Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

Políticas de Seguridad para personal de empresas proveedoras

Fecha: 11/03/2022

Referencia: **PSP v4.2**

Mediterráneo, 14 • 01010 Vitoria-Gasteiz • Posta-kutxatila / Apartado: 809 • 01080 Vitoria-Gasteiz • Tel. 945 01 73 00* • Fax. 945 01 73 01 • www.ejie.eus

Versión	Fecha	Resumen de cambios	Elaborado por:	Aprobado por:
1.0	01/12/2000	Primera versión	Responsable de Seguridad	Director General
2.0	05/05/2008	Adaptación al modelo ISO/IEC 27001:2005	Responsable de Seguridad	Director General
2.1	31/07/2008	Inclusión de cláusulas de control relacionadas con el Plan de Continuidad de Negocio	Responsable de Seguridad	Director General
2.2	08/10/2010	Revisión general	Responsable de Seguridad	Director General
3.0	14/03/2012	Adaptación global del documento para diferentes tipologías de servicio	Responsable de Seguridad	Director General
3.1	06/09/2013	Aprobación de Agustín Elizegi	Responsable de Seguridad	Director General
3.2	22/05/2014	Aprobación de Alex Etxeberria	Responsable de Seguridad	Director General
3.3	8/1/2016	Adaptación de los apartados 3.7, 3.8, 3.11 y 3.14 a los cambios introducidos en la versión 3.0 de las Políticas de Seguridad de EJIE	Responsable de Seguridad	Director General
4.0	26/11/2018	Actualización general, alineamiento con RGPD y revisión de requisitos específicos (apartado “políticas específicas”)	Responsable de Seguridad	Director General
4.1	6/5/2020	Se actualiza 3.4 a Se actualiza la información del apartado de “comunicación de incidencias”. Se incluye párrafo sobre el cifrado en el apartado “gestión técnica de cambios”. Se modifica el apartado 2.2 d Se actualiza 2.7.8 Se actualiza 3.9 (último párrafo) Se actualiza 3.11 a	Responsable de Seguridad	Director General
4.2	11/03/2022	Inclusión de cláusulas para la cadena de suministros Actualizacón general de requisitos	Responsable de Seguridad	Director General

Índice

1 Introducción

1.1 Propósito

En toda organización existe información 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 de este documento es establecer el marco normativo en relación a la seguridad de la información para los proveedores de EUSKO JAURLARITZAREN INFORMATIKA ELKARTEA – SOCIEDAD INFORMÁTICA DEL GOBIERNO VASCO, S.A. (en adelante EJIE), describiendo lo que se espera de todo el personal que trabaja para EJIE pero que pertenece a otras empresas proveedoras, y que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos de EJIE en general, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información y sistemas manejados por EJIE.

Para ello, las empresas proveedoras a las que se les remitan estas políticas de seguridad se responsabilizan de informar de ellas a las personas que destinen en EJIE, así como de obtener su compromiso por escrito de que se comprometen a respetar dichas Políticas.

La Política de Seguridad refleja requerimientos legales y éticos, tanto en actuaciones informales de los empleados que trabajan para EJIE pertenecientes a empresas proveedoras, como en la realización de su operativa.

Con dicho propósito, esta política contempla lo establecido en las Políticas de Seguridad de EJIE, y refleja las obligaciones a las que está sujeta EJIE por la legislación vigente, y en particular por el reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

1.2 Ámbito de aplicación

Todas las actividades desarrolladas para EJIE por personal que presta servicios para esta organización pero que pertenece a otras empresas proveedoras, vinculadas a través del correspondiente contrato de provisión de servicios.

El apartado “Políticas Generales de Seguridad para Proveedores” de la presente política será aplicable a cualquier proveedor, independientemente del tipo de servicio proporcionado.

Cada uno de los sub-apartados del apartado “Políticas Específicas de Seguridad para Proveedores” de la presente política será aplicable exclusivamente a aquellos proveedores cuyos servicios proporcionados se correspondan con la naturaleza del servicio indicado en cada caso, tal y como se indica al comienzo del citado apartado.

2 Políticas Generales de Seguridad para Proveedores

2.1 Cumplimiento de la Política General de Seguridad de EJIE

Todo el personal externo que desarrolle labores para EJIE deberá cumplir cumplirla Política General de Seguridad de EJIE, disponible en la web, observando sus directrices y colaborando en su aplicación dentro del ámbito de actuación de cada uno.

Las cesiones o subcontratos quedan en principio prohibidos y en el supuesto de que EJIE los autorice, la empresa subcontratista o cesionaria debidamente autorizada, quedará subrogada en todas las obligaciones y derechos de la subcontratista principal, en lo que se refiere a la parte del contrato cedido o subrogada y por lo tanto, deberá cumplir con la presente Política de Seguridad para empresas proveedoras de EJIE, tal y como queda reflejado en las Condiciones Generales de Contratación (apartado 1.7).

2.2 Prestación de servicios a EJIE

a) Los proveedores sólo podrán desarrollar para EJIE aquellas actividades cubiertas bajo el correspondiente contrato de provisión de servicios. De este modo, se entenderá que todas las actividades desarrolladas para EJIE por personal perteneciente a empresas proveedoras se encuadran en los contratos de provisión de servicios que vinculan a EJIE con estos proveedores.

b) Las actividades desarrolladas por el personal perteneciente a empresas proveedoras se realizarán de acuerdo a lo establecido en el correspondiente contrato de provisión de servicios, así como a las normas y procedimientos establecidos a tal efecto entre EJIE y el proveedor correspondiente.

c) La empresa proveedora proporcionará a EJIE periódicamente la relación de personas, perfiles, funciones y responsabilidades asociados al servicio provisto, e informará puntualmente de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.

d) De acuerdo a lo establecido en las cláusulas asociadas de provisión de servicios, todo el personal externo que desarrolle labores de EJIE deberá cumplir con las políticas de seguridad recogidas en el presente documento. En caso de incumplimiento de cualquiera de estas obligaciones EJIE se reserva el derecho de veto sobre el personal que haya cometido el incumplimiento, así como la adopción de las medidas sancionadoras que se consideren pertinentes en relación a la empresa contratada y que se aplicarán en base a la cláusula de penalización establecida en el Pliego de Condiciones Particulares, y que pueden llegar a la resolución de los contratos que tenga vigentes con dicha empresa. Asimismo, EJIE se reserva la potestad de incluir los incidentes de seguridad en los certificados de ejecución de servicios que las empresas adjudicatarias pudieran solicitar.

e) La empresa proveedora deberá asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio provisto, tanto a nivel específico en las materias correspondientes a la actividad asociada a la prestación del servicio como de manera transversal en materia de seguridad de la información, para lo cual deberá asegurarse, al menos, de que todo el personal asociado al servicio conoce y se compromete a cumplir las presentes Políticas de Seguridad.

f) Cualquier tipo de intercambio de información que se produzca entre EJIE y las empresas proveedoras se entenderá que ha sido realizado dentro del marco establecido por el contrato de provisión de servicios correspondiente, de modo que dicha información no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados a dicho contrato.

g) El área de seguridad Informática centraliza los esfuerzos globales de protección de los activos de EJIE, a fin asegurar el correcto funcionamiento de las tecnologías de la información que soportan los procesos de la organización.

h) De forma genérica, los activos incluyen toda forma de información, además de las personas y la tecnología que soportan los procesos de información.

2.3 Confidencialidad de la Información

a) El personal externo que tenga acceso a información de EJIE deberá considerar que dicha información, por defecto, tiene el carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella información de EJIE a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos a tal efecto por EJIE.

b) Se evitará la revelación, modificación, destrucción o mal uso de la información cualquiera que sea el soporte en que se encuentre contenida.

c) Se guardará por tiempo indefinido la máxima reserva y no se emitirá al exterior, información confidencial, salvo que esté debidamente autorizado.

d) Se minimizará el número de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera del alcance de terceros.

e) En relación a la utilización de agendas de contactos, de las herramientas ofimáticas dispuestas por EJIE, el personal únicamente introducirá datos personales como nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, y teléfono.

f) Ningún colaborador en proyectos, trabajos puntuales, etc., deberá poseer, para usos no propios de su responsabilidad, ningún material o información propia o confiada a EJIE.

g) 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. Asimismo, el empleado 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 con EJIE de su empresa. La utilización continuada de la información en cualquier formato o soporte distinta a la pactada y sin conocimiento de EJIE no supondrá, en ningún caso, una modificación de este punto.

h) Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para EJIE.

i) 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.

En el ámbito del tratamiento de datos personales se deberá deberán cumplir las siguientes normas de actuación, además de las consideraciones ya mencionadas:

j) El personal sólo podrá crear ficheros temporales que contengan datos de carácter personal cuando sea necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de los puestos de trabajo de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

k) No se albergarán datos de carácter personal en las unidades locales de disco de los puestos de trabajo. No se albergarán datos de carácter personal en las unidades locales de disco de los puestos de trabajo.

l) La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicada dicha información, únicamente podrá ser autorizada por el responsable del tratamiento y se realizará según el procedimiento definido.

m) Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar de acceso restringido al personal autorizado.

2.4 Propiedad intelectual

a) Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

b) Los empleados únicamente podrán utilizar material autorizado por EJIE para el desarrollo de sus funciones.

c) Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia en los Sistemas de Información de EJIE.

d) 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.

e) EJIE únicamente autorizará el uso de material producido por él mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

2.5 Intercambio de información

a) Ninguna persona debe ocultar o manipular su identidad bajo ninguna circunstancia.

b) La distribución de información ya sea en formato digital o papel se realizará mediante los recursos determinados en el contrato de provisión de servicios para tal cometido y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato. EJIE se reserva, en función del riesgo identificado, la implementación de medidas de control, registro y auditoría sobre estos recursos de difusión.

c) En relación al intercambio de información dentro del marco del contrato de provisión de servicios, se considerarán no autorizadas las siguientes actividades:

1. Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual.
2. Transmisión o recepción de toda clase de material pornográfico, mensajes o de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
3. Transferencia de información a terceras partes no autorizadas de material de la Organización o material que es de alguna u otra manera confidencial.
4. Transmisión o recepción de información que infrinja la normativa en vigor en materia de protección de protección de Datos de Carácter Personal o directrices de EJIE.
5. Transmisión o recepción de juegos y/o aplicaciones no relacionadas con el negocio.
6. Participación en actividades de Internet como grupos de noticias, juegos u otras que no estén directamente relacionadas con el servicio.
7. Todas las actividades que puedan dañar la buena reputación de EJIE están prohibidas en Internet y en cualquier otro lugar.

d) Toda salida de información que contenga datos de carácter personal (tanto en soportes informáticos como en papel o por correo electrónico) sólo podrá ser realizada por personal autorizado y con el debido permiso, cumpliendo el procedimiento definido.

e) Si el tratamiento de datos de carácter personal se llevase a cabo fuera de los locales donde están ubicados los datos, dicho tratamiento deberá ser autorizado expresamente por el responsable del tratamiento y, en todo caso, deberá garantizarse el nivel de seguridad necesario.

f) 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.

2.6 Uso apropiado de los recursos

a) El proveedor se compromete a informar periódicamente a EJIE de los activos con los que proporciona el servicio.

b) El proveedor se compromete a utilizar los recursos dispuestos para la provisión del servicio de acuerdo con las condiciones para las que fueron diseñados e implantados.

c) Los recursos que EJIE 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 proporcionados. EJIE se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

d) Cualquier fichero introducido en la red de EJIE o en cualquier equipo conectado a ella 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 software malicioso.

e) Se deberán restituir a EJIE todos los activos físicos y destruir o restituir a EJIE todos los activos de información, sin retraso injustificado, después de la finalización del contrato.

f) Se prohíbe expresamente:

1. El uso de los recursos proporcionados por EJIE para actividades no relacionadas con el propósito del servicio.
2. La conexión a la red de producción de EJIE de equipos y/o aplicaciones que no estén especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de EJIE o bajo supervisión de EJIE.
3. Introducir en los Sistemas de Información o la Red de EJIE contenidos obscenos, amenazadores, inmorales u ofensivos.
4. Introducir voluntariamente en la red de EJIE cualquier tipo de malware (programas, macros, applets, controles ActiveX, etc.), 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. Todo el personal con acceso a la red de EJIE 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.
5. Intentar obtener sin autorización explícita otros derechos o accesos distintos a aquellos que EJIE les haya asignado.
6. Intentar acceder sin autorización explícita a áreas restringidas de los Sistemas de Información de EJIE.
7. Intentar distorsionar o falsear los registros “log” de los Sistemas de Información de EJIE.

8. Intentar descifrar sin autorización explícita las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de EJIE.
9. Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros Usuarios, ni dañar o alterar los Recursos Informáticos de EJIE.
10. Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos responsabilidad de EJIE (Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del Código Penal).
11. Albergar Datos de Carácter Personal de EJIE o cuyo tratamiento haya sido encargado a EJIE en las unidades locales de disco de los puestos de usuario.

2.7 Responsabilidades del usuario

a) Los proveedores de servicios deberán asegurarse de que todo el personal que desarrolla labores para EJIE respete los siguientes principios básicos dentro de su actividad informática:

   1. Cada persona con acceso a información de EJIE es responsable de la actividad desarrollada por su identificador de usuario y todo lo que de él se derive. Por lo tanto, es imprescindible que cada persona mantenga bajo control los sistemas de autenticación asociados a su identificador de usuario, garantizando que la clave asociada sea únicamente conocida por el propio usuario, no debiendo revelarse al resto del personal bajo ningún concepto.
   2. Los usuarios no deberán utilizar ningún identificador de otro usuario, aunque dispongan de la autorización del propietario.
   3. Los usuarios conocen y aplican los requisitos y procedimientos existentes en torno a la información manejada.

b) Cualquier persona con acceso a información responsabilidad de EJIE deberá seguir las siguientes directivas en relación a la gestión de las contraseñas:

   1. Seleccionar contraseñas de calidad.
   2. Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
   3. Cambiar las contraseñas periódicamente y evitar reutilizar o reciclar viejas contraseñas.
   4. Cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión (“login”).
   5. Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
   6. Notificar cualquier incidente de seguridad relacionado con sus contraseñas como pérdida, robo o indicio de pérdida de confidencialidad.

c) Cualquier persona con acceso a información responsabilidad de EJIE deberá velar por que los equipos queden protegidos cuando vayan a quedar desatendidos.

d) Cualquier persona con acceso a información responsabilidad de EJIE deberá respetar al menos las siguientes políticas de escritorio limpio, con el fin de proteger los documentos en papel y dispositivos de almacenamiento removibles y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:

   1. Almacenar bajo llave los documentos en papel y los medios informáticos con información responsabilidad de EJIE en mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

2. No dejar desatendidos los equipos asignados a funciones críticas de EJIE, y bloquear su acceso cuando sea estrictamente necesario.
3. Proteger, siempre que se utilice información responsabilidad de EJIE, tanto los puntos de recepción y envío de información (correo postal, máquinas de scanner) como los equipos de duplicado (fotocopiadora, scanner). La reproducción o envío de información con este tipo de dispositivos quedará bajo la responsabilidad del usuario.
4. Retirar, sin retraso injustificado, cualquier información confidencial que sea responsabilidad de EJIE, una vez impresa.
5. Los listados con datos de carácter personal o información confidencial responsabilidad de EJIE deberán almacenarse en lugar seguro al que únicamente tengan acceso personal autorizado.
6. Los listados con datos de carácter personal o información confidencial responsabilidad de EJIE deberán eliminarse de manera segura una vez no sean necesarios.
7. Las personas con acceso a sistemas y/o información de EJIE nunca deberán sin autorización explícita, realizar pruebas para detectar y/o utilizar una supuesta debilidad o incidente de seguridad, en caso de identificarse incidentes o debilidades que puedan suponerse relacionadas con la seguridad de la información.
8. Ninguna persona con acceso a sistemas y/o información de EJIE intentará sin autorización explícita por ningún medio transgredir el sistema de seguridad y las autorizaciones. 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 o sea necesario para resolver alguna incidencia.
9. Ningún dato de carácter personal responsabilidad de EJIE será almacenado en equipos de usuario ni en soportes de información.

e) Todo el personal que acceda a la información y/o los sistemas responsabilidad de EJIE deberá seguir las siguientes normas de actuación:

1. Proteger la información confidencial perteneciente o cedida por terceros a EJIE de toda revelación no autorizada, modificación, destrucción o uso incorrecto, ya sea accidental o no.
2. Proteger todos los sistemas de información y redes de telecomunicaciones contra accesos o usos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.
3. Contar con la autorización necesaria para obtener el acceso a los sistemas de información y/o la información accedidos.
4. Conocer, aceptar y cumplir las presentes políticas antes de acceder a la información y/o los sistemas de EJIE.

f) Aquellos proveedores que tengan acceso habitual a la sede de EJIE deberán custodiar adecuadamente la tarjeta de acceso. Fuera de las instalaciones de EJIE no llevarán dicha tarjeta a la vista.

2.8 Equipos de usuario

a) Los proveedores de servicios deberán asegurarse de que todo el equipamiento informático de usuario utilizado para acceder a información responsabilidad de EJIE cumple las siguientes políticas:

1. Cuando se desatienda un puesto durante un periodo corto de tiempo el sistema deberá activar su bloqueo.

2. Ningún equipo de usuario dispondrá de herramientas que puedan transgredir el sistema de seguridad y las autorizaciones dentro de los sistemas de la organización salvo que sea necesario para la provisión del servicio.
3. Los equipos de usuario se mantienen de acuerdo a las especificaciones del fabricante.
4. Todos los equipos de usuario están adecuadamente protegidos frente a malware:
    - El software antivirus se deberá instalar y usar en todos los ordenadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
    - Se mantendrán al día con las últimas actualizaciones de seguridad disponibles.
    - El software antivirus deberá estar siempre habilitado. Se establecerá una actualización automática de los ficheros de definición de virus.

b) Se velará especialmente por la seguridad de todos los equipos móviles de usuario que contengan información responsabilidad de EJIE o permitan acceder a ella de algún modo:

1. Verificando que no incluyen más información responsabilidad de EJIE que la que sea estrictamente necesaria.
2. Garantizando que se aplican controles de acceso a dicha información.
3. Minimizando los accesos a dicha información en presencia de personas ajenas al servicio provisto a EJIE.
4. Transportando los equipos en fundas, maletines o equipamiento similar que incorpore la apropiada protección frente a golpes.
5. Tomando especiales precauciones en el exterior de las dependencias de EJIE para evitar la visión accidental por parte de terceras personas de la información responsabilidad de EJIE.

2.9 Gestión de equipamiento “hardware”

a) Los proveedores de servicios deberán asegurarse de que todos los equipos para la prestación de servicios, independientemente del tipo que sean, se gestionan apropiadamente. Los proveedores de servicios deberán asegurarse de que todos los equipos para la prestación de servicios, independientemente del tipo que sean, se gestionan apropiadamente. Para ello deberán cumplir las siguientes políticas:

1. El proveedor deberá mantener una relación actualizada de equipos y usuarios de dichos activos, o responsables asociados en caso de que los activos no sean de uso unipersonal. Dicha relación podrá ser requerida por EJIE en cualquier momento.
2. Siempre que un proveedor quiera reasignar algún equipo que haya contenido información responsabilidad de EJIE llevar a cabo los procedimientos de borrado seguro necesarios de forma previa a su reasignación.
3. En caso de que un proveedor quiera proceder a dar de baja de la relación de equipos de EJIE recibidos alguno de ellos, siempre deberá devolver a EJIE dicho activo, para que EJIE pueda tratar dicha baja de forma apropiada.
4. En caso de que un proveedor cese en la prestación del servicio, deberá devolver a EJIE toda la relación de equipos recibidos, tal y como establecen los correspondientes contratos de prestación de servicios. Sólo en el caso de activos de información el proveedor podrá proceder a su eliminación segura, en cuyo caso deberá notificar a EJIE dicha eliminación.

2.10 Comunicación de incidencias

a) La persona que detecte cualquier incidencia deberá ponerse en contacto con el servicio del centro de atención al usuario (CAU) de EJIE en caso de que detecte cualquier incidencia relacionada con la información, recursos de EJIE o los servicios proporcionados a EJIE.
   - Directamente al CAU si no hay impacto en el servicio (no requiere acción urgente)
   - A incidencias graves del CAU si hay impacto en el servicio y es necesario realizar acción urgente

b) Cualquier usuario podrá trasladar al Responsable de Seguridad de EJIE sugerencias, debilidades, vulnerabilidades y/o situaciones de riesgo que pueda tener relación con la seguridad de la información y las directrices contempladas en las presentes políticas de las que tenga conocimiento.

c) Se deberá notificar al CAU cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o soportes que contengan información, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos, etc.

d) El centro de atención al usuario (CAU) centraliza la recogida, análisis y gestión de las incidencias recibidas.

e) Si no se tuviera acceso al CAU, se deberán utilizar los cauces de comunicación establecidos dentro del propio servicio, de modo que sea el interlocutor de EJIE quien se ponga en contacto con el CAU.

2.10.1 Los medios de contacto son los siguientes:

Notificación de incidencias

- CAU (Centro de Atención de Usuarios):
  - Teléfono 945016440
  - Correo electrónico: cau-ejie@ejie.eus
- CAU – Gestión de incidencias graves:
  - Teléfono: 688672990
  - Correo electrónico: incidencias@ejie.eus

Notificación al responsable de seguridad

Correo electrónico: seguridad@ejie.eus

En relación con la protección de datos:

- Persona delegada: dpo@ejie.eus
- Ejercicio de derechos: lopd-ejie@ejie.eus

2.11 Gestión de contingencias

a) El servicio cuenta con un plan que permite su prestación aun en caso de contingencias.

b) El plan anterior ha sido desarrollado en función de los eventos capaces de causar interrupciones en el servicio y su probabilidad de ocurrencia.

c) El proveedor puede demostrar la viabilidad del plan de contingencias existente.

3 Políticas Específicas de Seguridad para Proveedores

3.1 Aplicabilidad de las Políticas Específicas de Seguridad para Proveedores

Todos los proveedores deberán cumplir, además de las políticas generales de seguridad para proveedores, las políticas específicas de seguridad recogidas en el presente apartado que les correspondan en cada caso, en función de las características del servicio prestado a EJIE.

Las tipologías de servicio que se contemplan son las que se indican a continuación.

- **Lugar de ejecución del servicio**: en función del lugar principal en el que se desarrollen los servicios se distinguen dos casos:
  - **EJIE**: El proveedor presta el servicio principalmente desde la propia sede de EJIE.
  - **Remoto**: El proveedor presta el servicio principalmente desde sus propias dependencias, pese a que se puedan llevar a cabo actividades puntuales en la sede de EJIE.
- **Propiedad de las infraestructuras TIC utilizadas**: en función de quién sea el propietario de las principales infraestructuras TIC (comunicaciones, equipos de usuario, software) utilizadas para prestar el servicio se distinguen dos casos:
  - **EJIE**: La mayor parte de las infraestructuras TIC utilizadas para prestar el servicio son propiedad de EJIE, siendo las proporcionadas por el proveedor una minoría o complementarias.
  - **Proveedor**: La mayor parte de las infraestructuras TIC utilizadas para prestar el servicio son propiedad del proveedor del servicio, siendo poco significativas dentro del servicio las proporcionadas por EJIE.
- **Nivel de acceso** a los sistemas de EJIE: en función del nivel de acceso a los sistemas de información de EJIE se distinguen tres casos:
  - **Sin acceso**: el servicio provisto no requiere de la utilización de los sistemas de información de EJIE, de modo que el personal que presta el servicio no dispone de cuentas de usuario en dichos sistemas.
  - **Con acceso de nivel de usuario**: el servicio provisto requiere de la utilización de los sistemas de información de EJIE, de modo que el personal que presta el servicio dispone de cuentas de usuario que les permiten acceder a alguno de dichos sistemas con privilegios habituales.
  - **Con acceso privilegiado**: el servicio provisto requiere de la capacidad de acceso privilegiado a los sistemas de información de EJIE, con capacidad para administrar dichos sistemas y/o los datos de producción que procesan.
- **Gestión de tecnologías** de EJIE: En función de si el proveedor gestiona las tecnologías y plataformas se distinguen dos casos:
  - **Sí**: el proveedor gestiona credenciales de acceso a tecnologías de EJIE, de modo que puede desempeñar roles de administración y/o privilegiados en dichas tecnologías y plataformas.
  - **No**: el proveedor accede a tecnologías o plataformas de EJIE en modo usuario, para lo que debe solicitar credenciales a EJIE.

En función de cada una de las cuatro categorías en las que se encuadre cada servicio, el proveedor deberá cumplir, adicionalmente a las políticas generales de seguridad, las políticas específicas recogidas en los apartados que se indican en la siguiente tabla:

	Lugar		Infraestructura		Acceso			Gestión de tecnologías	
	EJIE	Remoto	EJIE	Proveedor	Privilegiado	Usuario	Sin Acceso	Sí	No
Selección de personal	n.a.	n.a.	SÍ	NO	SÍ	SÍ	NO	SÍ	NO
Auditoría de seguridad	n.a.	n.a.	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO
Seguridad física	NO	SÍ	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Gestión de activos	n.a.	n.a.	SÍ	SÍ	n.a.	n.a.	n.a.	SÍ	NO
Arquitectura seguridad	NO	SÍ	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Seguridad sistemas	n.a.	n.a.	NO	SÍ	n.a.	n.a.	n.a.	Sí	n.a.
Seguridad red	NO	SÍ	n.a.	SÍ	SÍ	SÍ	NO	n.a.	n.a.
Trazabilidad de uso de los sistemas	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	SÍ	NO
Control y gestión de identidades y accesos	n.a.	n.a.	n.a.	n.a.	SÍ	SÍ	NO	n.a.	n.a.
Gestión de cambios	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	SÍ	NO
Seguridad en desarrollo	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	SÍ **(*)**	NO

(*) Sólo si existen tareas de desarrollo

SI: la responsabilidad del control recae sobre la empresa proveedora que tenga esa característica en el servicio

NO: la responsabilidad del control no recae sobre la empresa proveedora que tenga esa característica en el servicio

n.a.: esa característica en el servicio no es relevante para la determinación de la responsabilidad de la empresa proveedora en dicho control

El detalle de si deben confluir varias de las características o si, por el contrario, es suficiente con el cumplimiento de una de ellas, se establece en el primer párrafo de cada política específica indicadas a continuación.

3.2 Selección de personal

Todos los proveedores de servicios, independientemente del lugar en el que se preste, que utilicen infraestructura de EJIE o tengan acceso a los sistemas de información de EJIE o sean gestores de tecnologías, deberán cumplir las siguientes políticas de selección de personal:

a) El proveedor deberá verificar los antecedentes profesionales del personal asignado al servicio, garantizando a EJIE que en el pasado no ha sido sancionado por mala praxis profesional ni se ha visto envuelto en incidentes relacionados con la confidencialidad de la información tratada que le hayan supuesto algún tipo de sanción.

b) El proveedor deberá garantizar a EJIE la posibilidad de baja inmediata del personal asignado al servicio de cualquier persona en relación con la cual EJIE desee ejercer el derecho de veto, de acuerdo a los condicionantes establecidos en el apartado 3.2 – Prestación de servicios a EJIE.

3.3 Auditoría de seguridad

Todos los proveedores que utilicen infraestructura propia o de EJIE para la provisión del servicio o tengan acceso a los sistemas de información de EJIE o sean gestores de tecnologías, independientemente del lugar en el que se preste el servicio, deberán cumplir las siguientes políticas de auditoría de seguridad:

a) El proveedor deberá permitir que EJIE lleve a cabo al menos una auditoría de seguridad del servicio al año, colaborando con el equipo auditor y facilitando todas las evidencias y registros le sean requeridos.

b) El alcance y profundidad de cada auditoría será establecido expresamente por EJIE en cada caso. Las auditorías se llevarán a cabo siguiendo la planificación que se acuerde en cada caso con el proveedor del servicio.

c) EJIE se reserva el derecho de realizar auditorías extraordinarias adicionales, siempre que se den causas específicas que lo justifiquen.

3.4 Seguridad física

Todos los proveedores que presten servicio desde sus propias instalaciones deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad física:

a) La sede deberá ser una sede cerrada y deberá contar con algún sistema de control de acceso que garantice la prevención ante robo, destrucción o interrupción.

b) Existirá algún tipo de control de las visitas, al menos en áreas de acceso público y/o de carga y descarga.

c) La sede deberá contar, al menos, con sistemas de detección de incendios, y deberá estar construida de modo que ofrezca una suficiente resistencia frente a inundaciones.

d) Si se mantiene algún tipo de copia de información responsabilidad de EJIE, los sistemas que alberguen y/o procesen dicha información deberán estar ubicados en un área especialmente protegida, que incluya al menos las siguientes medidas de seguridad:

    1. El área especialmente protegida deberá tener un sistema de control de acceso independiente al de la sede.

2. Se limitará el acceso al personal externo a las áreas especialmente protegidas. Este acceso se asignará únicamente cuando sea necesario y se encuentre autorizado, y siempre bajo la vigilancia de personal autorizado.
3. Se mantendrá un registro de todos los accesos de personas ajenas.
4. El personal externo no podrá permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión.
5. El consumo de alimentos o bebidas en estas áreas especialmente protegidas estará prohibido.
6. Los sistemas ubicados en estas áreas deberán contar con algún tipo de protección frente a fallos de alimentación.

3.5 Gestión de activos

Todos los proveedores que presten servicios mediante infraestructura TIC o tecnologías (software, aplicaciones, etc.), independientemente de que estas sean propiedad de EJIE o del proveedor, deberán garantizar que se cumplen, al menos, las siguientes políticas de gestión de activos:

a) El proveedor deberá contar con un registro de activos actualizado en el que se puedan identificar los activos utilizados para la prestación del servicio.

b) Todos los activos utilizados para la prestación del servicio deberán tener un responsable, que se deberá asegurar de que dichos activos incorporan las medidas de seguridad mínimas establecidas por la organización, y que al menos deben ser las especificadas en la presente política.

c) El proveedor deberá notificar a EJIE las bajas de los activos utilizados para la prestación del servicio.

d) Siempre que un activo haya contenido información responsabilidad de EJIE, el proveedor deberá llevar a cabo las bajas de activos garantizando la eliminación segura de dicha información, aplicando funciones de borrado seguro o destruyendo físicamente el activo, para que la información que haya contenido no pueda ser recuperable. Si se requiere el proveedor aportará a EJIE certificado que confirme la eliminación segura de estos activos de información.

3.6 Arquitectura de seguridad

Todos los proveedores que presten servicio desde sus instalaciones deberán garantizar que se cumplen, al menos, los siguientes requisitos de arquitectura de seguridad::

a) Siempre que el proveedor de servicios realice trabajos de desarrollo y/o pruebas de aplicaciones para EJIE o con datos responsabilidad de EJIE, los entornos con los que se lleven a cabo dichas actividades deberán estar aislados entre sí y también aislados de los entornos de producción en los que se albergue o procese información responsabilidad de EJIE.

b) Todos los accesos a los sistemas de información que alberguen o procesen información responsabilidad de EJIE deberán estar protegidos, al menos, por un cortafuegos, que limite la capacidad de conexión a ellos.

c) Los sistemas de información que alberguen o procesen información responsabilidad de EJIE especialmente sensible deberán estar aislados del resto.

d) Los sistemas de información utilizados para la prestación de servicios a EJIE deberán contar con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

3.7 Seguridad de sistemas

Todos los proveedores de servicios que se presten mediante el uso de infraestructura TIC del proveedor o que gestionen tecnologías, deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad de sistemas:

a) Los sistemas de información que alberguen o traten información responsabilidad de EJIE deberán registrar los eventos más significativos en torno a su funcionamiento. Estos registros de actividad estarán contemplados dentro de la política de copias de seguridad de la organización.

b) Los relojes de los sistemas del proveedor que procesen o alberguen información responsabilidad de EJIE estarán sincronizados entre sí y con la hora oficial.

c) El proveedor del servicio garantizará que la capacidad de los sistemas de información que guarden o traten información responsabilidad de EJIE se gestiona adecuadamente, evitando potenciales paradas o malos funcionamientos de dichos sistemas por saturación de recursos.

d) Los sistemas de información que alberguen o procesen información responsabilidad de EJIE estarán adecuadamente protegidos frente a software malicioso, aplicando las siguientes precauciones:

   1. Se mantendrán los sistemas al día con las últimas actualizaciones de seguridad disponibles, en los entornos de prueba, desarrollo y producción.
   2. El software antivirus se deberá instalar y usar en todos los servidores y ordenadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
   3. El software antivirus deberá estar siempre habilitado. Se establecerá una actualización automática, de los ficheros de definición de virus tanto en los ordenadores personales como servidores, así como de bloqueo frente a la detección de virus informáticos.

e) El proveedor establecerá una política de copias de seguridad que garantice la salvaguarda de cualquier dato o información relevante para el servicio prestado, con una periodicidad máxima mensual.

f) Siempre que se utilice el correo electrónico en relación con el servicio prestado, el proveedor deberá respetar las siguientes premisas:

   1. No se permitirá la transmisión vía correo electrónico de información confidencial de EJIE salvo que la comunicación electrónica esté cifrada y el envío este expresamente permitido.
   2. No se permitirá 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.

g) Siempre que para la prestación del servicio se haga uso del correo electrónico de EJIE se deberán respetar, al menos, los siguientes principios:

   1. Se considerará al correo electrónico como una herramienta más de trabajo proporcionada con el fin exclusivo del servicio contratado. Esta consideración facultará a EJIE 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 de las personas y su derecho a la intimidad.
   2. El sistema de correo electrónico de EJIE no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares.

3. Los usuarios no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples usuarios).

h) El acceso a los sistemas de información que alberguen o procesen información responsabilidad de EJIE deberá realizarse siempre de forma autenticada, al menos mediante la utilización de un identificador usuario unipersonal y una contraseña asociada. Esta obligación deberá ser cumplida tanto por los usuarios "normales" como especialmente por los usuarios con privilegios de administración de dichos sistemas de información.

i) Los sistemas de información que alberguen o procesen información responsabilidad de EJIE deberán contar con sistemas de control de acceso que limiten el acceso a dicha información exclusivamente al personal del servicio.

j) Las sesiones de acceso a los sistemas de información que alberguen o procesen información responsabilidad de EJIE deberán bloquearse automáticamente tras un cierto tiempo de inactividad de los usuarios.

k) Siempre que se haga uso de software facilitado por EJIE se deberán atender las siguientes políticas:

1. Todo el personal que acceda a los Sistemas de Información de EJIE debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.
2. Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.
3. Se prohíbe el uso de software no validado por EJIE.
4. También está prohibido desinstalar cualquiera de los programas instalados por EJIE.

3.8 Seguridad de red

Todos los proveedores de servicios que accedan a sistemas de información de EJIE desde sus propias instalaciones y/o utilizando su propia infraestructura, deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad de red:

a) Las redes a través de las que circule la información responsabilidad de EJIE deberán estar adecuadamente gestionadas y controladas, asegurándose de que no existen accesos no controlados ni conexiones cuyos riesgos no estén apropiadamente gestionados por el proveedor.

b) Los servicios disponibles en las redes a través de las que circule la información responsabilidad de EJIE deberán limitarse en la medida de lo posible.

c) Las redes que permitan el acceso a la infraestructura TIC de EJIE deberán estar apropiadamente protegidas, debiéndose cumplir las siguientes premisas:

1. El acceso de usuarios remotos a la red de EJIE estará sujeto al cumplimiento de procedimientos de autenticación previa y validación del acceso.
2. Estas conexiones se realizarán por tiempo limitado y mediante la utilización de redes privadas virtuales o líneas dedicadas.
3. En estas conexiones no se permitirá ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas.

d) El acceso a las redes a través de las que circule la información responsabilidad de EJIE deberá estar limitado.

e) Todos los equipos conectados a las redes a través de las que circule la información responsabilidad de EJIE deberán estar apropiadamente identificados, de modo que los tráficos de red puedan ser identificables.

f) El teletrabajo, considerado como el acceso a la red corporativa desde el exterior, se regula mediante la aplicación de las siguientes políticas:

1. Se establecerán las medidas necesarias para la conexión segura a la red corporativa.
2. Se establecerán sistemas de monitorización y auditoría de seguridad para las conexiones establecidas.
3. Se controlará la revocación de derechos de acceso y devolución de equipamiento tras la finalización del periodo de necesidad del mismo.

Siempre que se haga uso del acceso a Internet proporcionado por EJIE se deberán respetar, adicionalmente, las siguientes políticas:

g) 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 objetivo de negocio de EJIE o al cumplimiento de su trabajo diario.

h) El acceso a Internet desde la red corporativa se restringe por medio de dispositivos de control incorporado en la misma. La utilización de otros medios de conexión deberá ser previamente validada y estará sujeta a las anteriores consideraciones sobre el uso de Internet.

i) Los usuarios no deberán usar el nombre, símbolo, logotipo o símbolos similares al de EJIE en ningún elemento de Internet (correo electrónico, páginas web, etc.) no justificado por actividades estrictamente laborales.

j) Únicamente se permitirá la transferencia de datos de o hacia Internet cuando estén relacionadas con actividades del negocio. La transferencia de ficheros no relativa a estas actividades (por ejemplo, la descarga de juegos de ordenador, ficheros de sonido y contenidos multimedia, etc.) estarán prohibidas.

Cualquier activo o servicio proporcionado por EJIE se utilizará sólo en el ámbito profesional para proporcionar los servicios contratados.

3.9 Trazabilidad de uso de los sistemas

Todos los proveedores de servicios relacionados con la gestión de tecnologías de EJIE, deberán garantizar que se cumplen, al menos, las siguientes políticas de trazabilidad de uso de los sistemas:

a) Se registrarán los accesos privilegiados conservándose dichos registros de acuerdo a la política de copias de seguridad de la organización.

b) Se registra la actividad de los sistemas utilizados para llevar a cabo dicho acceso privilegiado, conservándose dichos registros de acuerdo a la política de copias de seguridad de la organización.

c) Los errores y fallos registrados en la actividad de los sistemas se analizan, adoptándose las medidas necesarias para su subsanación.

3.10 Control y gestión de identidades y accesos

Todos los proveedores de servicios con acceso a sistemas de información de EJIE, deberán garantizar que se cumplen, al menos, las siguientes políticas de control y gestión de identidades y accesos:

a) Todos los usuarios con acceso a un sistema de información dispondrán de una autorización de acceso unipersonal compuesta de identificador de usuario y contraseña. Esta obligación deberá ser cumplida tanto por todos usuarios, sean éstos privilegiados o no.

b) Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

c) Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

d) 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.

e) La longitud mínima de la contraseña deberá ser de 6 caracteres.

f) Las contraseñas estarán constituidas por combinación de caracteres alfabéticos y numéricos.

g) Es recomendable utilizar las siguientes directrices para la selección de contraseñas:

   1. No usar palabras conocidas, ni palabras que se puedan asociar con uno mismo, por ejemplo, el nombre.
   2. La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos, etc.
   3. La clave debería ser algo prácticamente imposible de adivinar. Pero al mismo tiempo debería ser fácilmente recordada por el usuario. Un buen ejemplo es usar el acrónimo de alguna frase o expresión.
   4. La clave debería contener al menos un carácter numérico y uno alfabético.
   5. No se debería utilizar el identificador de usuario como parte de la clave secreta.

h) El proveedor deberá garantizar que periódicamente se constata que sólo tienen acceso a la información responsabilidad de EJIE el personal debidamente autorizado para ello.

i) Ningún usuario recibirá un identificador de acceso a los sistemas de EJIE hasta que no acepte formalmente la Política de Seguridad vigente.

j) Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

k) En caso de que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

l) En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 90 días. En caso contrario, se le podrá denegar el acceso y deberá contactar con el Centro de Atención a Usuarios para la obtención de una nueva.

m) Los accesos autorizados temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

n) En relación a datos de carácter personal, exclusivamente el personal autorizado para ello podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del tratamiento.

o) Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña y contactar con el Centro de Atención a Usuarios para notificar la incidencia.

3.11 Gestión de cambios

Todos los proveedores de servicios que sean gestores de tecnologías / infraestructura,deberán garantizar que se cumplen, al menos, las siguientes políticas de gestión de cambios:

a) Todos los cambios en la infraestructura TIC deberán estar controlados y autorizados, garantizándose que no forma parte de la infraestructura TIC ningún componente no controlado.

b) Se deberá verificar que todos los nuevos componentes introducidos en la infraestructura TIC del proveedor utilizada para la prestación del servicio funcionan adecuadamente y cumplen los propósitos para los que fueron incorporados.

c) Todos los cambios que se lleven a cabo se deberán realizar siguiendo un procedimiento formalmente establecido y documentado, que garantice que se siguen los pasos apropiados para realizar el cambio.

d) El procedimiento de gestión de cambios deberá garantizar que se minimizan los cambios sobre los componentes críticos, limitándose a los estrictamente imprescindibles.

e) Se deberán verificar todos los cambios sobre los componentes críticos, para comprobar que no se producen efectos adversos colaterales o no previstos sobre el funcionamiento de dichos componentes o sobre su seguridad.

f) Los proveedores deberán analizar las vulnerabilidades técnicas que presenten las infraestructuras utilizadas para la prestación del servicio, informando a EJIE de todas aquellas asociadas a los componentes críticos, con el fin de gestionar conjuntamente dichas vulnerabilidades.

g) Se deben utilizar algoritmos y protocolos de cifrado y "resumen" ("hash") que no sean vulnerables. Se utilizará como referencia la guía CCN-STIC 807 del Centro Criptológico Nacional como referencia.

3.12 Seguridad en desarrollo

Todos los proveedores de servicios que realicen actividades de desarrollo de aplicativos deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad en dicha actividad:

a) Todo el proceso de desarrollo de software externalizado será controlado y supervisado por EJIE, y se desarrollará de acuerdo con un proceso formal que determine las reglas a seguir.

b) Se incorporarán mecanismos de identificación, autentificación, control de acceso, auditoría e integridad en todo el ciclo de vida de diseño, desarrollo, implementación y operación de los aplicativos.

c) Las especificaciones de los aplicativos deberán contener expresamente los requisitos de seguridad a cubrir en cada caso.

d) Las aplicaciones que se desarrollen deberán incorporar validaciones de los datos de entrada que verifiquen que los datos son correctos y apropiados y que eviten la introducción de código ejecutable.

e) Los procesos internos desarrollados por las aplicaciones deberán incorporar todas las validaciones necesarias para garantizar que no se producen corrupciones de la información.

f) Siempre que sea necesario se deberán incorporar funciones de autenticación y control de integridad en las comunicaciones entre los diferentes componentes de las aplicaciones.

g) Se deberá limitar la información de salida ofrecida por las aplicaciones, garantizando que sólo se ofrece aquella pertinente y necesaria.

h) El acceso al código fuente de los aplicativos deberá estar limitado al personal del servicio.

i) Durante las fases de desarrollo y pruebas se llevarán a cabo pruebas específicas de las funcionalidades de seguridad.

j) En el entorno de pruebas sólo se utilizarán datos reales cuando hayan sido apropiadamente disociados o siempre que se pueda garantizar que las medidas de seguridad aplicadas sean equivalentes a las existentes en el entorno de producción.

k) Durante las pruebas de los aplicativos se verificará que no existen canales de fuga de información no controlados, y que por los canales establecidos sólo se ofrece la información prevista.

l) Sólo se transferirán al entorno de producción aquellos aplicativos que hayan sido expresamente aprobados.

4 Requisitos de seguridad para la externalización

EJIE establece distintos requerimientos a cumplir por parte del proveedor descritos en el documento **"Normativa para empresas proveedoras – Anexo I Infraestructura TIC / Seguridad física y del entorno".** Esta normativa tiene por objeto concretar la infraestructura utilizada para la prestación del servicio, indicar de manera detallada los controles obligatorios y otros elementos de los que se dota el proveedor para garantizar la seguridad física y del entorno. **El citado documento será de obligado cumplimiento en aquellos expedientes en los que se haya incluido como anexo**, constituyendo norma de referencia para las auditorías de cumplimiento.

5 Seguimiento y control

a) 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, EJIE 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.

b) 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.

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

6 Actualización de las Políticas de Seguridad

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas aportaciones legales en la materia, EJIE se reserva el derecho a modificar estas políticas cuando sea necesario. Los cambios realizados en estas políticas 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 las políticas de seguridad más recientes de EJIE por parte de su personal.