PURPLE BLOB.

NEW CHALLENGES,
SMART SOLUTIONS.

www.purpleblob.net

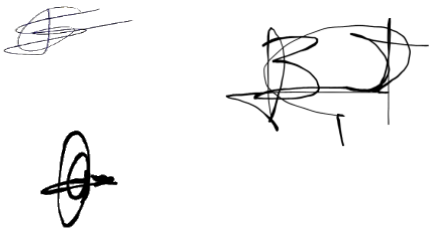
Política de Seguridad de la Información (PSI)

En ámbito NIS2 y ENS

Histórico de versiones

Versión	Autor(a)	Fecha	Cambios producidos desde la última versión
1.0	Adrián Delgado	May - 2026	Primera versión
1.1	Adrián Delgado	Sept - 2026	Revisión y validación

Histórico de aprobación

Versión	Aprobadores	Fecha	Firmas
1.0	Adrián Delgado Bingen Gárate Gorka García Jone Ibarzabal	Sept - 2026	

ÍNDICE

1 Misión

Purple Blob es una ingeniería basada en servicios informáticos y de telecomunicaciones. Como parte de su actividad, Purple Blob trabaja tanto para clientes industriales como para administraciones públicas.

Purple Blob tiene como principal objetivo diseñar y desarrollar soluciones digitales de alta calidad que promuevan un uso responsable, eficiente y seguro de la tecnología para solventar problemáticas concretas.

Por ello, la organización busca un nivel de seguridad máximo tanto en sus desarrollos como en sus servicios.

2 Principio normativo

Purple Blob no está obligado por ley a cumplir ninguna política concreta de seguridad.

En el plano plenamente legal, la contratación de servicios se acoge a sus propias condiciones generales y, en casos, a las particulares. Esto es aplicable a servicios puntuales de desarrollo y proyectos de ingeniería además de a mantenimientos y soporte.

Atendiendo al ENS, si bien Purple Blob presta servicios a administración pública, estos no revierten en ningún sistema que, por sus características o funcionalidades, queden obligados por el marco del esquema.

En el posible marco de la normativa NIS2 y su posible transposición final, atendiendo a los anexos I y II, Purple Blob no es una empresa con de sector crítico, esencial o importante, lo cual la exime de cumplir requisitos de seguridad específicos.

No obstante, Purple Blob tiene como compromiso y valor empresarial la ciberseguridad. A su vez, la naturaleza de su actividad y los sectores con los que trabaja requieren altas garantías de seguridad e interoperabilidad. Es por esta razón que, pese a no existir obligación, Purple Blob se compromete a cumplir la NIS2 y mantener un nivel MEDIO de acuerdo al ENS.

3 Marco legal y regulatorio

No obstante a las obligaciones directas descritas en el principio normativo Purple Blob se enmarca en una serie de leyes y normativas que son aplicables o pueden ser de aplicabilidad en casos concretos. Con el objetivo de mantener un nivel legal y regulatorio gestionable y actualizado se describen a continuación las principales normas de dicho marco:

Área	Norma/ requisito	Relevancia y aplicabilidad
Ciberseguridad	RD 311/2022 ENS	Aplicable en el perfil de cumplimiento medio.

Ciberseguridad	NIS2 (actual Ley 8/2011)	Relevante y de especial interés en su seguimiento.
Protección de datos	RGPD	Aplicable para datos de empleados y similares que sean personales y en caso de comenzar a tratar datos personales en aplicaciones o servicios.
Protección de datos	LOPDGDD	Aplicable para datos de empleados y similares que sean personales y en caso de comenzar a tratar datos personales en aplicaciones o servicios.
Servicios digitales	Ley 34/2022 (LSSI)	Limitada y aplicable solo en boletines comerciales o en caso de habilitar comercio electrónico
Telecomunicaciones	Ley General de Telecomunicaciones	Muy limitada y en caso de colaborar en proyectos de telecomunicaciones.
Administración pública	Ley 39/2025 Ley 40/2015 RD 203/2021	Limitada y en caso de prestar un servicio directo a la administración pública
Normas CCN-STIC e ITS	Normas CCN	Aplicable y recogida internamente en caso de las guías de sistemas utilizados.

Esta información se revisa anualmente (o en caso de detectar cambios, inmediatamente) para revisar posibles cambios, cumplimiento e incluso nuevas normativas y leyes aplicables.

4 Organización de seguridad

Purple Blob basa la organización de seguridad en el modelo de gobernanza básico propuesto por el ENS. La empresa cuenta con varios responsables y un comité, lo cuales se encargan tanto de la operativa como de la supervisión, revisión y gestión de incidentes.

4.1 Definición de comités y roles unipersonales

4.1.1 Comité de seguridad

El comité de seguridad de Purple Blob está formado por cuatro roles:

- Dirección general
- Dirección comercial
- Dirección de innovación
- Responsable de seguridad

4.1.2 Roles unipersonales

Purple Blob cuenta con los siguientes responsables y roles:

- Responsable de seguridad: Jone Ibarzabal
- Responsable del sistema: Gorka García
- Responsable de información: Jone Ibarzabal
- Responsable de servicios: Gorka García
- Trabajador/empleado: cualquier empleado de la compañía.

4.2 Funciones y responsabilidades

4.2.1 Comité de seguridad

El comité de seguridad tiene las siguientes funciones y responsabilidades:

a) Designar roles de la PSI.
b) Modificar la estructura y modelo de gobernanza de la compañía.
c) Revisar anualmente todos los documentos necesarios.
d) Atender y organizar comités de urgencia bajo petición del Responsable de Seguridad.
e) Responder a incidentes de seguridad mediante reuniones.

4.2.2 Responsable de seguridad

El Responsable de seguridad deberá cumplir las siguientes funciones y responsabilidades:

a) Determinar las acciones para lograr un nivel de seguridad adecuado a lo decidido por el comité u otros organismos pertinentes.
b) Coordinar las acciones del resto de responsables y roles para asegurar que se ejecuten satisfactoriamente.
c) Revisar la implantación y ejecución de dichas acciones.
d) Ser el principal contacto entre externos y la organización en materia de seguridad.
e) Elevar situaciones al comité en caso de requerir su apoyo o decisión.
f) Determinar las medidas de seguridad aplicables, en función de las valoraciones hechas por los Responsables de la Información y los Servicios.
g) Elaborar y aprobar la Declaración de Aplicabilidad, atendiendo a los requerimientos del Responsable de la Información y del Servicio.
h) Determinación de la categoría del sistema, atendiendo a las valoraciones del Responsable de la Información y del Servicio.
i) Comprobar que las medidas de seguridad de la información han sido adecuadamente implementadas por el Responsable del Sistema.
j) Participar en la elaboración y en la propuesta de la Política de Seguridad de la Información y los procedimientos, normativas e instrucciones en aplicación del ENS.

k) Analizar los riesgos antes del despliegue de los sistemas de inteligencia artificial en la entidad, atendiendo a las valoraciones del Responsable de la Información y del Servicio y, en su caso, del Delegado de Protección de Datos y supervisar su despliegue.
l) Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
m) En la gestión de los ciberincidentes, contando con los responsables de la entidad, de la información y de los servicios, calificará la peligrosidad de estos de acuerdo a la Guía CCN-STIC 817, actuando como punto de contacto con las autoridades competentes en materia de seguridad y, en función de los roles asignados en la Política podrá notificar los mismos, en su caso, al CCN-CERT. Cuando fuese precisa la notificación al CSIRT de referencia está deberá realizarse sin dilaciones indebidas y con carácter inmediato, sin perjuicio de la remisión de información ampliada de forma paulatina.

4.2.3 Responsable del sistema

El Responsable del sistema deberá cumplir las siguientes funciones y responsabilidades:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Adoptar las medidas correctoras derivadas de las auditorías de seguridad.
c) Suspender sistemas puntualmente en caso de detectar una deficiencia grave.

4.2.4 Responsable de información

El responsable de informacion deberá cumplir las siguientes funciones y responsabilidades:

a) Valorar y catalogar la información relevante tratada por la organización.
b) Establecer requisitos de seguridad en lo relativo a la información tratada y generada por la organización.
c) Establecer y revisar anualmente los niveles de seguridad de información y su aplicación.

4.2.5 Responsable de servicio

El responsable de servicio deberá cumplir las siguientes funciones y responsabilidades:

a) Determinar los niveles de seguridad de cada servicio.
b) Determinar el nivel de cada dimensión de seguridad (CITAD) de cada servicio.
c) Gestionar los cambios necesarios para implantar medidas de seguridad en los servicios.
d) Mantener los servicios dentro de su ámbito lógico y de aplicación.

4.3 Mecanismos de coordinación

Purple Blob cuenta con varias herramientas de comunicación internas válidas que permiten una coordinación fluida, registrada y trazable. En concreto, se cuenta con capacidad de llamada a teléfono móvil, chat corporativo, correo electrónico empresarial. A su vez, Purple Blob utiliza sistemas relevantes que sirven de apoyo a la coordinación, información y operativa: el ERP, la wiki y el repositorio de archivos.

Todos estos mecanismos son válidos y deben utilizarse para las siguientes tareas de forma general:

Mecanismo	Roles y funciones	Uso apropiado
Comunicación		
Móvil	Sólo comité y responsables	Avisos urgentes y necesidades puntuales que requieren respuesta inmediata
Chat corporativo	Todos	Comunicaciones urgentes que deben atenderse o recordatorios y avisos.
Correo electrónico	Todos	Avisos no urgentes, comunicaciones con archivos o formatos, comunicaciones que requieren una trazabilidad legal demostrable
Operación		
ERP	Todos	Actividades, tareas y reuniones
Wiki	Todos	Procesos informativos compartibles, transferencia de información

4.4 Procedimientos de designación de personas

Ante cualquier cambio requerido en los responsables, comité o inclusión de un nuevo rol, el comité deberá de realizar una reunión en menos de 7 días laborables. Esta podrá realizarse vía correo electrónico o de forma presencial.

Fruto de la misma, el Responsable de Seguridad deberá coordinar la actualización, validación y firma de todos los documentos relacionados en los que se presente esta nueva designación.

5 Directrices

La PSI es una política regida por el Responsable de seguridad pero construida por todos los responsables. Por ello, todos pueden impulsar cambios dentro de su área de responsabilidad mientras que, a su vez, cualquier imperativo legal o normativo afectará directamente a la misma. Por ello, la PSI podrá ser revisada y actualizada en los siguientes casos:

a) Por imperativo legal o normativo en normativas, certificaciones o designaciones realizadas por órganos externos a la organización que dispongan de la autoridad pertienente.
b) A petición del responsable de seguridad.
c) Por orden del comité de seguridad.
d) Por orden del responsable de servicios, información y/o sistema en lo relativo a sus respectivas áreas.
e) Con frecuencia anual mínima.

En cualquier caso Purple Blob busca una política unificada, coherente y seguible para asegurar su cumplimiento. Por tanto, se seguirán las siguientes normativas y directrices:

a) La PSI y otros documentos relacionados con la seguridad se constituirán, en la medida de lo posible, en un documento único. De este modo, pese a cumplir diferentes normativas, se preferirá el uso de un documento más extenso que la generación de varios específicos.
b) Los documentos se basarán en las normativas más completas y en la unión de los requisitos de las mismas siguiendo un criterio unificado de mayor requisito de seguridad.
c) El responsable de seguridad será el principal encargado de coordinar las actuaciones necesarias para modificar, adaptar, actualizar o pivotar cualquier política, procedimiento o documento relevante.
d) El comité deberá aprobar y firmar cualquier cambio relevante en el marco de la seguridad de la organización.

Purple Blob busca cumplir actualmente con las siguientes normativas:

Normativa	Nivel
ENS	Medio
NIS2	Clasificación equivalente a importante
ISO 22301	Completo

Por último, las acciones concretas de seguridad se basarán a su vez en estándares probados de implantación de medidas concretas. A modo de ejemplo y de forma enunciativa:

- NIST para seguridad en organización.
- OWASP para seguridad web.
- CVE para vulnerabilidades y riesgos derivados de las mismas.
- Etc.

5.1 Autenticación y control de acceso

La organización establece mecanismos de autenticación adecuados al nivel de seguridad requerido para garantizar que el acceso a los sistemas de información se realiza exclusivamente por usuarios debidamente autorizados.

Las credenciales de acceso serán parsonales, instransferibles y estarán bajo el control exclusivo de su titular. La organización establecerá medidas para su adecuada entrega, activación, protección, modificación, bloqueo y renovación durante todo su ciclo de vida.

Se aplicarán mecanismos de autenticación reforzada cuando el nivel de riesgo o las condiciones de acceso así lo requieran, especialmente en los accesos realizados desde zonas no controladas y en los accesos remotos.

Los accesos a los sistemas de información serán registrados y gestionados de acuerdo con los requisitos de trazabilidad y seguridad establecidos por la organización. Cualquier pérdida, revelación, sospecha de compromiso o uso indebido de credenciales deberá ser comunicado de forma inmediata y dará lugar a las medidas de bloqeuo, renovación o sustitución que correspondan.

Las medidas concretas de autenticación, gestión de credenciales y control de acceso se desarrollarán en la Normativa de Seguridad y en los procedimientos aplicables.

5.2 Protección criptográfica y custodia de soportes

La organización establecerá medidas de protección criptográfica para garantizar la confidencialidad e integridad de la información cuando resulte necesario de acuerdo con su clasificación, nivel de seguridad y condiciones de almacenamiento o transporte.

Los mecanismos criptográficos utilizados deberán emplear algoritmos, protocolos y parámetros autorizados por el Centro Criptológico Nacional, de acuerdo con las directrices y normativa aplicables.

Los soportes de información permanecerán bajo control y custodia de la organización durante todo su ciclo de vida, aplicándose medidas físicas y lógicas adecuadas para prevenir accesos, pérdidas, alteraciones o usos no autorizados.

La organización establecerá procedimientos específicos para el cifrado de soportes extraíbles, la gestión de las claves criptográficas y la protección de las copias de seguridad. En la normativa de seguridad los empleados cuentan con una explicación detallada y un procedimiento de seguridad adicional para la aplicación de esta protección.

5.3 Estructuración de la documentación

Purple Blob concibe la seguridad de la información, incluso en sistemas de información digitales, como un proceso general que no depende exclusivamente de medidas técnicas. Uno de los principales pilares para mantener una seguridad y control sobre esta información requiere una organización completa, trazable y gestionable de los documentos. En este apartado recogemos todos los documentos relativos a la seguridad de la información incluyendo además responsables, acceso, editores, validadores, actualización y revisión mínimas.

Documento	Responsable y validador	Editores	Ubicación	Actualización	Acceso
Política de seguridad de información (PSI)	Comité de seguridad	Comité de seguridad Responsables	Files	Anual/en caso de cambios relevantes y aprobación de responsable	Todos los empleados.
Normativa de seguridad	Comité de seguridad	Comité de seguridad Responsables	Files	Anual/en caso de cambios relevantes y aprobación de responsable	Todos los empleados.
Procedimientos de seguridad	Responsable de seguridad Responsable de sistemas	Comité de seguridad Responsables	Wiki	Anual/en caso de cambios relevantes y aprobación de responsable	Se dividen en comunes a todos los empleados, exclusivos de administración de sistemas y exclusivos de responsables de seguridad de la

					información.
Instrucciones técnicas y guías CCN-STIC	Responsable de sistemas Responsable de servicios Responsable de información	Responsables	Files	Anual/en caso de cambios relevantes y aprobación de responsable	Todos los empleados.
Análisis de riesgos	Responsable de seguridad	Responsables	Eramba	Anual/en caso de cambios relevantes y aprobación de responsable	Responsables de seguridad de información.
Análisis de impacto de negocio (BIA)	Comité de seguridad	Comité de seguridad Responsables	Files	Anual/en caso de cambios relevantes y aprobación de responsable	Responsables de seguridad de información.
Declaración de aplicabilidad (SoA)	Responsable de seguridad	Responsables	Files	Anual/en caso de cambios relevantes y aprobación de responsable	Responsables de seguridad de información.
Inventario	Responsable de sistemas Responsable de servicios	Responsables	Eramba Odoo (equipos de trabajo personales)	Anual/en caso de cambios relevantes y aprobación de responsable	Responsables de seguridad de información.
Plan de continuidad de	Responsable de	Responsables	Files	Anual/en caso de cambios	Administración de sistemas y

negocio (PCN)	seguridad			relevantes y aprobación de responsable	responsables de seguridad de información.
Plan de recuperación ante desastres (DRP)	Responsable de seguridad	Responsables	Files	Anual/en caso de cambios relevantes y aprobación de responsable	Administración de sistemas y responsables de seguridad de información.
Plantillas de registro (incidentes, identificación, entrada y salida de equipos...)	Responsable de seguridad	Responsables	Files	Anual/en caso de cambios relevantes y aprobación de responsable	Administración de sistemas y responsables de seguridad de información.
Plan de formación y concienciación	Responsable de seguridad	Responsables	Files	Anual/en caso de cambios relevantes y aprobación de responsable	Todos los empleados.
Auditorías internas y externas	Responsable de seguridad	Responsables	Files	Anual/en caso de cambios relevantes y aprobación de responsable	Responsables de seguridad de información.
Control de cambios y revisiones en documentos	Responsable de seguridad	Responsables	Files	Anual/en caso de cambios relevantes y aprobación de responsable	Responsables de seguridad de información.

5.4 Segregación de funciones y tareas

La organización aplica el principio de segregación de funciones y tareas en sus entornos operativos y de gestión tecnológicos, especialmente en aquellas actividades que impliquen acceso privilegiado, cambios críticos, gestión de accesos, administración de sistemas, recuperación o supervisión.

Ninguna persona acumulará competencias o privilegios sobre los activos de información que le permitan autorizar, ejecutar, registrar, auditar o modificar operaciones críticas de forma unilateral, sin un mecanismo de supervisión, validación cruzada o aprobación previa por parte de otra figura o rol autorizado, cuando la naturaleza de la operación lo requiera.

5.5 Protección de datos personales

Cuando los sistemas de información de la organización traten datos personales, éstos seran tratados de acuerdo con la normativa aplicable en materia de protección de datos personales, incluyendo el reglamento General de Protección de Datos (RGPD), la Ley Orgánica 3/2018 y demás normativa que resulte de aplicación.

La organización aplicará las medidas técnicas y organizativas necesarias para garantizar la protección de los datos personales frente a su pérdida, alteración, destrucción, acceso o tratamiento no autorizado, teniendo en cuenta la naturaleza, alcance, contexto y fines del tratamiento y los riesgos para los derechos y libertades de las personas.

Los requisitos específicos de protección de datos aplicables a cada tratamiento serán identificados por el Responsable de Seguridad y serán considerados en el diseño, implantación, operación y modificación de los sistemas de información.

Los tratamientos de datos personales deberán estar identificados y gestionados de acuerdo con las responsabilidades establecidas por la organización, incluyendo, cuando corresponda, la realización de análisis de riesgos y evaluaciones de impacto relativas a la protección de datos.

Las medidas de seguridad derivadas de la normativa de protección de datos y de los análisis de riesgos realizados deberán integrarse en las medidas de seguridad aplicables a los sistemas de información.

De forma específica, Purple Blob no cuenta con un Delegado de Protección de Datos (DPD) ya que no incurre en ninguno de los casos expuestos en el artículo 37.1 del RGPD. En este sentido, la compañía no trata datos personales de forma sistemática o a gran escala en ninguno de sus servicios o proyectos.

Sin embargo, existen sistemas en los que puede existir un tratamiento interno ocasional, por lo que Purple Blob recoge las mismas en un Registro de Actividades de Tratamiento dentro de sus registro internos.

Finalmente, recordamos que la gestión de incidentes tiene en cuenta el proceso de aviso a las autoridades en caso de comprobar o tener indiciones de una posible fuga de datos personales.

6 Calificación de la información

La información trata en Purple Blob se clasifica en base a los siguientes niveles:

- USO OFICIAL – C. ALTO: Información cuya revelación pueda causar perjuicio grave: ciertos informes de ciberseguridad/pentest, exportaciones de producción, información sensible de clientes, secretos técnicos, información personal especialmente sensible o material que el análisis de riesgos sitúe en C ALTO.
- USO OFICIAL – C. MEDIO: Procedimientos internos; documentación de proyecto; ofertas no públicas; documentación técnica; código fuente interno sin secretos; configuraciones no sensibles; contratos y documentación administrativa ordinaria.
- PÚBLICA: información que se recibe de forma externa a Purple Blob y ya es pública antes de ser compartida.

Cualquier información cuya confidencialidad no se describa debe considerarse confidencial. Cualquier medio no etiquetado deberá considerarse como medio con información confidencial.

Toda persona con acceso a información de la organización deberá preservar su confidencialidad, integridad y disponibilidad, evitando accesos, modificaciones, divulgaciones o destrucciones no autorizadas.

La información únicamente podrá utilizarse para fines relacionados con las actividades autorizadas de la organización y deberá conservarse y eliminarse de acuerdo con los procedimientos establecidos.

A su vez, toda información contenida es responsabilidad de una única persona. Para ello, Purple Blob define el responsable de la información dependiendo de su proveniencia, situación actual y uso:

- Responsable de sistema: responsable de aquella información únicamente relacionada con los sistemas físicos o digitales de Purple Blob en el ámbito técnico y de seguridad de red. Esto incluye configuraciones, claves criptográficas, certificados y otros elementos propios de los sistemas y su puesta en marcha.
- Responsable de servicios: responsable de toda la información contenida en los servicios internos de la empresa a nivel de aplicación, es decir, información de usuarios, facturas, partes médicos y cualquier otro elemento contenido en los mismos.
- Responsable de información: responsable de toda la información de la empresa que no quede contenido exclusivamente en los sistemas

informáticos, es decir, acuerdos de colaboración, partes médicos físicos, contratos laborales, acuerdos de servicio, etc.

- Trabajador: cualquier información que se le haya facilitado de forma interna o externa para el cumplimiento de sus obligaciones laborales.

En cualquier caso, Purple Blob se reserva el derecho a investigar responsables en caso de que se hayan cometido negligencias en el transcurso del trabajo por cualquier integrante o parte externa de la organización.

Los responsables de la información deben catalogar el nivel de confidencialidad de la misma de forma clara y avisar a cualquier parte que deba interactuar con la misma de dicho nivel y las obligaciones que conlleva. Los responsables también deberán aprobar la salida de soportes de información, borrado o cualquier otra actividad relacionada con la información correspondiente.

6.1 Marcado de soportes

Purple Blob establece como obligatorio el marcado de los soportes de información que contengan información sometida a requisitos específicos de protección. Los documentos en papel, documentos electrónicos, contenidos multimedia, soportes extraíbles, copias de seguridad y demás medios de almacenamiento deberán incorporar las marcas o metadatos definidos por la organización, indicando el mayor nivel de confidencialidad de la información contenida. La creación, copia, exportación o incorporación de información a un soporte obliga al usuario responsable a verificar el marcado antes de su almacenamiento, distribución, transporte o entrega. La clasificación y cualquier cambio de nivel se realizarán conforme a los criterios aprobados por el Responsable de la Información. Las reglas operativas, plantillas, responsabilidades y evidencias se desarrollan en la Norma de clasificación y marcado de soportes de información, de obligado cumplimiento para todo el personal incluido en su alcance.

7 Concienciación y formación

Purple Blob reconoce la concienciación y la formación de sus empleados como un pilar fundamental de la seguridad de la empresa. Como tal, los empleados y procesos seguidos constituyen uno de los principales vectores de ataque, así como una fuente de riesgos asociados a dimensiones como la disponibilidad, la trazabilidad y la confidencialidad incluso en situaciones en las cuales no existe un atacante directo.

Por este motivo la organización persigue desde el diseño de sus servicios, desarrollos, procesos y sistemas internos una compartimentación que, siguiendo los principios de mínimos privilegios, evite tanto el acceso como el uso inseguro de datos y sistemas.

Sin embargo, la concienciación y formación son herramientas básicas para asegurar que cualquier medida implantada a nivel de sistema y organización resulta

realmente efectiva. Por ello, Purple Blob sigue un plan de formación y concienciación anual basado en:

- Disposición de recursos de concienciación de seguridad disponibles para todos los empleados.
- Especificación clara y trazable de los roles, responsabilidades y derechos de los empleados en materia de información, sistemas y resultados de su trabajo en la organización.
- Formación anual de principios básicos de ciberhigiene para todos los empleados.
- Formación anual de principios aplicados al desarrollo y sistemas para los empleados técnicos que trabajan en estas áreas.

8 Caracterización del puesto de trabajo

Dentro de las tareas que puede ocupar un perfil dentro de Purple Blob existen dos casos diferenciados. En primer lugar, proyectos o actividades que residen autocontenidas en un proyecto. En este caso, los trabajadores deben firmar obligatoriamente un acuerdo de confidencialidad que regula sus obligaciones y protección de datos confidenciales.

No obstante, en actividades que o bien son comunes a toda la empresa (gestión de recursos humanos, comunicación con externos, firma de documentos contractuales) o relacionadas con sistemas multiproyecto (gestión de sistemas, generación y configuración de clústers de máquinas, etc.) los empleados pueden acceder a información y niveles de administración de gran responsabilidad. Por ello, la organización regula el manejo aplicando todas y cada una de las siguientes medidas:

- Las referencias laborales y formativas de todos los trabajadores serán revisadas en el momento de contratación o en la adquisición de nuevos certificados o similares.
- Los trabajadores siempre tendrán un acceso mínimo tanto en base a sus privilegios como a los sistemas, interfaces y funcionalidades que pueden obtener.
- Se utilizarán el número mínimo de perfiles con acceso privilegiado tanto a máquinas como a sistemas puramente digitales.
- No se iniciará ni compartirá credencial alguna hasta que el empleado no haya firmado el acuerdo de confidencialidad y normativa de seguridad de la empresa.
- No se compartirán credenciales generales o se dará acceso a información de empresa hasta comprobar las referencias laborales y formativas.

A su vez Purple Blob establecerá por cada puesto de trabajo de esta tipología responsabilidades específicas, que pueden incluir:

- El nivel y tipo de acceso a la información y a los sistemas de información.

- Las obligaciones de confidencialidad, integridad y disponibilidad de la información.
- El cumplimiento de las políticas, procedimientos y medidas de seguridad establecidos por la organización.
- La custodia y uso adecuado de las credenciales, equipos, dispositivos y demás recursos puestos a disposición del empleado.
- La obligación de comunicar cualquier incidente, vulnerabilidad, pérdida, uso indebido o circunstancia que pueda afectar a la seguridad de la información.
- Las responsabilidades asociadas al tratamiento de información especialmente protegida o de carácter sensible, cuando corresponda.
- Las obligaciones específicas derivadas de la administración de sistemas, gestión de privilegios u otras funciones con impacto relevante en la seguridad.
- Las responsabilidades relativas a la conservación, protección y eliminación de la información conforme a los procedimientos establecidos.

En general esto se realizará mediante la normativa de seguridad, pudiendo ser específico por proyecto y realizando en ese caso un documento que refleje todas las particularidades que deberá estar firmado por el trabajador antes del acceso a la información o sistemas.

9 Gestión de riesgos

9.1 Plan de análisis

Purple Blob se compromete a realizar un análisis de revisión de riesgos en los siguientes casos:

a) Bajo requerimiento legal o normativo pertinente.
b) Bajo petición de cualquiera de los responsables.
c) En caso de incidente grave.
d) En caso de introducción de nuevos sistemas o procesos.
e) En caso de descubrimiento de riesgos no contemplados.
f) Anualmente en forma de revisión llevada a cabo por el responsable de seguridad.

Este análisis se realiza en una herramienta digital trazable que permite además mantener una actualización constante y efectiva del mismo, así como generar calendarios de revisión.

9.2 Criterios de evaluación de riesgos

Purple Blob sigue la normativa ISO 22301 para la continuidad de negocio. Para ello, cuenta con el documento BIA (Business Impact Analysis, Análisis de Impactos en el Negocio) el cual puede resumirse en los siguientes conceptos básicos:

a) Identificación de servicios y procesos de negocio principales de la organización. Este paso se realiza por el responsable de servicios.
b) Identificación de impactos y coste sobre los servicios y procesos de negocios principales de la organización, estimando los mismos en niveles Bajo, Medio o Alto en base a su coste en seguridad personal, económico, laboral, legal y reputacional. Este paso se realiza por el comité de seguridad.
c) Cálculo de indicadores objetivos, los cuales son decididos por el comité:
    a. RTO (Recovery Time Objective, Tiempo máximo de recuperación), definido como el tiempo en el que el servicio o proceso vuelve a la normalidad después de un incidente.
    b. MTPD (Maximum Tolerable Period of Disruption, plazo máximo tolerable de interrupción) defnido como el tiempo máximo al que la organización está dispuesta a llegar antes de considerarse irrevocablemente afectada.
    c. RPO (Recovery Point Objective, Objetivo de Punto de Recuperación). Nivel mínimo de servicio o proceso en el que la organización considera que se ha recuperado hasta un nivel que no constituye una amenaza grave.
d) Cálculo de indicadores reales, los cuales son calculados por el responsable del sistema y el responsable de servicios, los cuales muestran los niveles actuales de RTO, MTPD y RPO.
e) Generación de BIA, documento que muestra los servicios y procesos junto con su impacto y los indicadores, tanto objetivos como actuales, de cada uno de ellos. Finalmente, en caso de que los indicadores actuales no cumplan con el objetivo, el BIA recoge estrategias de mejora para lograrlos indicando un plan y un responsable. El BIA es generado por el responsable de seguridad y aprobado por el comité.

9.3 Directrices de tratamiento

En principio, el BIA será un documento privado accesible sólo a los responsables de seguridad y al personal técnico delegado de sistemas y servicios que deban conocerlo. En este sentido, se recuerda que por la metodología seguida Purple Blob genera un PCN (Plan de Continuidad de negocio) el cual sí puede ser revisado por cualquier empleado de sistemas.

Finalmente, la organización pondrá su BIA a disposición de colaboradores, auditores, certificadores y otros posibles agentes adecuados que requieran comprobar su contenido como parte de su garantía de seguridad organizacional. El contacto principal para esta compartición será el responsable de seguridad.

9.4 Proceso de aceptación de riesgo residual

Purple Blob acepta el hecho de que en la mayoría de servicios y procesos la eliminación completa del riesgo no es factible. Por ello, además de los objetivos

marcados por el BIA, la organización busca satisfacer los niveles de seguridad de otras normativas asociadas.

Si bien esto reduce el riesgo con criterios marcados y de eficacia probada, se genera un riesgo residual que debe minimizarse y contenerse en la medida de lo posible. Para ello, Purple Blob sigue la siguiente estrategia:

a) Revisión anual de los documentos por los diferentes responsables, que podrán proponer actuaciones de mejora incluso más allá de los objetivos especificados por el BIA.
b) PCN que muestra procesos de recuperación en caso de incidentes.

9.5 Integración con el análisis de riesgos en protección de datos

Purple Blob no maneja datos privados y, por tanto, la protección de datos se basa en las directrices de tratamiento marcadas previamente.

10 Proceso de revisión de la PSI

Purple Blob se compromete a la revisión anual de la PSI. No obstante, con el objetivo de mantener una actitud proactiva en materia de seguridad, todos los responsables y empleados podrán pedir una revisión justificada de la misma. Por ello, se presenta el siguiente proceso de revisión unificado:

a) Aviso. Tanto los empleados como los responsables podrán avisar de incidentes, fallos, contradicciones o simplemente mejoras detectadas que ameriten una revisión de la PSI mediante un correo electrónico o chat privado con el responsable de seguridad.
b) Reunión. El responsable de seguridad generará una reunión mediante correo electrónico o ERP con el comité para repasar el aviso en caso de considerarlo necesario.
c) Revisión. El comité revisará y contestará al aviso, generando el responsable de seguridad una serie de actuaciones en el ERP o por correo electrónico en caso de requerir cambio y modificaciones.
d) Posible validación. En caso de cambio, el responsable de seguridad elevará el o los documentación para aprobación y firma.

11 Contratación de recursos externos y Acuerdos de Nivel de Servicio

11.1 ANS

Debido a su actividad Purple Blob requiere de contratación de recursos externos que impactan directamente sobre sistemas de información relevantes. Por ello, cuando la organización recurra a recursos, servicios o proveedores externos que soporten o puedan afectar a la seguridad de los sistemas de información incluidos en el ámbito del Esquema Nacional de Seguridad (ENS), deberá establecerse, con carácter previo a la efectiva utilización del servicio, un Acuerdo de Nivel de Servicio (ANS/SLA) formalizado contractualmente con el proveedor.

El ANS deberá definir, como mínimo:

- La identificación y descripción del servicio contratado, incluyendo su alcance, funcionalidades, dependencias y condiciones de prestación.
- Los niveles de servicio comprometidos y los indicadores que permitan verificar su cumplimiento.
- El servicio mínimo admisible, entendido como el nivel mínimo de disponibilidad, capacidad, continuidad, soporte y demás características necesarias para garantizar la prestación del servicio en condiciones aceptables para la organización.
- Los mecanismos de monitorización, medición, seguimiento y reporte de los niveles de servicio.
- Los procedimientos y plazos de comunicación, gestión, escalado y resolución de incidencias.
- Las responsabilidades y obligaciones de la organización y del proveedor, incluyendo aquellas relacionadas con la seguridad de la información, la continuidad del servicio, la gestión de incidentes y la protección de la información tratada.
- Las condiciones aplicables a la subcontratación de servicios que puedan afectar al cumplimiento de los requisitos de seguridad.
- Las condiciones de revisión y actualización del ANS cuando se produzcan cambios relevantes en el servicio, en los riesgos, en los requisitos de seguridad o en el marco normativo aplicable.
- Las consecuencias derivadas del incumplimiento de los niveles de servicio o de las obligaciones establecidas, incluyendo, cuando proceda, medidas correctoras, penalizaciones, compensaciones, planes de mejora y las condiciones de resolución o rescisión contractual.

El proveedor deberá asumir contractualmente las responsabilidades que le correspondan sobre los servicios prestados y deberá colaborar con la organización en las actividades de seguimiento, control y verificación del cumplimiento de los niveles de servicio y de los requisitos de seguridad aplicables.

No se permitirá la puesta en producción o utilización efectiva de un recurso o servicio externo sujeto a esta política mientras no se hayan formalizado las condiciones contractuales y el ANS correspondiente, salvo las excepciones expresamente autorizadas por la organización y debidamente justificadas y documentadas.

11.2 Requisitos de conformidad ENS de los proveedores

Los proveedores externos que, por la naturaleza de los servicios prestados, resulten relevantes para el cumplimiento del ENS deberán acreditar, cuando sea exigible, que disponen de la correspondiente certificación de conformidad con el ENS para el sistema de información que soporta los servicios prestados a la organización.

La certificación deberá corresponder a una categoría igual o superior a la categoría ENS aplicable al servicio o sistema de información de la organización y disponer de un alcance suficiente para cubrir los servicios efectivamente prestados (niveles MEDIO o ALTO).

La organización deberá verificar la vigencia, categoría y alcance de la certificación antes de la contratación y, cuando proceda, durante la vigencia de la relación contractual. Esta verificación y la evidencia correspondiente deberán quedar documentadas.

Cuando un proveedor no esté obligado a disponer de una certificación de conformidad con el ENS, se deberán establecer contractualmente las medidas de seguridad y requisitos equivalentes que resulten necesarios, de acuerdo con el análisis de riesgos, la naturaleza del servicio y los requisitos de seguridad aplicables y en un documento firmado por ambas partes.

El incumplimiento de los requisitos de conformidad, de los niveles de servicio o de las obligaciones de seguridad establecidos contractualmente podrá dar lugar a la aplicación de las medidas correctoras y consecuencias previstas en el contrato, incluyendo, cuando corresponda, la suspensión del servicio o la resolución de la relación contractual.