiento y comprometerse formalmente a acatar esta Política de Seguridad. Es obligación de la empresa proveedora poner en conocimiento de su personal la presente Política de Seguridad. Para ello, los contratos o pedidos que se formalicen entre EDP España y las empresas proveedoras de servicios relacionados con los sistemas de información, recogerán de forma expresa que se conoce esta Política y se comprometen a respetarla, así como que asumen las responsabilidades en que pueden incurrir en caso de no cumplirlas.

4. ACRONIMOS Y ABREVIATURAS

Termino	Abreviatura
LOPDGDD	Ley Orgánica 3/2018 de Protección de Datos y de Garantía de los Derechos Digitales.
LSSI	Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico, Ley 34/2002, de 11 de Julio.
ICS	Información Comercialmente Sensible.
LSE	Ley 24/2013, de 26 de diciembre, del Sector Eléctrico.
LSH	Ley 34/1998, de 7 de octubre, del Sector de Hidrocarburos.
PDCA	Plan-Do-Check-Act: el ciclo de Deming o espiral de mejora continua
RGPD	REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE
EDPE	EDP España

5. DEFINICIONES

Concepto	Definición
Plan-Do-Check-Act	Estrategia de mejora continua de la calidad en cuatro pasos.

6. DESARROLLO METODOLÓGICO

6.1. Observaciones

Esta Política de Seguridad es propiedad de EDP España, tiene carácter Público y únicamente está permitida su utilización y difusión con carácter interno a la empresa proveedora de personal de servicio y por personal autorizado.

6.2. Desarrollo de la Política de Seguridad

6.2.1. Política General de Seguridad de la Información

La dirección de EDP España, como política general de la empresa, garantiza la adecuada gestión de la seguridad de la información procesada y/o albergada por los sistemas y servicios contemplados en el alcance. Para desarrollar esta política, la dirección de EDP España se compromete a:

- ✓ Llevar a cabo un análisis de riesgos periódico que permita mantener una adecuada visión de los riesgos de seguridad de la información a los que están expuestos los activos y desarrollar las medidas necesarias para limitar y reducir dichos riesgos, definiendo las medidas de seguridad a establecer.
- ✓ Desarrollar una completa normativa de seguridad que regule las condiciones en las que la empresa, dentro del alcance establecido, debe desarrollar su actividad para respetar los requerimientos de seguridad establecidos.
- ✓ Destinar los recursos y medios necesarios para desarrollar todas las medidas de seguridad que se determinen, manteniendo un adecuado balance entre coste y beneficio.
- ✓ Establecer un plan de formación y concienciación en materia de seguridad de la información que ayude a todo el personal implicado a conocer y cumplir las medidas de seguridad establecidas y a participar de forma proactiva en la gestión de la seguridad de la información.
- ✓ Desarrollar todas las medidas necesarias para garantizar la adecuada gestión de los incidentes de seguridad que puedan producirse, y que permitan la resolución tanto de las incidencias menores como de las situaciones que puedan poner en riesgo la continuidad de las actividades contempladas.
- ✓ Establecer periódicamente un conjunto de objetivos e indicadores en materia de seguridad de la información que permitan el adecuado seguimiento de la evolución de la seguridad dentro de la empresa.
- ✓ Establecer una metodología de revisión, auditoría y mejora continua del sistema, siguiendo un ciclo PDCA que garantice el mantenimiento continuo de los niveles de seguridad deseados. EDP España establece los procedimientos y formas de actuación necesarias para garantizar el correcto desarrollo de esta política, que se plasman en un sistema de seguridad, documentado y conocido por todo el personal de EDP España, y que cumple los requisitos establecidos en la norma.

6.2.2. Principios generales

Tal y como se ha establecido en el ámbito de aplicación, todo el personal externo que desarrolle labores para EDP España deberá cumplir con la Política de Seguridad recogida en el presente documento. En caso de incumplimiento de cualquiera de estas obligaciones, EDP España se reserva el derecho de veto sobre el personal externo que haya cometido la infracción, así como la adopción de las medidas sancionadoras que se consideren pertinentes en relación a la

empresa contratada, y que pueden llegar a la resolución de los contratos que tenga vigentes con dicha empresa. Todo el personal que acceda a los sistemas de información de EDP España deberá seguir las siguientes normas de actuación:

- ✓ Proteger la información confidencial perteneciente o cedida por terceros a EDP España de toda revelación no autorizada, modificación, destrucción o uso incorrecto, ya sea accidental o no.
- ✓ Proteger todos los sistemas de información y redes de telecomunicaciones contra accesos o usos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.
- ✓ Para obtener el acceso a los sistemas de información propios o bajo supervisión de EDP España será necesario disponer de un acceso autorizado.
- ✓ Será necesario conocer, aceptar y cumplir la presente Política antes de poder acceder a los sistemas de información de EDP España. De forma adicional, todo el personal con responsabilidades específicas dentro del ámbito de actuación indicado deberá asegurarse de que se cumplen las siguientes medidas:
  - ❖ Con carácter general, todo diseño, desarrollo, implementación y operación deberá incorporar mecanismos de identificación, autenticación, control de acceso, auditoría e integridad, que se especificarán para cada caso concreto.
  - ❖ Se deberán incorporar identificaciones seguras y únicas para la autenticación de usuarios.
  - ❖ Para un correcto funcionamiento en materia de seguridad deberán compartirse las labores de seguridad entre usuarios, administradores y los encargados directos de la propia seguridad.
  - ❖ Deberán tomarse todas las precauciones posibles para proteger físicamente los sistemas y prevenirlos frente al robo, destrucción o interrupción.
  - ❖ Deberá existir un plan de recuperación del sistema para el caso en que se dé robo, destrucción o interrupción del servicio.
  - ❖ Deberá asegurarse la confidencialidad de la información almacenada, tanto en formato electrónico como no electrónico.
  - ❖ Todos los intervinientes en el plan de continuidad de negocio deberán conocer y saber aplicar cuando sea necesario dicho plan.
  - ❖ El personal del área de operación deberá tener conocimiento de los procedimientos de recuperación de datos de carácter personal, de sanitización de los soportes de datos de carácter personal y del procedimiento de registro entrada/salida de dichos soportes.
  - ❖ Se prohíbe cualquier actividad ajena a la reflejada en el contrato de servicio.
  - ❖ La empresa colaboradora debe formar en cuestiones básicas de ciberseguridad a sus empleados y aportar evidencias de dicha formación.

El Departamento de Seguridad Lógica de EDPE centraliza los esfuerzos globales de protección de los activos de EDP España, a fin de asegurar el correcto funcionamiento de las tecnologías de la información que soportan los procesos de la organización. De forma genérica, los activos incluyen toda forma de información, además de las personas y la tecnología que soportan los procesos de información.

El Departamento de Seguridad Lógica de EDPE dispondrá de un inventario actualizado sobre las Empresas Colaboradoras que contará con los siguientes datos:

- Nombre y responsable de la contrata (teléfono y correo electrónico de contacto).
- Responsable[1] de la seguridad de la información de la contrata (teléfono y correo electrónico de contacto).
- Responsable de la contrata en EDP.
- Actividades desarrolladas por la contrata.

Por cada contrata, también deberá informarse de los usuarios y equipos corporativos utilizados.

El responsable de la contrata en EDP deberá informar al Departamento de Seguridad Lógica de EDPE cuando haya alteraciones de cualquiera de estos datos.

6.2.3. Confidencialidad de la Información

La confidencialidad de la información se define como la garantía de que la información no es divulga a personas no autorizadas.

Con el fin de preservarla:

- ✓ El personal externo que tenga acceso a información de EDP España deberá considerar que dicha información, por defecto, tiene el carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella información de EDP España a la que haya tenido acceso a través de los medios de difusión pública de información.
- ✓ Los usuarios protegerán la información confidencial a la que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentre contenida esa información.
- ✓ Los empleados de las empresas colaboradoras solo utilizarán y accederán a aquella información estrictamente necesaria que les permita ejecutar las tareas para las cuales han sido contratados.
- ✓ Se guardará por tiempo indefinido la máxima reserva y no se emitirá al exterior información confidencial en cualquier tipo de soporte, salvo que esté debidamente autorizado.
- ✓ Se utilizará el menor número de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera del alcance de terceros.
- ✓ En relación a la utilización de agendas de contactos dispuestas por EDP España (por ejemplo, Outlook) el personal externo únicamente introducirá determinados datos personales que sean indispensables como nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.
- ✓ Ningún colaborador externo en proyectos o trabajos puntuales deberá poseer, para usos no propios de su responsabilidad, ningún material o información propia o confiada a EDP España tanto ahora como en el futuro.
- ✓ En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado de la empresa proveedora de servicios entre en posesión de información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.

[1] El responsable de la Seguridad de la Información de la contrata y el responsable de la contrata pueden ser el mismo

- ✓ Asimismo, el empleado de la empresa proveedora deberá devolver el o los soportes mencionados inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación de su empresa con EDP España. La utilización continuada de la información en cualquier formato o soporte distinta a la pactada y sin conocimiento de EDP España no supondrá, en ningún caso, una modificación de este punto.
- ✓ Una vez finalizada la relación contractual entre EDP y la Empresa Colaboradora, tanto ésta como los empleados de la misma deberán guardar secreto profesional, quedando totalmente prohibido compartir cualquier tipo de información clasificada obtenida de las tareas asociadas a su relación con EDP. Además, la empresa colaboradora está obligada a destruir físicamente toda la documentación y datos obtenidos, tanto en papel, como en cualquier soporte físico. Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para EDP España.
- ✓ El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos, previsto en el artículo 197 del Código Penal, que puede dar derecho a exigir compensaciones.
- ✓ Para garantizar la seguridad de los Datos de Carácter Personal albergados en ficheros automatizados, el personal que pertenece a empresas proveedoras de servicios deberá observar las siguientes normas de actuación, además de las consideraciones ya mencionadas:
  - ❖ El personal sólo podrá crear ficheros temporales que contengan datos de carácter personal cuando sea necesario para el desempeño de su trabajo. Estos ficheros deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.
  - ❖ Queda expresamente prohibida la salida de soportes informáticos o papel que contengan datos de carácter personal, fuera de los locales en los que esté ubicada dicha información.
  - ❖ El propietario de la información se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
  - ❖ Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse de forma cifrada en un lugar de acceso restringido al personal autorizado.

6.2.4. Información comercialmente sensible (ICS)

De acuerdo con las obligaciones de separación de actividades recogidas en la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos, y en la Ley 24/2013, de 26 de diciembre, del Sector Eléctrico, las sociedades que realicen actividades reguladas tienen la prohibición de compartir información comercialmente sensible con las empresas del grupo al que pertenecen, en el caso de que éstas realicen actividades liberalizadas.

Por ello, es necesario que en la ejecución del servicio contratado el proveedor guarde la confidencialidad de la información comercialmente sensible que las diferentes distribuidoras de EDP en España le proporcionen.

Así, para facilitar el cumplimiento de la regulación relativa a la separación de actividades se incluirá en el contrato una cláusula que recoja dicha obligación por parte del proveedor.

A los efectos de este punto, se considerará información comercialmente sensible cualquier información concreta referida al ejercicio de las actividades reguladas que no sea pública y que, de comunicarse o haberse comunicado a las actividades liberalizadas, podría influir, de manera apreciable, en el resultado de su negocio o suponerles una ventaja competitiva en el desarrollo de las actividades liberalizadas que realizan.

La empresa colaboradora deberá someterse al tratamiento que las distribuidoras tengan establecido para dicha información.

La empresa colaboradora se asegurará de que todos los medios humanos que intervengan en la ejecución del servicio respetan el deber de confidencialidad en los términos que han sido señalados.

En caso de incumplimiento, EDP España se reserva el derecho a resolver el contrato. En cualquier caso, la empresa colaboradora asumirá íntegramente la responsabilidad que derive de dicho incumplimiento y deberá indemnizar a las sociedades del Grupo EDP que pudieran verse perjudicadas por el mismo.

6.2.5. Control de acceso físico a instalaciones de EDP ESPAÑA

Se establecen las siguientes normas:

- ✓ El personal externo no podrá permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión.
- ✓ Se limitará el acceso al personal de soporte externo a las áreas especialmente protegidas. Este acceso, como el de cualquier otra persona ajena que requiera acceder a áreas protegidas, se asignará únicamente cuando sea necesario y se encuentre autorizado, y siempre bajo la vigilancia de personal autorizado. El sistema de control mantendrá un registro de todos los accesos de personas ajenas.
- ✓ Se acompañará a los visitantes en áreas protegidas y el sistema registrará la fecha y hora de su entrada y salida. Dichas personas deberán ir provistos de la debida tarjeta de identificación o permiso correspondiente y pasar por alguno de los sistemas de control de acceso físico. Sólo se permitirá el acceso previa identificación de la persona de contacto en EDP España.
- ✓ Se consideran áreas especialmente protegidas:
  - o Salas Técnicas.
  - o Centros de Proceso de Datos.
  - o Salas de Control o de Mando.
  - o Despacho de Gestión de Energía.
  - o Despacho Central de Distribución.
  - o Salas con armarios o equipamiento de Redes y Comunicaciones.
  - o Salas con armarios o equipamiento eléctrico o electrónico.
  - o Despachos de Dirección.
  - o Instalaciones Técnicas de Gas y Electricidad.
  - o Botiquines y despachos médicos.

6.2.6. Uso apropiado de los recursos

Los recursos que EDP España pone a disposición del personal externo, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para

la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso. Queda terminantemente prohibido:

- ✓ El uso de estos recursos para actividades no relacionadas con el propósito del servicio, o bien la extralimitación en su uso.
- ✓ La búsqueda o explotación de vulnerabilidades en cualquier aplicación o equipos.
- ✓ Los equipos y/o aplicaciones que no estén especificados como parte del software o de los estándares de los recursos informáticos propios de EDP España o bajo supervisión de EDP España.
- ✓ Introducir en los sistemas de información o la red corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
- ✓ Ejecutar software desde dispositivos externos.
- ✓ La conexión de lápices de memoria o dispositivos de almacenamiento externos sin la debida autorización por parte del responsable.
- ✓ Introducir voluntariamente cualquier tipo de malware (programas, macros, applets, controles ActiveX, etc.), greyware, dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. El proveedor tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.
- ✓ Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.
- ✓ Intentar acceder a áreas restringidas sin la debida autorización.
- ✓ Intentar distorsionar o falsear los registros, “log” de los sistemas de información.
- ✓ Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.
- ✓ Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, o dañar o alterar los recursos informáticos.
- ✓ Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos. Estos actos podrían constituir un delito de daños, según la legislación vigente.
- ✓ Albergar datos de carácter personal en las unidades locales de disco de los puestos (ordenadores personales) de usuario.
- ✓ Cualquier fichero introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y control de virus.
- ✓ Conectar cualquier tipo de dispositivo no homologado a la red de comunicaciones de EDP. Tienen la consideración de equipos homologados, los ordenadores corporativos de EDP y los ordenadores de proveedor que cumplan los requisitos mínimos exigidos en el documento “Requisitos de conexión de Empresas Colaboradoras a la red de datos de EDP España” y que además hayan sido previamente inventariados y aprobada su conexión por el Departamento de Seguridad Lógica de EDP Sucursal en España.
- ✓ Cualquier tipo de actividad ajena a la propia de las tareas a realizar por parte del colaborador.

6.2.7. Protección frente a malware

Los recursos que el proveedor utiliza para la prestación del servicio a EDP España deberán seguir las siguientes indicaciones:

- ✓ Se mantendrán los sistemas actualizados con los últimos parches de seguridad disponibles y deberán disponer de navegador web con las últimas versiones.
- ✓ El software antivirus se deberá instalar y usar en todos los servidores, en su caso, y en todos los ordenadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
- ✓ El software antivirus deberá estar siempre habilitado y sin posibilidad de desactivación por parte del usuario. Se establecerá una actualización automática de los ficheros de definición de virus tanto en los ordenadores personales como servidores, en su caso, así como de bloqueo frente a la detección de virus informáticos.
- ✓ Todo el software debe estar correctamente licenciado, por lo que se prohíbe expresamente el uso de programas piratas, crackers y/o aplicaciones que permitan la ejecución sin licencia.
- ✓ En caso de que sea detectado cualquier malware en uno de los equipos conectados a la red de EDP, dicho equipo será desconectado de dicha red sin que sea necesario aviso previo. El Departamento de Seguridad Lógica EDPE notificará con los medios disponibles el problema encontrado por lo que será responsabilidad de la contrata la eliminación del malware detectado. La conexión de nuevo a la red corporativa debe ser autorizada por el Departamento de Seguridad Lógica de EDPE, la cual solicitará toda la información necesaria sobre el equipo con el fin de asegurar la limpieza de este.

6.2.8. Intercambio de información

Se establecen las siguientes normas:

- ✓ Los usuarios no deben ocultar o manipular su identidad bajo ninguna circunstancia.
- ✓ No se permite el uso de usuarios genéricos.
- ✓ La distribución de información ya sea en formato digital o papel se realizará mediante los dispositivos facilitados por EDP España para tal cometido y con la finalidad exclusiva de facilitar las funciones del puesto. EDP España se reserva, en función del riesgo identificado, la implementación de medidas de control, registro y auditoría sobre estos dispositivos de difusión. Está prohibido compartir ficheros a través de plataformas no autorizadas por EDP. Cualquier tipo de dato del Grupo EDP requiere su almacenamiento en servidores ubicados en el espacio europeo.
- ✓ En relación al intercambio de información, se considerarán no autorizadas las siguientes actividades:
  - ❖ Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual.
  - ❖ Transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
  - ❖ Transferencia de ficheros a terceras partes no autorizadas de material de EDP o material que es de alguna u otra manera confidencial.
  - ❖ Transmisión o recepción de ficheros que infrinjan la Ley de Protección de Datos de Carácter Personal o directrices de EDP España.
  - ❖ Transmisión o recepción de juegos y/o aplicaciones no relacionadas con el negocio.

- ❖ Participación en actividades de Internet como grupos de noticias, juegos, apuestas u otras que no estén directamente relacionadas con el negocio.
- ❖ Todas las actividades que puedan dañar la buena reputación de EDP España están prohibidas en Internet y en cualquier otro lugar. Esto se refiere también a actividades realizadas para el propio beneficio económico del usuario o de terceras partes, y a actividades de naturaleza política.
- ❖ Almacenar información clasificada o personal en recursos distintos a los que EDP pone a disposición del Colaborador.

- ✓ La transmisión de datos de carácter personal de nivel alto a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.
- ✓ Queda prohibido el tratamiento de información que contenga datos de carácter personal fuera de los locales autorizados y habilitados para tal.

6.2.9. Uso del correo electrónico

La cuenta de correo electrónico tiene la consideración de herramienta que la empresa colaboradora pone a disposición de sus empleados para el desempeño de los trabajos contratados.

Se establece el siguiente criterio general:

- ✓ Cada usuario de los sistemas informáticos de EDP España dispondrá de una cuenta de correo electrónico específica y única, asignada exclusivamente a dicho usuario.
- ✓ Con carácter general, los usuarios externos no dispondrán de una dirección de correo del Grupo EDP
- ✓ En el momento de su registro, el usuario externo debe aportar una dirección de correo del dominio de su propia empresa (preferible) o bien una dirección de correo personal.
- ✓ Los dominios del correo electrónico de las EECC deberán disponer de los siguientes registros de seguridad:
  - o SPF correctamente configurado.
  - o DKIM para la firma de mensajes.
  - o DMARC no se considerará obligatorio, pero si recomendable.
  - o Sistemas de antivirus integrado.

  En caso de no disponer de estos registros correctamente configurados, no es posible garantizar la correcta recepción de los correos.

Este criterio general es compatible con el hecho de que dichos usuarios externos pueden acceder a los buzones de correo genéricos que sean preciso para desarrollar su operativa de trabajo. El envío de correos desde estos buzones genéricos no identifica al emisor.

De forma excepcional, en consideración a las circunstancias que se justifiquen, y siempre previa autorización expresa, un usuario externo podría disponer de una dirección de correo del Grupo EDP. En tal caso, el responsable del servicio de EDP España debe cursar la correspondiente solicitud que deberá ser evaluada conjuntamente por Recursos Humanos y Seguridad Lógica de EDP España.

La utilización del correo electrónico por parte de los usuarios externos estará sujeta a las siguientes normas:

- ✓ Se considera al correo electrónico una herramienta más de trabajo provista al usuario con el fin de ser utilizada conforme al uso para el cual está destinada. Esta consideración facultará a EDP España a implementar sistemas de control destinados a velar por la protección y el buen uso de este recurso. Esta facultad, no obstante, se ejercerá salvaguardando la dignidad del usuario y su derecho a la intimidad.
- ✓ El sistema de correo electrónico de EDP España no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares.
- ✓ Está expresamente prohibido el uso de las infraestructuras de comunicaciones de EDP para el envío o recepción de correo electrónico, incluso desde cuentas personales, que contenga cualquier tipo de mensaje publicitario, dañino, malware, pornográfico, relacionado con juegos de azar, etc.
- ✓ Los usuarios no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples usuarios).
- ✓ Queda expresamente prohibido el uso de la dirección de correo electrónico de EDP para darse de alta en cualquier tipo de actividad ajena a las tareas que realiza, así como para su uso personal.
- ✓ La dirección de correo electrónico no podrá ser compartida entre varios usuarios excepto que se trate de un buzón genérico al que accedan distintos colaboradores.
- ✓ No está permitida la transmisión vía correo electrónico de información que contenga datos de carácter personal de nivel alto, salvo que la comunicación electrónica esté cifrada y el envío este expresamente permitido.
- ✓ No está permitida la transmisión vía correo electrónico de información confidencial de EDP España salvo que la comunicación electrónica esté cifrada y el envío este expresamente permitido.
- ✓ Los usuarios deben ser muy cuidadosos con todos aquellos correos de remitentes desconocidos o que incluyan algún fichero que no sea esperado, en caso de dudas deberán informar de ello al Departamento de Seguridad Lógica (seguridad.logica@edpenergia.es) que les dará las pautas de acción.
- ✓ En caso de que un colaborador reciba correos sospechosos de contener cualquier tipo de malware o phishing, debe ponerlo en conocimiento Departamento de Seguridad Lógica de EDP España (seguridad.logica@edpenergia.es).

6.2.10. Conectividad a Internet

La utilización de Internet por parte de los usuarios externos estará sujeta a las siguientes normas:

- ✓ Internet es una herramienta de trabajo. Todas las actividades en Internet deberán estar en relación con tareas y actividades de trabajo. Los usuarios no deben buscar o visitar sitios que no sirvan como soporte al servicio prestado a EDP España.
- ✓ Todo el tráfico desde y hacia Internet será inspeccionado en búsqueda de amenazas. En caso de que algún equipo se encuentre accediendo a sitios clasificados como maliciosos (pornografía, juego, etc.) o ajenos al negocio podrá ser desconectado de la red sin que sea necesario aviso previo.
- ✓ El Grupo EDP se reserva el derecho de, en lo permitido por el marco legal, y sin aviso previo, limitar el acceso total o parcial a Internet a partir de la red informática y terminales del Grupo EDP.
- ✓ El acceso a Internet desde la red corporativa se restringe por medio de dispositivos de control incorporados en la misma.

- ✓ Los usuarios no deberán usar el nombre, símbolo, logotipo de EDP o símbolos similares al de EDP España en ningún elemento de Internet (correo electrónico, páginas web, etc.) no justificado por actividades estrictamente laborales.
- ✓ Únicamente se permitirá la transferencia de datos de o a Internet en conexión con las actividades del servicio prestado a EDP España. La transferencia de ficheros no relativa a estas actividades (por ejemplo, la descarga de juegos de ordenador, ficheros de sonido y contenidos multimedia) está prohibida, quedando expresamente prohibido el uso de software tipo P2P o torrents.

6.2.11. Responsabilidades del usuario

Todo usuario externo, por el mero hecho de serlo, asume determinadas responsabilidades:

- ✓ Cada usuario será responsable de su identificador y todo lo que de él se derive, por lo que es imprescindible que este sea únicamente conocido por el propio usuario; no deberá revelarlo al resto de usuarios bajo ningún concepto.
- ✓ El usuario será responsable de todas las acciones registradas en los sistemas informáticos de EDP España con su identificador.
- ✓ Los usuarios deberán seguir las directivas definidas en relación a la gestión de las contraseñas.
- ✓ Los usuarios deberán asegurar que los equipos quedan protegidos cuando estén desatendidos.
- ✓ Se establecerán las siguientes políticas de escritorio limpio para proteger documentos en papel y dispositivos de almacenamiento removibles con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:
  - ❖ Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
  - ❖ Bloquear su equipo de trabajo impidiendo el acceso al mismo a cualquier otro usuario.
  - ❖ Apagar el equipo al final de la jornada.
  - ❖ Asegurar la confidencialidad de los documentos tanto en los puntos de recepción y envío de información (correo postal, máquinas de escáner y fax) como en los equipos de duplicado (fotocopiadora, fax y escáner).
  - ❖ La reproducción o envío de información con este tipo de dispositivos queda bajo la responsabilidad del usuario.
  - ❖ Los listados con datos de carácter personal o información confidencial deberán almacenarse en lugar seguro al que únicamente tengan acceso personal autorizado.
  - ❖ Los listados con datos de carácter personal o información confidencial deberán eliminarse de manera segura una vez no sean necesarios.
- ✓ En caso de identificarse incidentes o debilidades relacionadas con la seguridad de la información, se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar esta supuesta debilidad o incidente de seguridad.

6.2.12. Equipos de usuario

Sobre el equipamiento informático asociado al puesto del usuario se establecen los siguientes principios:

- ✓ Todos los puestos de usuario con conectividad a recursos informáticos de EDP España estarán controlados por EDP España.

- ✓ Ningún usuario intentará por ningún medio transgredir el sistema de seguridad y las autorizaciones, ni dispondrá de herramientas que puedan realizarlo.
- ✓ Se prohíbe la captura de tráficos de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditoría expresamente autorizadas por el Departamento de Seguridad Lógica de EDPE.
- ✓ Todos los equipos informáticos deben estar cifrados.
- ✓ En ningún caso los equipos deben quedar desatendidos, en caso de ausencias del usuario por un corto periodo de tiempo deben quedar bloqueados, en su defecto cuando la ausencia se prolongue durante más tiempo deberán quedar apagados.
- ✓ En caso de pérdida o robo de un equipo o soporte, debe informarse lo antes posible al departamento de Sistemas de la información.

6.2.13. Identificadores de usuario y contraseñas

El personal de empresas proveedoras de servicios que accede a los sistemas de información de EDP España dentro de su ámbito de trabajo, es responsable de asegurar que los datos, las aplicaciones y los recursos informáticos sean usados únicamente para el desarrollo de la operativa propia para la que fueron creados e implantados. Este personal está obligado a utilizar los recursos de EDP España y los datos contenidos en ellos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales. Para obtener el acceso a los sistemas de información este personal debe disponer de un acceso autorizado (identificador de usuario y contraseña) sobre el que, como usuarios de sistemas de información, deben observar los siguientes principios de actuación y buenas prácticas:

- ✓ Cuando el usuario recibe su identificador de acceso a los sistemas de EDP España se considera que acepta formalmente la Política de Seguridad vigente.
- ✓ Las credenciales de acceso a los sistemas de EDP son estrictamente confidenciales.
- ✓ Todos los usuarios con acceso a un sistema de información dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.
- ✓ Los intentos de logon sin éxito son limitados en número.
- ✓ Todos los intentos de logon son registrados, tanto tengan éxito o no.
- ✓ Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- ✓ Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
- ✓ Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- ✓ Los usuarios no deben incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- ✓ Las contraseñas estarán constituidas por combinación de caracteres alfanuméricos y símbolos.
- ✓ Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista ni al alcance de terceros.
- ✓ La cuenta de usuario es nominativa y no deberá ser compartida con nadie más.
- ✓ Los usuarios no deben utilizar las mismas contraseñas para uso personal y profesional.
- ✓ Los accesos autorizados temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
- ✓ En relación a datos de carácter personal, exclusivamente el personal autorizado para ello en el Documento de Seguridad podrá conceder, alterar o anular el acceso autorizado

sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

- ✓ Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder de inmediato al cambio de su contraseña y contactar con el Departamento de Seguridad Lógica de EDP España.
- ✓ El cambio de la contraseña se realizará en la herramienta de gestión de accesos de EDP España.

6.2.14. Software

Sobre el software se establecen los siguientes principios:

- ✓ EDP España facilitará al proveedor un documento que incluirá directrices a seguir en relación con el software de los equipos ("Conexión de Empresas Colaboradoras a la red de datos de EDP en España)".
- ✓ Todo el personal que accede a los sistemas de información de EDP España debe utilizar únicamente las versiones de software indicadas y siguiendo sus normas de utilización.
- ✓ Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.
- ✓ Se prohíbe el uso de software no homologado.
- ✓ Se prohíbe el uso de software sin su respectiva licencia.
- ✓ Se prohíbe el uso de software crackeado o pirateado.
- ✓ No está permitido la ejecución de software desde dispositivos extraíbles.

6.2.15. Conexión a la red

Sobre la conexión a la red se establecen los siguientes principios:

- ✓ En caso de que el proveedor necesite acceder a la red de EDP para la prestación de los servicios, debe solicitar el documento "Conexión de Empresas Colaboradoras a la red de datos de EDP en España" a la dirección de correo seguridad.logica@edpenergia.es, identificando la empresa, persona de contacto y propuesta a la que opta.
- ✓ El acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación previa validación del acceso.
- ✓ Las conexiones VPN establecidas por los proveedores deberán ser VPN Client to Site y mediante equipos terminales de acuerdo con las requisitos del documento previo y utilizando el servicio de cliente VPN proporcionado a tal efecto.
- ✓ El Grupo EDP se reserva el derecho de, sin aviso previo, bloquear, suspender, alterar o monitorizar los servicios soportados en su red informática y puestos a disposición de las entidades externas.
- ✓ No se deberá conectar a ninguno de los recursos de EDP España ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas a la red corporativa.
- ✓ Nadie deberá conectarse a la red corporativa a través de otros medios que no sean los definidos.
- ✓ Está expresamente prohibido la conexión de equipos no suministrados o autorizados por EDP a la red corporativa.
- ✓ EDP se reserva el derecho a desconectar de la red corporativa y sin aviso previo a cualquier equipo utilizado por un proveedor cuando se detecten actividades que contravengan los principios y normas expresados en el presente documento.

- ✓ Cuando los colaboradores externos se encuentren desplazados o de viaje y tengan necesidad de utilizar las aplicaciones de EDP, se pondrá a su disposición una herramienta designada por el Departamento de Tecnologías de la Información, para ello su responsable en EDP realizará la solicitud correspondiente en el catálogo de Service Now. Asimismo, para la realización de estas conexiones desde el exterior no deben utilizarse redes WiFi públicas.
  - o En aquellos casos en los que sea necesario múltiple factor de autenticación, la empresa colaboradora deberá facilitar un smartphone a su colaborador en el que recibir el token de autenticación vía SMS o aplicación móvil para acceso a los sistemas.
  - o El tiempo de conexión deberá ser el mínimo y necesario para el desempeño del servicio.

6.2.16. Gestión de accesos

Existe un proceso formal para el registro, concesión, alteración y revocación de accesos a los usuarios, aplicable a todos los sistemas de Información del Grupo EDP.

Se establecen los siguientes principios:

- ✓ Se debe asegurar la comunicación de las reglas y responsabilidades en el uso de los sistemas de información del Grupo EDP a los usuarios al atribuirles cualquier acceso a los sistemas.
- ✓ Para cada sistema existe un conjunto de perfiles y privilegios que se atribuyen a los usuarios de acuerdo con sus necesidades.
- ✓ Los privilegios de acceso a los sistemas se atribuyen a los usuarios considerando las necesidades efectivas para el desempeño de sus funciones, no debiendo ser atribuidos ni por exceso ni por defecto.
- ✓ Los sistemas del Grupo EDP, por omisión, bloquean el acceso a los usuarios no autorizados.
- ✓ Los privilegios de acceso a los sistemas garantizan una correcta segregación de funciones. En los casos en los que no es posible garantizar la segregación de funciones, están implementados los controles compensatorios adecuados.
- ✓ Cualquier solicitud de atribución o modificación de privilegios de acceso a los sistemas del Grupo EDP se refleja en la herramienta de gestión de identidades y accesos y posteriormente debe ser aprobada.
- ✓ Los accesos y respectivos privilegios solo se implementan en los sistemas después de obtener todas las aprobaciones necesarias.
- ✓ Se mantiene un registro formal de todos los usuarios autorizados y respectivos privilegios de acceso a los sistemas del Grupo EDP.
- ✓ Las modificaciones en las necesidades de acceso a los sistemas deben llevar aparejados los ajustes a los derechos de acceso.
- ✓ Los privilegios de acceso a los sistemas atribuidos a los usuarios son revocados de forma automática cuando termina su relación profesional con el Grupo EDP.
- ✓ Se realiza una revisión periódica con el fin de eliminar o bloquear cuentas redundantes o innecesarias.
- ✓ Los usuarios deben tener asociados, identificadores individuales (user ID), protegidos por contraseña.
- ✓ La nomenclatura utilizada en la generación de los identificadores obedece a reglas definidas por el Grupo EDP.

- ✓ El identificador de usuario permite reconocer su identidad, pero nunca sus niveles de privilegios.
- ✓ El identificador debe ser personal, de uso exclusivo y único para todos los sistemas (cuando sea técnicamente viable).
- ✓ Los identificadores de los usuarios que ya no tienen vínculo con el Grupo EDP no pueden ser atribuidos a otros usuarios, excepto en áreas de gran rotación de personas (por ejemplo, Contact Center).
- ✓ En los casos de áreas de gran rotación referidas en el punto anterior, debe existir una aprobación formal de la excepción por el responsable del área.
- ✓ Para las excepciones debe quedar registrado y mantenido un histórico de las personas asociadas a un user ID y el tiempo que durado dicha asociación (fechas de inicio y de fin).
- ✓ El Grupo EDP se reserva el derecho de, sin aviso previo, bloquear, suspender, modificar y monitorizar a los usuarios de sus sistemas y los respectivos privilegios de acceso.
- ✓ El responsable de la empresa colaboradora debe notificar al responsable en EDP de la misma, todos los cambios habidos en cuanto a las personas, identidades y equipos que estén conectados a la red corporativa. Además, el responsable de EDP tiene la obligación de comunicar esta información al Departamento de Seguridad Lógica de EDPE, el cual mantendrá un inventario actualizado de las conexiones realizadas a la red corporativa por las contratas.
- ✓ En los casos en que se requiera la instalación de aplicaciones corporativas en smartphones o tablets de la empresa colaboradora, esta aceptará su inclusión en el sistema de gestión remota (MDM) del Grupo EDP y aceptará las políticas generales de uso de los sistemas indicados en cada caso. Esto supondrá el control del software instalado en el dispositivo y se garantizará la privacidad del usuario.

6.2.17. Propiedad intelectual

En relación a la Propiedad Intelectual se aplicarán los siguientes principios:

- ✓ Las entidades externas que acceden a Internet a partir de la red informática y terminales del Grupo EDP son responsables de respetar los derechos de propiedad intelectual aplicables a los contenidos accedidos.
- ✓ Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.
- ✓ Los usuarios externos únicamente podrán utilizar material autorizado por su empresa o por EDP España para el desarrollo de sus funciones.
- ✓ Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia.
- ✓ Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.
- ✓ EDP España únicamente autorizará el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

6.2.18. Incidencias

En el caso de detectarse alguna incidencia relacionada con los sistemas de información se seguirán las siguientes normas:

- ✓ Se deberá notificar al Departamento de Seguridad Lógica de EDPE (seguridad.logica@edpenergia.es) cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados, dispositivos de almacenamiento, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos, etc.
- ✓ Todo el personal externo deberá ponerse en contacto con el servicio del centro de atención al usuario (Global Service Desk) en caso de que detecte cualquier incidencia relacionada con la información o los recursos informáticos de EDP España.
- ✓ El centro de atención al usuario de EDP España (Global Service Desk) centraliza la recogida, análisis y gestión de las incidencias recibidas.
- ✓ Cualquier usuario podrá trasladar al Departamento de Seguridad Lógica de EDPE (seguridad.logica@edpenergia.es) sugerencias y/o dudas, que pueda tener relación con la seguridad de la información y las directrices contempladas en la presente Política.

6.3. Requisitos de seguridad para la externalización

La empresa proveedora debe documentar y aplicar la sistemática adecuada para asegurar los siguientes requisitos:

- ✓ El personal afectado debe conocer y aplicar la Política de Seguridad.
- ✓ Deben cumplirse los requisitos reglamentarios y normativos aplicables (LOPDGDD, RGPD, LSSI, ICS).
- ✓ EDP España facilitará al proveedor un documento con las directrices a seguir para la conexión a su red corporativa y la instalación de los puestos de trabajo (“Conexión de Empresas Colaboradoras a la red de datos de EDP en España”).
- ✓ La lista de usuarios autorizados y el registro de accesos estarán disponibles para su verificación por parte del responsable del servicio.
- ✓ El acceso ocasional a las instalaciones de personas no autorizadas deberá quedar registrado. Estas personas estarán debidamente identificadas y acompañadas en todo momento por personal autorizado.
- ✓ El responsable del servicio por parte de EDP España podrá verificar estas condiciones personalmente o delegar en otra persona de EDP España o en otra empresa especializada. Deberá facilitarse el acceso para los aspectos relacionados con auditorías internas o externas cuando EDP España lo estime conveniente.
- ✓ El proveedor notificará al Departamento de Seguridad Lógica de EDPE (seguridad.logica@edpenergia.es) si se ha producido una brecha de seguridad o cualquier cambio en el sistema de seguridad en el momento en que se detecte. Dicha brecha será tomada como una no conformidad según su sistema de calidad ISO 9000 (o procedimiento equivalente).
- ✓ El sistema debe tener en cuenta el procedimiento de devolución/destrucción de los datos y activos una vez finalizado el servicio. En caso de detectarse algún incumplimiento de estos requisitos, será registrado en su sistema de calidad ISO 9000 (o procedimiento equivalente) dónde se establecerán las acciones correctivas y preventivas pertinentes y se dará seguimiento de la misma hasta su cierre en un plazo máximo acordado con el responsable del servicio.

EDP España se reserva el derecho de exigir:

- ✓ La implementación de cualquier mecanismo que EDP España considere necesario para garantizar la seguridad de acceso a sus datos y activos. Asimismo, podrá exigir las

penalizaciones y/o las garantías apropiadas en función de los riesgos de incumplimiento o deterioro de los activos del servicio.

- ✓ La presencia y colaboración, de todas las empresas colaboradoras y proveedoras y su mejor ayuda en la restauración –bajo la coordinación directa de EDP España- de la actividad normal de sus operaciones de negocio, después de que éstas hayan sido interrumpidas por una emergencia o desastre.
- ✓ La tenencia de políticas y planes de continuidad de negocio o contingencias que permitan asegurar la continuidad de las actividades de estas compañías en el caso de que se vieran afectadas por una catástrofe o situación de desastre. De igual forma, EDP España se reserva el derecho de auditar la existencia y grado de implantación de los mencionados planes.

6.4. Seguimiento y control

Con el fin de velar por el correcto uso de los mencionados recursos, a través de los mecanismos formales y técnicos que se considere oportunos, EDP España comprobará, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente, la correcta utilización de dichos recursos por todos los usuarios. En caso de apreciar que alguien utiliza incorrectamente aplicaciones y/o datos, principalmente, así como cualquier otro recurso informático, se le comunicará tal circunstancia y se le facilitará, en su caso, la formación necesaria para el correcto uso de los recursos.

En caso de apreciarse mala fe en la incorrecta utilización de las aplicaciones y/o datos, principalmente, así como cualquier otro recurso informático, EDP España ejercerá las acciones que legalmente le amparen para la protección de sus derechos.

6.5. Actualización de la Política de Seguridad

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas aportaciones legales en la materia, EDP España se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todas las empresas proveedoras de servicios a las que les aplique utilizando los medios que se consideren pertinentes. Es responsabilidad de cada empresa proveedora garantizar la lectura y conocimiento de la Política de Seguridad más reciente de EDP España por parte de su personal.

En caso de incoherencias, se debe seguir la legislación oficial vigente y el documento será modificado con el fin de evitar conflictos legales.

6.6. Otros

El cumplimiento de esta política no exime a la empresa colaboradora del cumplimiento de los contratos que tiene con EDP.