POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (PSI)

Información general

1.1. Control documental

Clasificación de seguridad:	**Público**
Versión:	**1**
Fecha edición:	**30/09/2022**
Fichero:	**BTP-PSI_v1.r2**

1.2. Estado formal

Preparado por:	**Revisado por:**	**Aprobado por:**
Nombre: Alejandro Grande Fecha: 06/07/2021	Nombre: Juan José Aza Fecha: 30/09/2022 	Nombre: Juan de la Vega Fecha: 30/09/2022 

1.3. Control de versiones

Versión	Partes que cambian	Descripción cambio	Autor cambio	Fecha cambio
1.0	Original	Creación del documento	Alejandro Grande	06/07/2021
V1.r2.	Sin cambios	Revisión anual	Juan José Aza	30/09/2022

Índice

1. Política de Seguridad de la Información

1.4. Introducción

Este documento contiene el Desarrollo de la Política de Seguridad de la Información (en lo sucesivo PSI) de BTP ONETEC, S.L. en lo sucesivo BTP, la cual se realiza de manera complementaria y en desarrollo de la Declaración de Prácticas de Certificación de BTP, así como a su Política de Seguridad de la Información, por lo que se regulan las condiciones, formas y aspectos de la seguridad de la información, respecto de los servicios de confianza prestados.

1.5. Política de seguridad de la información

La Dirección de BTP reconoce la importancia de identificar y proteger sus activos de información, y en especial los de los clientes, evitando la pérdida, la divulgación, modificación y utilización no autorizada de toda su información, comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

Es responsabilidad de la Dirección de BTP:

1. Establecer periódicamente objetivos sobre la gestión de la Seguridad de la Información, y las acciones necesarias para su desarrollo.
2. Establecer la sistemática de análisis del riesgo, evaluando el impacto y las amenazas.
3. Implementar las acciones necesarias para reducir los riesgos identificados que se consideren inaceptables, según los criterios establecidos por el Comité de Seguridad.
4. Aplicar los controles necesarios y sus correspondientes métodos de seguimiento.

5. Cumplir con los requisitos asumidos por BTP, legales, reglamentarios, de cliente y las obligaciones contractuales de seguridad.
6. Promover la concientización y formación en materia de seguridad de la información a todo el personal de BTP.
7. Aportar los recursos necesarios para garantizar la continuidad del negocio de la empresa.

La Seguridad de la Información se caracteriza como la preservación de:

a) su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

b) su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información;

c) su integridad, asegurando que la información se mantiene invariable y trazable.

1.6. Objetivos de la seguridad de la información

Los objetivos de seguridad de la información se definen por parte del Comité de seguridad de la información en las reuniones periódicas, en base a la documentación y registros aportados por el SGSI, los cuales serán aprobados por el Comité estratégico o en su defecto por la Dirección.

Las metas y objetivos estarán de acuerdo con la Política de BTP y el análisis del contexto.

Los objetivos de seguridad se agrupan entorno a los siguientes bloques de trabajo:

- Protección del conocimiento, la información y los datos.
- Protección de las tecnologías de la información y las comunicaciones.
- Protección de las instalaciones, edificios y estancias.
- Protección de los activos de la compañía.

- Protección de la continuidad del negocio.
- Cumplimiento con los estándares legales y normativos.

Esta documentación (que incluye no-conformidades, acciones correctoras y preventivas, auditorías internas, registros de formación, etc.) tiene que servir como base de referencia para el establecimiento de objetivos medibles y cuantificables orientados a la mejora continua del servicio.

Los objetivos quedan recogidos en la herramienta que da soporte al sistema de gestión de seguridad de la información.

1.7. Administración de la Política de Seguridad

La presente Política de Seguridad es administrada por BTP en su condición de Prestador de Servicios Electrónicos de Confianza de acuerdo con las previsiones del Reglamento 910/2014 del 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. Asimismo, la misma cumple con los requisitos exigidos por el Sistema de Gestión de la Seguridad de la Información implementado por BTP.

Las modificaciones a este documento y sus correspondientes aprobaciones se realizan a través del procedimiento de Gestión documental y si fuera necesario según lo previsto en la Política de gestión de cambios de BTP, considerando los roles y responsabilidades previstos en el proceso de toma de decisión. Igualmente, las responsabilidades sobre la implementación de la política de seguridad se rigen asignan a través del mencionado procedimiento.

1.8. Del alcance y ámbito de aplicación

Esta política de seguridad se aplicará a la ejecución de las actividades relacionadas con los servicios del Prestador de Servicios de Confianza, esto es Gestión del ciclo de vida de los certificados electrónicos (emisión, validación, mantenimiento y revocación).

En consecuencia, la presente política será de cumplimiento obligatorio para todo el personal de BTP, y también para cualquier tercero que intervenga o participe en la ejecución de las actividades relacionadas con la prestación de dichos servicios.

1.9. Comunicación

La Presente Política de Seguridad será notificada a todos los empleados, terceros y partes interesadas que participen en la ejecución de actividades relacionadas con la prestación de los servicios de confianza y de certificación. En la medida en que sea aplicable, será incluida dentro de los planes de formación del personal y terceros vinculados.

2. Desarrollo de la PSI

La presente política de seguridad se realiza en forma complementaria y en desarrollo directo de la Declaración de Políticas de Certificación de BTP, que regula las condiciones, formas y aspectos de la seguridad de información, respecto de los servicios de seguridad de la información.

2.1. Normas y referencias

- Norma ISO/IEC 27001, puntos: A.5, A.8.3.2, A.11.2.4, A.11.2.7 y A.13.2.1.
- Reglamento 910/2014 del 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

2.2. Desarrollo de la Política

A continuación, se definen los controles y procedimientos de seguridad que garantizan la aplicación de la política de seguridad, los cuales se organizan en los siguientes puntos.

- Controles de seguridad.
- Controles en la gestión de la seguridad.
- Tratamiento de la información.

3. Controles de Seguridad

3.1. Controles de seguridad física

Estas medidas resultan aplicables a las instalaciones donde se producen las operaciones vinculadas a la prestación de servicios de confianza. La gestión de las instalaciones corresponde a Uanataca, S.A., como proveedor de la infraestructura de clave pública (PKI) que sustenta el servicio de confianza de BTP.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso.

a) Controles de acceso;
b) Clasificación y tratamiento de la información;
c) Seguridad física y del entorno;
d) Aquellas orientadas a los usuarios finales, como:
    i. Uso aceptable de activos.
    ii. Política de pantallas y escritorios despejados.
    iii. Transferencia de información.
    iv. Teletrabajo y dispositivos móviles.
    v. Restricciones en la instalación y el uso del software.
e) Transferencia de información;
f) Copias de seguridad;
g) Protección frente a malware.
h) Gestión de vulnerabilidades técnicas;
i) Controles criptográficos;
j) Seguridad de las comunicaciones;
k) Política de privacidad y de protección de los datos personales; y,
l) Relaciones con los proveedores.

3.2. Seguridad Física y el Entorno

Los equipos y sistemas de la Infraestructura de Clave Pública, se alojarán en un rack/armario aislado físicamente de otras infraestructuras hospedadas en el Data Center.

El Centro de Datos de producción y alta disponibilidad se ubica en instalaciones seguras de un proveedor de servicios de hospedaje para procesamiento de datos.

3.3. Controles de acceso a la información sensible

Los equipos informáticos al servicio de la PKI, se encuentran protegidos con medidas de seguridad que impiden el libre acceso a la información allí contenida. Los documentos electrónicos y registros digitales relativos a las actividades críticas de certificación y registro se encuentran protegidos contra posible destrucción, alteración de datos, incluyendo especialmente información confidencial y datos personales de los suscriptores y firmantes de los certificados digitales.

Adicionalmente, todo el personal que desarrolle funciones fiables, que le permita acceder a información sensible dentro de los sistemas de información, se autenticará en los sistemas mediante autenticación fuerte con certificado electrónico.

3.4 De otros entornos y ambientes

3.4.1. Seguridad de los servidores de almacenamiento

La información relacionada con los procesos de la PKI se guarda de manera segura y se dispone de servidores de respaldo con la finalidad de eliminar el riesgo asociado a una única ubicación. Se dispone de copia de respaldo de las claves privadas de la AC fuera de los centros de procesamiento de datos de la PKI en lugares cercanos a sus instalaciones.

3.4.2. Conexiones

- Operador neutro de comunicaciones.
- Interconexión entre clientes.
- 2 MMR con acceso al edificio independientes

3.4.3. Seguridad

Las infraestructuras físicas relativas a la PKI se protegen a través de:

- Vallas anti-trepamiento con sensor de movimientos automatizado y pilones anti alunizajes.
- Seguridad perimetral externa
- Control de acceso biométrico
- Circuito cerrado de CCTV con video análisis
- Sistema de Alarma perimetral
- Personal de seguridad 24x7
- Notificaciones a central receptora de alarmas externa

3.4.4. Entorno controlado

- Sistema de alarma y monitorización 24x7 centralizado
- Agente extintor 3M Novec 1230
- Sistema de detección temprana (VESDA)
- Soporte CSU 24x7

3.4.5. Certificaciones

Las instalaciones donde se encuentra alojada la infraestructura PKI, cuentan con las siguientes certificaciones:

- ISO 9001:2008
- ISO 27001

3.4.6. Potencia eléctrica

- Doble acometida de 2 MW. (Fase I) 4 MW (Fase II)
- Distribución eléctrica modular
- Líneas A+B por Rack protegidas con UPS y Generador en redundancia 2N

3.4.7. Climatización

- Pasillo frío confinado

- Pasillo caliente con recuperación del aire
- Free Cooling
- Sistemas de alta eficiencia N+1

3.4.8. Racks

- Tamaño: 600x1000x47u
- Potencia: de 16 hasta 64 Amperios por rack (monofásica o trifásica)

Además de lo anterior, se disponen espacios físicos, con medidas de control de acceso, donde almacena los documentos físicos contentivos de la información crítica de los servicios de verificación y registro. El acceso a este espacio físico se encuentra restringido con sistemas de control de acceso biométrico y/o llaves, los cuales serán controlados y autorizados de forma centralizada.

4. Controles de Seguridad

4.1. Auditorias y Detección de Intrusiones

BTP somete sus sistemas a auditorías periódicas de acuerdo con los requerimientos del Reglamento (UE) 910/2014 eIDAS, sobre los sistemas que se encuentran directamente vinculados con la prestación de los servicios de confianza. Asimismo, UANATACA como proveedor de la infraestructura de clave pública se somete a auditorías de conformidad según el Reglamento eIDAS y a auditorías de acuerdo con la Norma ISO/IEC 27001.

Igualmente se somete a las auditorias en las formas, condiciones y alcance descrito en su Declaración de Prácticas de Certificación, con el fin de verificar su conformidad con el mismo.

En base a los resultados de las auditorías, establece controles y acciones de seguimiento sobre las incidencias verificadas.

Periódicamente se realizan pruebas de la seguridad del sistema en busca de vulnerabilidades. En el caso de ser detectadas se abre una incidencia interna con prioridad alta para realizar las acciones necesarias para corregir la vulnerabilidad. En el caso de no existir una solución definitiva en el momento de haber sido analizado se tomarán las medidas que minimicen el riesgo hasta tener la solución definitiva. El escaneo de vulnerabilidades se realiza tal y como se describe en el Manual de seguridad interno de BTP.

También se realizan pruebas de intrusión de manera activa con el de determinar las debilidades de seguridad. Las pruebas tienen por objeto de garantizar el cumplimiento normativo la concienciación del personal y nuestra capacidad para identificar y responder a los incidentes de seguridad. El test de intrusión se realiza tal y como se describe en el Manual de seguridad interno de BTP.

4.1.1. Pruebas Internas

Esta prueba simula un ataque interno en la zona segura por un usuario autorizado, con privilegios de acceso estándar. El objetivo es estimar el impacto que una persona autorizada podría causar.

4.1.2. Pruebas Externas

Estas pruebas de penetración se dirigen a los servidores o dispositivos de la compañía que son visibles externamente, incluyendo servidores de nombres de dominio (DNS), servidores de correo electrónico, servidores web o firewalls. El objetivo es averiguar si un atacante externo puede entrar y hasta dónde puede llegar una vez que ha obtenido acceso.

4.2. De los Activos

Se mantiene un inventario sobre los activos que componen la infraestructura, y demás equipos que pueden estar vinculados a las operaciones de los servicios de confianza y de certificación. En este sentido, se documenta la incorporación y/desincorporación de cualquier elemento componente de la infraestructura de clave pública que sustenta la prestación de sus servicios de confianza.

La documentación de las acciones indicadas en el párrafo anterior contendrá indicación expresa de los procedimientos de seguridad que se adoptaron para la ejecutar dichas actividades, de acuerdo a la Declaración de Prácticas de Certificación y los protocolos de gestión de llaves criptográficas si hubiese lugar.

4.3. Configuración

Se revisa periódicamente la configuración y condiciones de sus sistemas para detectar disparidades con sus políticas.

5. Tratamiento de la información

5.1. De la eliminación y destrucción

Conforme a la Declaración de Prácticas de Certificación y procedimientos propios del SGSI, se realiza la eliminación de los soportes de la información en forma segura, asegurando que la información no puede ser recuperada.

En relación con los soportes en papel, se utilizan máquinas trituradoras de papel para su posterior desecho, o alternativamente la utilización de papeleras donde la documentación de deposita previa inutilización manual para su posterior desecho controlado. En el caso de soportes magnéticos, es posible su reutilización siempre que hayan sido sometidos a un proceso de borrado permanente o formateo que verifique que la información que estaba allí contenida no puede ser recuperada. En el caso de que estos soportes formen parte de la infraestructura de clave pública a través de la que se prestan servicios electrónicos de confianza los procesos de borrado y manipulación deberán documentarse.

En el caso de que se optase por desechar o eliminar un soporte magnético de información, se procederá a través de su destrucción física a través de múltiples perforaciones, su incineración o inutilización a través de fuerza física, de acuerdo con el caso de que se trate.

5.2. Custodia de la información

BTP se asegura de custodiar y preservar los Logs de todos los sistemas de su infraestructura destinada a la prestación de sus servicios electrónicos de confianza, por un mínimo de 7 años a partir de su generación.

Igualmente, BTP custodia la información relativa al ciclo de vida de los certificados y los suscriptores/firmantes por un período de 15 años contados a partir de la expiración de estos.

5.3. De la información sensible

La información sensible será clasificada de acuerdo como clasificada, de acuerdo con las previsiones de la Declaración de Prácticas de Certificación. La clasificación de la información se especificará en cada política o manual de procedimientos aprobados, los cuales describirán la forma y condición del manejo de la información.

En cualquier caso, la Dirección de BTP podrá a su discreción restringir o permitir el acceso a la información por parte de los empleados basados en el principio de acceso mínimo requerido para el desarrollo de sus funciones.

5.4. Del intercambio de información

Toda la información que sea objeto de intercambio ya sea en la propia compañía, entre empresas del grupo o terceras partes debe estar controlada, adoptando por lo tanto procedimientos y controles que aseguren la protección de esta.

Para ello se asegurará la protección de la información en el momento de ser transferida o intercambiada y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad con aquellos terceros con quienes se realice dicho intercambio.

En virtud de lo anterior, se definirá:

1. Modelos de acuerdo de confidencialidad para empleados y terceros ajenos a la compañía, incluyendo compromisos de no divulgación de la información, retorno o destrucción de esta una vez cumplido.
2. Canales de comunicación electrónica idóneos para el intercambio seguro de información.
3. Métodos de intercambio de comunicación físicos que aseguren la correcta protección de la información.

6. Otras Consideraciones

6.1. Revisión del plan

BTP revisará la presente política de seguridad anualmente.

Sin perjuicio de lo anterior, se revisará este documento si se materializase alguna de las amenazas o riesgos sobre los servicios y/o procesos esenciales detallados en el mismo, adoptando las medidas que sean necesarias para que la incidencia no se repita.

Las modificaciones del plan para la gestión de la continuidad se realizarán de acuerdo con lo previsto en la Política de Gestión de cambios de BTP.