SGSI.01-03 – Política de Seguridad de la Información

Control de cambios		
Versión	**Fecha**	**Descripción de cambios**
1	15/01/2025	Primera versión del documento.
1.1	21/10/2025	Errata fecha e incorporación de firma
1.2	14/11/2025	Revisión anual – Sin cambios
2	26/02/2026	16. Obligaciones del personal (referencia a uso aceptable de activos) Actualización a la nueva guía 805: 6.1. Alcance estratégico 6.4.4 Recuperación 15. Gestión de incidentes de seguridad
Nivel de clasificación		
Público		

ÍNDICE

1. Aprobación y entrada en vigor

Texto aprobado por la Dirección de **BTP ONETec,** en adelante **BTP**.
Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hora hasta que sea reemplazada por una nueva versión.

2. Introducción

BTP depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada a los servicios prestados.
El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuidad de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.
Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implican que deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de los servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.
BTP debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos TIC.
BTP debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en adelante (ENS).

3. Alcance

Esta Política de seguridad será de obligado cumplimiento para todos los miembros de **BTP que dan soporte a las actividades** de prestación de los siguientes servicios:

- Diseño, desarrollo e implantación de soluciones tecnológicas para la prestación de servicios de comunicación digital certificada y Servicios Electrónicos de Confianza.

4. Misión

La Misión de **BTP** es prestar servicios de comunicación y marketing masivos, que impulsen y/o faciliten unas comunicaciones óptimas y una máxima consecución de resultados.

Los valores de **BTP** son.

- Orientación al Cliente y al resultado: como medio para garantizar la permanencia de la compañía, desarrollando y planificando conjuntamente fórmulas que den estabilidad y valor añadido a las partes, buscando una relación estable y duración en el tiempo. Flexibilidad con el cliente, adaptación a sus necesidades particulares, respuesta rápida ante cambios.
- Potenciación del capital humano: el principal recurso con el que contamos son las personas: su experiencia, formación y conocimientos profesionales, que avalan y garantizan el buen fin de las tareas encomendadas. El trabajo en equipo, la comunicación transparente y la disponibilidad son tres pilares que soportan y enriquecen las relaciones personales en nuestra Organización.
- Flexibilidad: Somos “conseguidores” para nuestros clientes, flexibles por naturaleza.
- Calidad de servicio. Los trabajos se hacen conforme a los requisitos del cliente, con rigor, incluso para servicios de muy bajo coste. Se cumplen los compromisos del cliente siempre. Ante incidencias se cuenta con tiempos de respuesta bajos. Fiabilidad. La empresa valora la calidad del trabajo bien hecho y la promueve.
- Capacidad de renovarse y adaptación a los tiempos. Según detectamos necesidades u oportunidades saber desarrollarlas y aprovecharlas. tener productos con ciclos de vida complementarios y que aseguren su supervivencia.
- Trato al cliente muy directo, cercano y personalizado.

La visión de **BTP** es posicionarnos como una empresa de comunicación y marketing cada vez más global, con una cartera de productos y servicios de mayor recorrido y futuro, que evolucione de forma acompasada a la nueva realidad, retos y canales, adaptándonos a ello para seguir siendo relevantes y aportar el máximo valor a nuestra cartera de clientes. Ser una empresa ágil, con procesos optimizados y con una adecuada planificación, ejecución y medición de resultados.

5. Marco Normativo

La Dirección de **BTP** vela por el cumplimiento de los requisitos de la legislación aplicable y reglamentaria en materia de seguridad de la información.
Se toma como referencia básica en materia de Seguridad de la Información la normativa siguiente:

- UNE-ISO/IEC 27001:2023, Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.
- UNE-EN ISO/IEC 27002:2023, Seguridad de la información, ciberseguridad y protección de la privacidad. Control de la seguridad de la información.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- DIRECTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS 2).
- REGLAMENTO DE EJECUCIÓN (UE) 2024/2690 DE LA COMISIÓN de 17 de octubre de 2024 por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Real Decreto ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- Ley 9/2014, de 9 de mayo, de Telecomunicaciones.
- Reglamento (UE) 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento Europeo eIDAS).
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

6. Principios Básicos

Los principios básicos son las directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

6.1. Alcance estratégico

La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente.

6.2. Seguridad como proceso integral

La seguridad en **BTP** se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. **BTP** considera la seguridad de la información como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

6.3. Gestión de la seguridad basada en los riesgos

En **BTP** el análisis y gestión de riesgos es parte esencial del proceso de seguridad. La gestión de riesgos permitirá a **BTP** el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

6.4. Prevención, detección, respuesta y conservación

6.4.1. Prevención

BTP debe evitar, o al menos prevenir en la medida de lo posibles, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evolución de amenazas y riesgos. Estos controles, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

6.4.2. Detección

BTP, establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo

dispuesto en el artículo 10 del ENS (vigilancia continua y reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS, Existencia de líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

6.4.3. Respuesta

BTP:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa puntos de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

6.4.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, las distintas áreas de **BTP** deben desarrollar, cuando sea necesario, planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio de actividades de recuperación.

6.4.5. Conservación

Para garantizar la disponibilidad de los servicios, **BTP**, dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

6.5. Existencia de líneas de defensa

El sistema de información de **BTP** dispondrá de una estrategia de protección constituida por diferentes capas, de forma que cuando una de las capas sea comprometida, permita desarrollar una acción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad del que el sistema sea comprometido en su conjunto, minimizando el impacto final sobre el mismo.
Existirán líneas de defensa constituidas tanto por medidas organizativas, físicas y lógicas.

6.6. Vigilancia continua y reevaluación periódica

BTP llevará a cabo una vigilancia continua que permita la detección de actividades o comportamientos anómalos y su oportuna respuesta.
La evaluación permanente del estado de la seguridad de los activos permite a **BTP** medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. **BTP** reevaluará y actualizará periódicamente las medidas de seguridad, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

6.7. Diferenciación de responsabilidades

Los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.

6.8. Diferenciación de responsabilidades

BTP tendrá en cuenta la diferenciación de responsabilidades en su sistema de información, siempre que sea posible. El detalle de las atribuciones de cada responsable, los mecanismos de coordinación y la resolución de conflictos se detallarán a lo largo de la presente política de seguridad.

7. Requisitos mínimos

Esta política de seguridad de la Información complementa las políticas de seguridad de **BTP** en materia de protección de datos de carácter personal.

Esta Política de Seguridad de seguridad se desarrollará aplicando los siguientes requisitos mínimos:

- Organización e implantación del proceso de seguridad, de acuerdo al marco organizativo definido en el **apartado 8 de esta Política.**
- Análisis y gestión de los riesgos, de acuerdo a lo previsto en el procedimiento **PS01 Planificación.**
- Gestión de personal, de acuerdo a lo previsto en el procedimiento **PS09 Gestión de Personal.**
- Profesionalidad, de acuerdo a lo previsto en el procedimiento **PS09 Gestión de Personal.**
- Autorización y control de los accesos, de acuerdo a lo previsto en el procedimiento **PS03 Control de Acceso.**
- Protección de las instalaciones, de acuerdo a lo previsto en el procedimiento **PS08 Protección de instalaciones.**
- Adquisición de productos, de acuerdo a lo previsto en el procedimiento **PS05 Recursos externos y servicios en nube.**
- Seguridad por defecto, de acuerdo a lo previsto en el procedimiento **PS04 Explotación.**
- Integridad y actualización del sistema, de acuerdo a lo previsto en el procedimiento **PS04 Explotación.**
- Protección de la información almacenada y en tránsito, de acuerdo a lo previsto en los procedimientos **PS14 Protección de la información y PS11 Protección de comunicaciones**
- Prevención ante otros sistemas de información interconectados, de acuerdo a lo previsto en el procedimiento **PS05 Recursos externos y servicios en nube.**
- Registro de actividad, de acuerdo a lo previsto en el procedimiento **PS04 Explotación.**
- Incidentes de seguridad, de acuerdo a lo previsto en el procedimiento **PS04 Explotación.**
- Continuidad de la actividad, de acuerdo a lo previsto en el procedimiento **PS06 Continuidad del servicio.**
- Mejora continua del proceso de seguridad, de acuerdo a lo previsto en el procedimiento **PG04 Mejora continua.**

8. Organización de la seguridad

La implantación de la Política de Seguridad en **BTP** requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) Comité de Seguridad de la Información

b) Responsables del Servicio

c) Responsables de la Información

d) Responsable de Seguridad de la Información

e) Responsable del Sistema

f) Delegado de protección de datos personales

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles.

8.1. Comité de seguridad de la información

El Comité de Seguridad de la Información coordina la seguridad de la información en **BTP** Dicho Comité está compuesto por cada una de las figuras anteriormente mencionadas.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión y propuesta de la Política de Seguridad de la Información, para su aprobación por la Dirección.
- Revisión y propuesta de la Normativa de Seguridad de la Información para su aprobación por la Dirección.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinados a garantizar la Seguridad de dichos activos;

- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Promover mecanismos para asegurar la concienciación, educación y formación en materia de seguridad de todo el personal.
- Coordinar y promover las acciones necesarias, relacionadas con el cumplimiento legal y normativo, en temas relacionados con la seguridad de la información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

8.1.1. Responsable de la Información

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.
- Determina los niveles de seguridad de la información, valorando las consecuencias de un impacto negativo.
- Es el Propietario del Riesgo de los activos esenciales de información.

8.1.2. Responsable del Servicio

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Determina los niveles de seguridad de la información, valorando las consecuencias de un impacto negativo.
- Es el Propietario del Riesgo de los activos esenciales de servicios.

8.1.3. Responsable de Seguridad de la Información

El Responsable de Seguridad:

- Es nombrado por la Dirección de **BTP**.
- Es el responsable de la definición, coordinación, implantación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo a los objetivos estratégicos de la organización.
- Es el Punto de Contacto (PoC).
- Es el Propietario de todos los activos de **BTP** en lo que respecta a la norma ISO 27001. En el inventario de activos podrá especificarse un responsable del Activo, en el que el Propietario del Activo delega la toma de decisiones respecto a dicho activo.

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.

- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de **BTP.**

- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:

    - La estrategia de seguridad de la información definida por el Comité de Seguridad.
    - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de **BTP** y normativa de desarrollo.

- Supervisar (como responsable último) los incidentes de seguridad informática producidas en **BTP**.

- Difundir en **BTP** las normas y procedimientos contenidos en la Política de Seguridad de la Información de **BTP** y normativa de desarrollo, así como las funciones y obligaciones de **BTP** en materia de seguridad de la información.

- Supervisar y colaborar en las auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables tales como el RGPD.

- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de **BTP**.

8.1.4. Responsable del Sistema

Es responsable último de asegurar la ejecución de medidas para asegurar los activos y servicios de los Sistemas de Información, que soportan la actividad **BTP**, de acuerdo a los objetivos estratégicos de **BTP**.

Es el Propietario del Riesgo de todos los activos, con excepción de los activos esenciales (Servicios e Información).

Las funciones del Responsable del Sistema de la Información son las siguientes:

- Seleccionar y establecer las funciones y obligaciones a los técnicos informáticos encargados de personificar una gestión de la seguridad de los activos de **BTP**, conforme a la estrategia de seguridad definida.

- Establecer la actuación de los técnicos informáticos, en los distintos entornos de seguridad que se designen.

- Garantizar la actualización del inventario de activos de Sistemas de Información de **BTP**.

- Asegurar que existe el nivel de seguridad informática adecuado para cada uno de los activos inventariados, coordinando el correcto desarrollo, implantación, adecuación y operación de los controles y medidas destinados a garantizar el nivel de protección requerido.

- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en **BTP.**

- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.

- Mantener y actualizar las directrices y políticas de seguridad de los Sistemas de Información y normativa asociada.

8.1.5. Delegado de Protección de datos

De acuerdo a lo previsto en el artículo 39 del RGPD, las funciones del Delegado de Protección de Datos son las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

8.1.6. Propietario de Activos

El propietario de un activo, entendiendo por tal al responsable de dicho activo, tendrá las siguientes responsabilidades:

- Definir si el activo está afectado por la normativa aplicable en materia de Protección de Datos y aplicar, en su caso, los procedimientos correspondientes.
- Asegurarse de que el software que se utiliza tiene licencia.
- Definir quiénes pueden tener acceso a la información, cómo y cuándo, de acuerdo con la clasificación de la información y la función a desempeñar.
- Asegurarse de que el activo cuenta con el mantenimiento adecuado
- Asegurarse de que el personal le informa inmediatamente de cualquier violación de seguridad o mal uso de la información o los sistemas. El propietario del activo deberá informar a su vez al responsable de Seguridad para tratar la incidencia.
- Asegurarse de que la plantilla cuenta con la formación adecuada, conoce y comprende la Política de Seguridad y pone en práctica las directrices de seguridad.
- Asegurarse de que los soportes y equipos que contengan información sean desechados según lo establecido.
- Implementar las medidas de seguridad necesarias en su área para evitar fraudes, robos o interrupción en los servicios.

- Mantener documentación actualizada de todas las funciones críticas para asegurar la continuidad de las operaciones en caso de que alguien no esté disponible.
- Informar al responsable de Seguridad cuando ocurran cambios de personal que afecten al acceso de la información o los sistemas (cambio de función o departamento, causar baja en la empresa) para que se modifiquen apropiadamente los permisos de acceso.
- En los casos que aplique, asegurarse de que el personal y los contratistas tienen cláusulas de confidencialidad en sus contratos y son conscientes de sus responsabilidades.

8.1.7. Propietario del Riesgo

El propietario del riesgo, asociado a uno o varios activos de información, tendrá las siguientes responsabilidades:

- Participar en el desarrollo del análisis y evaluación de riesgos realizada al menos con carácter anual
- Verificar la conformidad con los niveles de riesgo aceptable y colaborar en la aprobación de los mismos (que le afecten), así como la gestión de los riesgos asociado a los activos de información y los riesgos de los que es responsable.
- Asegurarse de que el personal le informa inmediatamente de cualquier violación de seguridad o mal uso de la información o los sistemas. El propietario del riesgo deberá informar a su vez al responsable de Seguridad para tratar la incidencia.
- Informar al responsable de Seguridad cuando ocurran cambios del personal, la organización, o del resto de los activos de información, que pueda implicar una revisión o actualización del análisis de riesgos, o de los permisos de acceso asignados

8.2. Procedimientos de designación

Se designan, mediante acta formal las siguientes responsabilidades:

- **Responsable del Servicio**
- **Responsable de la Información**
- **Responsable de Seguridad**
- **Responsable del Sistema**
- **Delegado de protección de datos**

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

El Responsable de Seguridad de la Información será nombrado por la Dirección a propuesta del Comité de Seguridad.

8.3. Resolución de conflictos

En caso de conflicto entre los diferentes responsables y/o entre diferentes servicios de **BTP**, éste será resuelto por el superior jerárquico de los mismos con la mediación del Responsable de Seguridad. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad, elevando a la Dirección aquellos casos en los que no tenga suficiente autoridad para decidir.

En la resolución de estas controversias se tendrán siempre en cuenta las exigencias derivadas de la protección de datos de carácter personal.

9. Datos de carácter personal

BTP trata datos de carácter personal.

Todos los sistemas de información de **BTP** se ajustarán a los niveles de seguridad requeridos por la normativa vigente en materia de Protección de Datos de Carácter Personal, identificada en el apartado 5. Marco Normativo, de la presente Política de Seguridad de la Información.

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con **BTP**.

10. Objetivos de seguridad

La Dirección de **BTP** establecerá objetivos y metas enfocados hacia la evaluación del desempeño en materia de seguridad de la información, así como a la mejora continua en sus actividades, reguladas en el Sistema de Gestión de Seguridad de la Información que desarrolla esta política.

11. Mejora continua del Sistema de Seguridad de la Información

BTP garantiza un análisis continuo de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.

La Dirección de **BTP** se compromete al cumplimiento de mejora continua del Sistema de Gestión de Seguridad de la Información que desarrolla esta política.

12. Gestión de riesgos

Para todos los sistemas sujetos a esta Política de Seguridad de la Información debe realizarse periódicamente una evaluación de los a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información gestionada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información gestionados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

13. Estructuración de la documentación

Las directrices para la estructuración, gestión y acceso a la documentación de seguridad del SGSI del **BTP**, se definen en el procedimiento "**PG01 Control de documentación.**
Se ha establecido un marco normativo en materia de seguridad de la información estructurado en diferentes niveles, de forma que los principios y los objetivos marcados en la política de seguridad de la institución tengan un desarrollo específico:

- Primer nivel: la presente Política de Seguridad de la Información, que debe ser aprobada por la Dirección de **BTP** a propuesta del Comité de Seguridad.
- Segundo nivel: la normativa de seguridad de la información aprobada por la Dirección de **BTP**. En ella se establecerán unas normas de uso aceptable de los sistemas de información.
- Tercer nivel: los procedimientos de seguridad de la información, en los que se detallará la manera correcta de realizar determinados procesos de modo que se proteja en todo momento la seguridad y la información. Estos procedimientos han de ser aprobados por el Comité de Seguridad.
- Cuarto nivel: estándares de seguridad, instrucciones técnicas, buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc. Estos documentos han de ser aprobados por el Comité de Seguridad.

Los documentos que integran el SGSI se encuentran, en soporte digital, a disposición de todo el personal al que le sea necesario para el desempeño de las funciones relacionadas con su puesto de trabajo. Estará disponible para su consulta, sin posibilidad de modificación.

14. Calificación de la información

Para calificar la información de **BTP,** atenderá a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas.
Tanto el responsable de cada información manejada por el sistema como los criterios de calificación de la información, que determinarán el nivel de seguridad requerido, se establecen en el procedimiento **PS14 Protección de la información.**

15. Gestión de incidentes de seguridad

BTP dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios. Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

16. Obligaciones del personal

Todos y cada uno de los usuarios de los sistemas de información de **BTP** son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los miembros de **BTP** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de **BTP** recibirán formación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **BTP**, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

La aceptación de las normas de uso aceptable de activos y confidencialidad queda formalizada mediante la firma por parte de los empleados de los siguientes documentos:
- Política de gestión de dispositivos móviles.
- Cláusula informativa de seguridad y protección de datos.
- Acuerdo de confidencialidad

16.1. Incumplimiento

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

17. Terceras partes

Las empresas y organizaciones externas que, con ocasión de su colaboración con **BTP** para la prestación de un servicio, accedan o gestionen activos de información de **BTP** o de sus usuarios, directa o indirectamente (en sistemas propios o ajenos), comparten la responsabilidad de mantener la seguridad de los sistemas y activos de **BTP**, por lo que deberán asumir las siguientes obligaciones:

- No difundir ninguna información relativa a los servicios proporcionados a **BTP** sin autorización expresa para ello.
- Informar y difundir a su personal las obligaciones establecidas en esta Política.
- Aplicar las medidas estipuladas por RGPD en el tratamiento de los datos personales responsabilidad de **BTP** que traten por razón de la prestación del servicio.
- Aplicar los procedimientos para la gestión de seguridad relacionados con los servicios proporcionados a **BTP**. Especialmente se deben aplicar los procedimientos relacionados con la gestión de usuarios, tales como notificaciones de altas y bajas, identificación de los usuarios, gestión de contraseñas, etc., en el sentido descrito en la presente política y normativa reguladora que sea de aplicación.
- Notificar cualquier incidencia o sospecha de amenaza a la seguridad de algún sistema o activo de **BTP** a través de los mecanismos que se determinen, colaborando en la resolución de las mismas relacionados con los sistemas, servicios o personal de la propia entidad.
- Implantar medidas en sus propios sistemas y redes para prevenir la difusión de virus y/o código malicioso a los sistemas de **BTP**. Específicamente, cualquier equipo conectado a la red corporativa de **BTP** debe disponer de un antivirus actualizado preferiblemente de forma automática.
- Implantar medidas en sus propios sistemas y redes para prevenir el acceso no autorizado a los sistemas de **BTP** desde otras redes. Entre otros, se deben aplicar las actualizaciones de seguridad en sus sistemas y se debe mantener un sistema cortafuegos para proteger las conexiones desde Internet y otras redes no confiables.

BTP se reserva el derecho de revisar la relación con la entidad externa en caso de incumplimiento de las anteriores obligaciones.

18. Revisión de la política de Seguridad de la Información

Esta política será revisada de manera anual y ante cambios significativos en el Sistema de Gestión de Seguridad de la Información de **BTP**.

	Dirección: 
	Fecha: 26/02/2026