Código RSC.PG.07.001	**Fecha de emisión** 02.12.2021	**Fecha de última actualización** 02.12.2021
Área Engineering		
Unidad / Building Block Responsable Corporate Security		
Equipo Corporate Security		

Política General de Seguridad de la Información y Ciberseguridad

Indice

1. Introducción

1.1 La presente Política es una trasposición de la Política General de Seguridad de la Información del Holding (Casa Matriz), por lo que, en aquellas directrices cuya participación involucra al BBVA Perú y a la Casa Matriz se denominará el "Grupo". Asimismo, cabe destacar que, durante la elaboración de la presente Política se ha tomado en consideración el cumplimiento de la regulación local y normativa interna.

1.2 La presente Política emana de la siguiente regulación externa:

- Resolución SBS N° 504-2021: Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad
- Resolución SBS N° 877-2020: Reglamento para la Gestión de la Continuidad del Negocio
- Resolución SMV Nº 027-2016-SMV/01:Reglamento de Gestión del Riesgo Operacional
- Resolución SBS N° 6523-2013: Reglamento de Tarjetas de Crédito y Débito
- Resolución SBS N° 5570-2019: Modificación Reglamento de Tarjetas de Crédito y Débito

1.3 El BBVA Perú (en adelante, "BBVA" o el "Banco") y sus Empresas Subsidiarias utilizan todo tipo de información (propia, de clientes y de terceros) para el desarrollo de sus diferentes actividades y para la propia gestión de las entidades, que se considera necesario proteger como si de otro tipo de activo se tratase.

1.4 Por ello, el Banco ha considerado oportuno desarrollar la presente Política General de Seguridad de la Información y Ciberseguridad (en adelante, la "Política") con el objetivo de establecer, mantener y gestionar los controles de seguridad sobre su procesos.

1.5 A efectos de esta Política, se entiende por Seguridad de la Información y Ciberseguridad la protección física y lógica de la información, proporcionada por clientes, terceros o información propia del Banco y/o Subsidiarias, de la que se vale BBVA en el desarrollo de sus actividades para cumplir con su propósito. Se incluye la protección de los activos tecnológicos de tipo físico que contengan información, tales como, Centros de Procesamiento de Datos, cabinas de disco, dispositivos, redes de comunicaciones, ordenadores, etc.; y los de tipo lógico, tales como, aplicaciones, sistemas de procesamiento y almacenamiento de datos, fondos y activos financieros tanto de origen interno como de clientes, siempre que estén incorporados en los

Sistemas de Información del Banco, etc., referidos conjuntamente en adelante como "Recursos".

2. Objeto y ámbito de aplicación

Objeto

2.1 El objeto de la presente Política es definir los principios fundamentales de gestión de la Seguridad de la Información y Ciberseguridad en el Banco, Red de Oficinas y Subsidiarias, así como, su modelo de gestión y de gobierno.

2.2 La presente Política se dirige a proteger la información, en lo relativo a su confidencialidad, integridad y disponibilidad, en todo su ciclo de vida (generación, tratamiento y destrucción), ya sea internamente, con independencia del medio de acceso a la información (en edificios corporativos, oficinas, otras instalaciones por medio de teletrabajo, etc.), o en servicios externalizados en proveedores. Los equipos encargados de la seguridad lógica, seguridad física y la ciberseguridad velarán por que los sistemas estén adecuadamente protegidos ante eventos accidentales o intencionados que puedan poner en riesgo la protección de la información, implementando a tal fin las medidas que consideren apropiadas en cada momento.

2.3 En cuanto a la protección de los Recursos, esta Política persigue preservar la seguridad de las instalaciones y edificios en los que el Banco procesa y almacena la información.

Ámbito de aplicación

2.4 La presente Política aplica a la Sede Central del BBVA, Red de Oficinas y Empresas Subsidiarias.

3. Principios generales

3.1 El BBVA apuesta por la implementación de un modelo de gestión de la Seguridad de la Información y Ciberseguridad, que se rige por los siguientes principios:

- Integridad.
- Debida diligencia.
- Transparencia.
- Consecución de un negocio rentable y sostenible a largo plazo.
- Cumplimiento de la legislación aplicable en cada momento.

3.2 En este contexto y con carácter específico para el ámbito de Seguridad de la Información y Ciberseguridad la presente Política establece los siguientes principios:

- Establecer un marco organizativo y un modelo de gobierno en el ámbito de Seguridad de la Información y Ciberseguridad.
- Definir, desarrollar e implantar los controles técnicos y organizativos que resulten necesarios para garantizar la Seguridad de la Información y Ciberseguridad en el Banco.
- Garantizar el alineamiento de las medidas de Seguridad de la Información y Ciberseguridad implantadas con la estrategia del Banco.
- Promover una cultura de Seguridad de la Información y Ciberseguridad para el personal interno y externo fomentando la concientización y sensibilización sobre la importancia de la Seguridad de la Información y Ciberseguridad y sobre cómo incorporarla a su actividad ordinaria.
- Considerar la Seguridad de la Información y Ciberseguridad como un proceso de mejora continua, que permita alcanzar niveles de seguridad cada vez más elevados mediante la adopción de mejores prácticas.

4. Disposiciones / directrices de la Política

4.1 El modelo de gestión de Seguridad de la Información y Ciberseguridad en el BBVA se basa en unas directrices generales en materia de seguridad establecidas por la Disciplina de Corporate Security para todo el Banco, en el modelo operativo de Seguridad y en el modelo de control de la actividad de Seguridad, que asegura una adecuada gestión de las operaciones y mitigación de los riesgos existentes. Todo ello, de forma coherente con el modelo de control interno de tres líneas de defensa que se describe en el apartado 4.1.3.

4.1.1 Directrices Generales de Seguridad de la Información y Ciberseguridad

El BBVA cuenta con un modelo de seguridad y ciberseguridad que engloba el conjunto de procesos, elementos organizativos y herramientas de las que se sirve la Disciplina de Corporate Security para proteger los recursos del Banco, de sus clientes y, en su caso, de terceros con los que se relaciona, incluyendo la información. Este modelo ha ido evolucionando para hacer frente a las nuevas amenazas, pasando de una respuesta puramente reactiva, a una preventiva basada en datos y herramientas de analítica avanzada.

Para la evolución y despliegue de dicho modelo, el Banco se apoya en un Programa de Seguridad y Ciberseguridad, que consiste en un conjunto de proyectos y acciones que permiten alcanzar los niveles de protección deseados, gobernado de manera centralizada y ejecutado allí donde sea necesario emplear recursos de cara a cubrir las necesidades detectadas.

Asimismo, la Disciplina de Corporate Security cuenta con un set de indicadores operativos que permiten realizar un seguimiento adecuado de la función y desempeño en este ámbito.

Por otro lado, la actividad de Seguridad de la Información y Ciberseguridad estará sujeta al cumplimiento de la normativa legal vigente y las políticas y normativas vigentes en el BBVA en todo momento, independientemente de que se lleve a cabo internamente o mediante la contratación de empresas externas. A tal fin, el modelo de control interno del Banco deberá asegurar este cumplimiento de la normativa legal e interna del Banco en todo momento.

4.1.2 Modelo Operativo de Seguridad

El Modelo Operativo de Seguridad consiste en un conjunto de procesos que proporcionan al Grupo una protección suficiente en función de la exposición al riesgo de seguridad en todo momento. Estos procesos se ejecutarán de forma centralizada, y con carácter global, de forma que se puedan obtener sinergias y aprovechar el conocimiento de un servicio centralizado. No obstante, los procesos de Seguridad de la Información y Ciberseguridad que, por su naturaleza, requieran de mayor cercanía y conocimiento del negocio local, se podrán ejecutar localmente desde las geografías bajo unas directrices definidas por el Head de Corporate Security (en adelante, "CSO Global").

La segmentación entre los servicios de prestación local y global será revisada de manera periódica en el seno del modelo de madurez de servicios, y el nivel de calidad en la prestación de ambos servicios será objeto de monitorización periódica.

4.1.3 Modelo Control de la Actividad de Seguridad de la Información y Ciberseguridad

El modelo de control y gestión de la Seguridad de la Información y Ciberseguridad del Grupo está alineado con el modelo de control interno del Grupo basado en tres líneas de defensa.

Las distintas funciones de control (primera, segunda y tercera líneas de defensa) del Grupo cooperarán activa y regularmente en la supervisión de la aplicación de la Política y del control del riesgo de seguridad de la información, de acuerdo con las atribuciones que les hayan sido conferidas:

a. **Corporate Security:** Como primera línea de defensa será la encargada de la gestión de los procesos de Seguridad de la Información y Ciberseguridad en el BBVA.
b. **Risk Control Specialist (RCS)**: Como segunda línea de defensa define el marco general de mitigación y control de los riesgos de Seguridad de la Información y Ciberseguridad y lo contrasta con el ambiente de control implementado.
c. **Auditoría Interna de BBVA:** Realiza una revisión independiente del modelo de gestión, verificando el cumplimiento y la eficacia de las políticas establecidas, y proporciona información independiente sobre el ambiente de control.

4.2 Los controles que prevengan la materialización de riesgos de Seguridad de la Información y Ciberseguridad estarán identificados y serán objeto de verificación de su correcta definición y funcionamiento, de acuerdo al modelo de control del Grupo.

4.3 Con el objeto de realizar un enfoque integral de la Seguridad de la Información y Ciberseguridad, el proceso de admisión de iniciativas del BBVA contempla los riesgos de Tecnología y Seguridad, Seguridad de la Información y de los datos, donde dependiendo de la naturaleza de la iniciativa se requerirán de medidas y/o controles adecuados para implantar dicha iniciativa de acuerdo a su nivel de riesgo.

4.4 La actividad propia de Seguridad de la Información y Ciberseguridad, proporcionada internamente o mediante la contratación de empresas externas, estará sujeta al cumplimiento de la normativa legal vigente y de las políticas y normativas vigentes en el BBVA en todo momento. El modelo de control deberá asegurar este cumplimiento de la normativa legal e interna del Banco.

5. Modelo de gobierno y supervisión (Términos de aprobación, revisión y supervisión)

5.1 La presente Política ha sido aprobada por el Directorio de BBVA Perú en fecha 15 de diciembre de 2021 y entrará en vigor al día siguiente de su aprobación.

5.2. La Política ha sido elaborada y coordinada por la Disciplina de Corporate Security, con la colaboración de los equipos involucrados, dentro del ámbito de sus respectivas competencias.

5.3. El Head de la Disciplina de Corporate Security será el responsable, en el ámbito ejecutivo, de la presente Política y, por tanto, se encargará de someterla a aprobación, así como de su publicación, promoviendo su conocimiento por parte de las personas sujetas a la misma.

5.4. El responsable de la Política conocerá su grado de aplicación, apoyándose en la información proporcionada por los responsables de las áreas a las que aplique, y adoptará las medidas

necesarias en caso de que no se esté aplicando adecuadamente, reportando de ello según corresponda.

5.5. Por su parte, los responsables de las áreas afectadas por la Política facilitarán, en sus respectivos ámbitos de responsabilidad y cuando corresponda, la dotación de los medios, sistemas y organización suficientes para su cumplimiento.

5.6. El control sobre el grado de cumplimiento tanto de esta Política como de su desarrollo se llevará a cabo de acuerdo con el Modelo de Control Interno. Las distintas funciones de control de BBVA cooperarán activa y regularmente en la supervisión de la aplicación de esta Política, de acuerdo con las atribuciones que les hayan sido conferidas.

5.7. Con una periodicidad mínima anual, o ante la ocurrencia de cualquier evento que requiera de cambios en la presente Política, la unidad de Corporate Security procederá a su revisión y someterá a la consideración de los equipos responsables aquellas actualizaciones y modificaciones que en cada momento se consideren necesarias o convenientes.

5.8. Los incumplimientos de las disposiciones de esta Política se encuentran sujetos a las sanciones contempladas en el Código de Conducta del BBVA.

5.9. Las personas que tengan conocimiento, indicio o sospecha de una actuación o situación relacionada con la sociedad que, aunque no esté comprendida en el ámbito de su responsabilidad, pueda ser contraria a esta Política, a la normativa interna que la desarrolla o a los valores y pautas establecidos, deberá comunicarlo por los circuitos correspondientes, pudiendo siempre hacerlo en el Canal de Denuncia a través de los cauces indicados en el Código de Conducta.

Glosario

- **Ciberseguridad:** También conocida como seguridad informática o seguridad de tecnología de la información. Es el área relacionada con la informática que se enfoca en la protección de la infraestructura tecnológica y todo lo vinculado con la misma y especialmente la información contenida en un sistema informático o que se comunica a través de la red interna o externa de la compañía.
- **Confidencialidad:** Propiedad por la que la información no se pone a disposición o se revela sin autorización a individuos, entidades, procesos o sistemas.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable por una entidad autorizada, así como de encontrarse a disposición de las personas que deben acceder a ella en el momento en que la precisen.

- **Información:** Conjunto de datos con significado o conocimientos que pueden ser comunicados, presentados o almacenados, con independencia del soporte en el que se encuentren.
- **Integridad:** Propiedad de salvaguardar la exactitud y completitud de un activo de información.
- **Recurso:** En el contexto de esta Política son los medios de los que se vale la Entidad para cumplir con su propósito. Los recursos pueden ser físicos, en la medida que contengan o procesen información, (como Centros de Procesamiento de Datos, ordenadores, cabinas de disco, etc) o lógicos (sistemas, aplicaciones, información, etc). A efectos de esta Política también se consideran como Recursos los fondos y activos financieros tanto de origen interno como de clientes, siempre que estén incorporados en los Sistemas de Información del Banco.
- **Seguridad:** Protección de los recursos tanto de BBVA como de los que faciliten los clientes para la prestación de los servicios.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Transposición**: fórmula de extensión a las filiales que consiste en la adopción de una Política General, Norma o Procedimiento con alcance de Grupo, mediante la cual se incorporan las especificidades requeridas por la filial, asegurando su alineamiento con la Regulación Interna que corresponda.

Control de Cambios

Fecha	Descripción del Cambio	Autor	Revisor	Aprobador
02/12/2021	▬ Creación del documento.	Gleny Fernández	Antonio Avila	Directorio de BBVA Perú