

Seguridad Cibernética y de la Información

Código	PO-SI-0001
Edición N°	04
Fecha	20-Nov-2025

La información aquí contenida es estrictamente CONFIDENCIAL y propiedad exclusiva de Banesco y sus empresas filiales; no puede ser copiada, divulgada o transmitida a personas distintas a la organización sin la previa aprobación por escrito de la empresa.

Contenido

I. Información General de la Política	3
1. Introducción	3
2. Objetivo y Alcance	3
3. Referencias Normativas, Disposiciones Legales y Pautas Reglamentarias	3
II. Políticas	3
III. Glosario de Términos	3
IV. Anexos	4
V. Aprobación del Documento	4
VI. Historia de Cambios	4

I. Información General de la Política

1. Introducción

Los Principios de Seguridad Cibernética y de la Información son unas declaraciones de las responsabilidades, conductas y ética aceptadas que regulan la planificación de la seguridad de la información de **BANESCO BANCO MÚLTIPLE, S.A.**

Estas se encuentran organizadas de acuerdo con los controles de seguridad establecidos por el Reglamento de Seguridad Cibernética y de la Información (RSCI), el cual provee las directrices y requerimientos necesarios para establecer un sistema de gestión de seguridad confiable, flexible y en cumplimiento con la normativa aplicable.

2. Objetivo y Alcance

La presente política tiene como propósito establecer los lineamientos específicos de Seguridad Cibernética y de la Información para **BANESCO BANCO MÚLTIPLE, S.A.**, en alineación con el Reglamento de Seguridad Cibernética y de la Información, así como con la Política Corporativa de Ciberseguridad de Banesco Internacional. Asimismo, busca comunicar a todos los colaboradores de la organización el compromiso institucional con el acceso, uso y manejo responsable de la información y de los activos de la organización, garantizando su protección y adecuada gestión.

Esta Política aplica para todos los Colaboradores de **BANESCO BANCO MÚLTIPLE, S. A.**, personal subcontratado, proveedores de servicio, consultores, pasantes, terceros, entes reguladores que accedan de manera interna o externa a cualquier tipo de información de la Organización, independientemente de la ubicación, medio, formato o presentación en la cual se encuentre.

3. Referencias Normativas, Disposiciones Legales y Pautas Reglamentarias

- Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología.
- Norma ISO /IEC 27000 y 17799 respecto a las mejores prácticas recomendadas en temas de seguridad de la información.
- Norma ISO/IEC 27034 en cuanto a las mejores prácticas en la seguridad de aplicaciones.
- Normas emitidas por el Instituto Nacional de Normas y Tecnología (NIST), referente a las gestiones para reducir los riesgos de ciberseguridad y proteger su información.
- Reglamento de Seguridad Cibernética y de la Información, aprobado por la Junta Monetaria.
- PO-SEG-001. Políticas Corporativas de Ciberseguridad

II. Políticas

A. Generales.

1. La gestión de la ciberseguridad y de la seguridad de la información en la organización se alinea con los marcos y metodologías de arquitectura empresarial, tales como TOGAF, con el fin de garantizar la integración coherente de la seguridad en todos los dominios tecnológicos y de negocio.
2. La Arquitectura de seguridad de la organización podrá desarrollarse tomando como referencia la metodología TOGAF, asegurando la integración de los principios de ciberseguridad dentro del ciclo de vida de la arquitectura empresarial.
3. La información de **BANESCO BANCO MÚLTIPLE S.A.** debe ser clasificada por su Propietario, siguiendo los criterios de la Organización, de acuerdo con su valor para el negocio, criticidad, sensibilidad, riesgo de pérdida o compromiso, y/o requerimientos legales de retención.
4. La información del negocio constituye un activo esencial para **BANESCO BANCO MÚLTIPLE S.A.**, por lo que deberá ser protegida de manera proporcional a su valor, criticidad y función dentro de la organización.
5. Se prohíbe la captura, grabación, reproducción, copia o extracción de información perteneciente a **BANESCO BANCO MÚLTIPLE, S.A.** hacia terceros o hacia dispositivos personales de colaboradores, salvo que exista una autorización expresa y formal emitida por las áreas competentes para dichos fines.
6. El acceso a los activos de información de **BANESCO BANCO MÚLTIPLE S.A.** debe ser controlado en función de las necesidades del negocio, mediante la asignación de privilegios estrictamente limitados a lo requerido por los usuarios de la Organización para la realización de las responsabilidades asociadas con el rol que desempeñan a través de la Gerencia de Seguridad Cibernética y de la Información.
7. **BANESCO BANCO MÚLTIPLE, S.A.** proveerá a sus colaboradores los equipos tecnológicos necesarios —como computadoras, dispositivos móviles u otros medios autorizados— para el desempeño de sus funciones y la conexión segura a la red corporativa. Dichos equipos deberán ser utilizados exclusivamente para fines laborales, conforme a los requerimientos de seguridad establecidos por la organización y con el propósito de garantizar la protección y aseguramiento de la información institucional.
8. Los dispositivos de almacenamiento extraíbles, como USB, CD/DVD-ROM u otros medios similares, permanecerán bloqueados en los equipos pertenecientes a **BANESCO BANCO MÚLTIPLE S.A.** para la entrada y salida de datos, con el fin de garantizar la protección y aseguramiento de la información corporativa. Cualquier excepción a esta restricción deberá estar debidamente justificada y contar con la aprobación formal conforme a lo establecido en la NR-SI-0006 Norma de Excepción de Políticas de Seguridad.

9. Estará prohibido el uso de equipos personales para la conexión a la red local de **BANESCO BANCO MÚLTIPLE S.A.** con la finalidad de no introducir riesgos dentro de la red corporativa a través de fallas de seguridad provenientes de dichos equipos, salvo justificación establecida para tales fines en la **NR-SI-0006 Norma Excepción de Políticas de Seguridad**, y aceptación de los requerimientos de seguridad institucionales al respecto.
10. **BANESCO BANCO MÚLTIPLE, S.A.** Garantizará el cumplimiento de todas las regulaciones y normativas locales aplicables en materia de privacidad y seguridad de la información, asegurando que sus procesos, prácticas y sistemas estén alineados con los requisitos legales vigentes en la jurisdicción donde opera.
11. La propiedad intelectual, incluyendo patentes, derechos de autor, invenciones o cualquier tipo de información generada en el marco de las operaciones de **BANESCO BANCO MÚLTIPLE, S.A.**, será de propiedad exclusiva de la organización. Asimismo, la institución se compromete a respetar los derechos de autor y las licencias de uso de terceros, asegurando que únicamente se instale y utilice en los sistemas corporativos software licenciado y previamente aprobado por las áreas competentes.
12. Todo proyecto de desarrollo de aplicaciones o software, ya sea interno o externo, para **BANESCO BANCO MÚLTIPLE S.A.**, deberá contar con la definición clara de los roles y perfiles de usuario de acuerdo con los requerimientos establecidos por los propietarios del proyecto. Esta información deberá ser documentada en la Matriz de Perfiles de Usuario y sometida a revisión y validación por el área de Seguridad de la Información antes de la puesta en producción, asegurando el cumplimiento de principios de segregación de funciones y control de accesos.
13. Asegurar que los terceros que procesan información de **BANESCO BANCO MÚLTIPLE S.A.** o mantengan interconexión con sus sistemas o recursos tecnológicos cumplan con los lineamientos de confidencialidad, seguridad de la información y protección de datos corporativos, conforme a las políticas y normativas vigentes de la institución.
14. **BANESCO BANCO MÚLTIPLE S.A.** mantendrá e implementará estrictamente el principio de Segregación de Funciones (SoD) en todos los procesos de negocio y sistemas críticos garantizando que un mismo colaborador no tenga en su perfil de usuario, la capacidad de ser Gestor (creador/ejecutor) y Aprobador l(autorizado) de una misma transacción o proceso de control.

B. Responsabilidades de Seguridad Cibernética y de la Información

15. Desarrollar y actualizar los lineamientos para la seguridad de los datos, en función de los riesgos a los cuales se encuentra expuesta la Organización y acorde a las mejores prácticas, a fin de apoyar la implantación de un Modelo de Seguridad efectivo a lo largo del tiempo.

16. Establecer programas de capacitación y de transformación de la cultura en Seguridad Cibernética y de la Información dirigidos a todos sus colaboradores, incluyendo acciones específicas orientadas a concienciar y guiar a sus clientes externos sobre buenas prácticas de seguridad. Estos programas deberán garantizar la adopción de comportamientos seguros y la difusión de la importancia de la protección de la información tanto dentro como fuera de la organización.
17. Garantizar que cada colaborador, contratista o tercero que requiera acceso a los recursos de cómputo, sistemas y activos de información, posea una Identidad Digital Única e Inaplazable (Identificación personal). Dicha identidad deberá ser sometida a un proceso de autenticación robusto antes de conceder cualquier acceso.
18. Vigilar el estricto cumplimiento de las presentes **Políticas de Seguridad de la Información** y alertar de forma inmediata, cuando se detecte una violación a la misma, siendo esta regida por el **RE-DIS-0001 Reglamento Disciplinario por Incumplimiento de los Reglamentos, Normas, Procedimientos Y Políticas De La Organización**.
19. Revisar la Matriz de Perfiles de Usuarios, conforme lo establecido en el **PR-SI-0006 Procedimiento para la Revisión Recurrente Roles y Permisos de Aplicaciones**.
20. Se deberá conformar una mesa de trabajo integrada por el área experta solicitante y las áreas correspondientes de apoyo, con el propósito de evaluar solicitudes o casos específicos que presenten posibles conflictos o desviaciones en materia de segregación de funciones o asignación de roles. Dicha mesa será responsable de analizar los riesgos asociados desde la perspectiva de Seguridad de la Información y de definir las medidas correctivas o controles compensatorios necesarios para mitigar los impactos identificados.
 - a. De aprobarse la solicitud o el caso presentado de forma permanente, Capital Humano deberá actualizar el mapa descriptivo de la posición, y el área de Seguridad de la Información, la **Matriz de Perfiles de Usuarios**.
 - b. De aprobarse la solicitud o el caso presentado de forma temporal, se deberá especificar el tiempo de duración para fines de seguimiento, por parte del área de Seguridad de la Información.
21. Informar al Vicepresidente del área que corresponda el usuario experto citado en el artículo anterior, el resultado de la mesa de evaluadora.
22. Se deberá establecer y mantener una gestión integral de accesos para los colaboradores a los sistemas e infraestructuras tecnológicas de BANESCO BANCO MÚLTIPLE, S.A., definiendo límites, niveles de privilegio y controles adecuados que garanticen el principio de mínimo privilegio y la protección de los activos de información.
23. Implementar (o Gestionar) soluciones tecnológicas y mecanismos de seguridad para la prevención, detección y mitigación de amenazas, incluyendo software malicioso

(malware) e intrusiones, en los sistemas de información y la infraestructura tecnológica de BANESCO BANCO MÚLTIPLE, S.A.. Estas medidas deberán garantizar la confidencialidad, integridad y disponibilidad de los activos de información, así como un monitoreo continuo que permita responder de manera oportuna ante incidentes de seguridad.

C. Responsabilidades del Colaborador Banesco.

24. Todos los colaboradores de BANESCO BANCO MÚLTIPLE, S.A. Son responsables de garantizar la seguridad de la información bajo su manejo, considerando su clasificación, los riesgos asociados y las medidas de protección aplicables, asegurando que los activos de información se utilizan y gestionan de manera segura y conforme a los lineamientos institucionales.

25. Las áreas responsables de proyectos y nuevos requerimientos deberán asegurar la participación y apoyo de Seguridad de Información, en las actividades que impacten los procesos y áreas de negocio en función de los siguientes medios:

- Prueba y compensación.
- Red de sucursales.
- Medios de pago (Tarjetas).
- Canales Electrónicos (Cajeros Automáticos y Banca Virtual).
- Plataformas Corporativas de Sistemas e Infraestructura Tecnológica y Comunicaciones.

26. Todos los colaboradores de BANESCO BANCO MÚLTIPLE, S.A. deberán reportar de manera inmediata al buzón del equipo de Seguridad Cibernética y de la Información cualquier situación, incidente o evento que pueda comprometer los activos de información de la organización, garantizando así la detección oportuna y la protección de la información corporativa.

27. Se prohíbe abrir correos electrónicos provenientes de remitentes desconocidos o sospechosos, con el objetivo de prevenir la exposición a amenazas cibernéticas, incluyendo phishing, malware y otros ataques dirigidos. En caso de recibir un correo sospechoso, los colaboradores deberán:

- No interactuar con enlaces, archivos adjuntos o solicitudes contenidas en el mensaje.
- Reportar inmediatamente el correo al buzón o canal oficial del área de SCI.
- Eliminar el correo de manera segura siguiendo los procedimientos establecidos por la organización.

Estas acciones son obligatorias para proteger la información y los sistemas de BANESCO BANCO MÚLTIPLE, S.A. de posibles compromisos de seguridad.

28. No compartir información sensible o confidencial a través de las redes de la organización, tanto con personal interno como externo, salvo que exista autorización

expresa y se utilicen canales seguros aprobados por la organización para la transmisión de dicha información.

29. Todo colaborador de **BANESCO BANCO MÚLTIPLE, S.A.** deberá participar de manera obligatoria en los programas continuos de cultura y sensibilización sobre Seguridad Cibernética y de la Información, con el propósito de fortalecer la conciencia, responsabilidad y cumplimiento de las políticas y buenas prácticas establecidas por la institución.
30. Todo colaborador de **BANESCO BANCO MÚLTIPLE, S.A.** es responsable de identificar, gestionar y reportar los riesgos asociados al uso de los sistemas de información e infraestructura tecnológica dentro de su ámbito de trabajo, asegurando el cumplimiento de las políticas, procedimientos y controles de seguridad establecidos por la institución.

D. Seguridad Física y Ambiental

31. Todos los medios de procesamiento de información crítica o confidencial deberán mantenerse en áreas seguras, con perímetros, barreras físicas y controles de acceso establecidos. Se prohíbe el acceso no autorizado y los equipos deberán estar protegidos contra daño, interferencia o pérdida, asegurando la confidencialidad, integridad y disponibilidad de la información. La protección física de los equipos es obligatoria y su cumplimiento será supervisado y auditado periódicamente por las áreas correspondientes en la entidad.
32. Queda prohibido el ingreso de líquidos, alimentos u otros objetos no esenciales al centro de datos de BANESCO BANCO MÚLTIPLE, S.A.
33. Se restringe el ingreso de equipos electrónicos personales, tales como radios, televisores, reproductores de audio u otros dispositivos similares, en las áreas cercanas a los equipos del centro de datos, con el fin de prevenir interferencias, daños a la infraestructura tecnológica y garantizar la seguridad de la información.

E. Comunicaciones y Operaciones

34. Se deberán establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de información.
35. Los sistemas operacionales y de software de aplicación deberán estar sujetos a un estricto control gerencial del cambio.
36. Se deberán establecer las responsabilidades y procedimientos gerenciales formales para asegurar un control satisfactorio de todos los cambios en el equipo, software o procedimientos. Cuando se realizan los cambios, se deberá mantener un registro de auditoría conteniendo toda la información relevante.
37. Las actividades de desarrollo de sistemas se realizan en los entornos de desarrollo especializados, los cuales deben estar separados de los ambientes de producción y preproducción, y protegido contra el acceso no autorizado.
38. Se deberán proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y software se pueda recuperar después de un desastre o falla.
39. Los dispositivos de red deberán ser configurados para funcionar de acuerdo a su rol y se establecerán controles de seguridad para evitar cambios no autorizados.
40. Las redes deberán ser protegidas por controles físicos de seguridad, con el apoyo de documentación actualizada y el etiquetado de los componentes esenciales.
41. El acceso desde y hacia redes inalámbricas, será limitado a los usuarios y dispositivos autenticados y autorizados. El canal de transmisión debe ser cifrado para salvaguardar la información sensible en tránsito.
42. Todas las contraseñas y cuentas predeterminadas se deberán cambiar antes de la implementación del sistema.

F. Adquisición, desarrollo y mantenimiento de los sistemas de información

43. Los requerimientos del negocio, incluidos los de Seguridad Cibernética y de la Información, deberán ser contemplados durante la fase de especificaciones de requerimientos.
44. Los requisitos de Seguridad Cibernética y de la Información para los sistemas que estén en el ciclo de desarrollo, deberán ser considerados en el diseño de dichos sistemas y aplicaciones.
45. Los sistemas y aplicaciones en desarrollo deberán ser probados en una zona dedicada de pruebas que simulan el entorno de producción, antes de que el sistema o aplicación sea publicado en ambiente de producción.

46. Los sistemas y aplicaciones en desarrollo deberán ser sometidos a pruebas de Seguridad Cibernética en las fases requeridas dentro del ciclo de desarrollo, previo a su publicación en los ambientes de producción.
47. El acceso al código fuente de los sistemas y los paquetes asociados se deberán controlar estrictamente para evitar la introducción de una funcionalidad no autorizada y para evitar cambios no intencionados.
48. Se deberán documentar y hacer cumplir los procedimientos formales de control de cambio para minimizar la corrupción de los sistemas de información. La introducción de sistemas nuevos y los cambios importantes a los sistemas debieran realizarse después de un proceso formal de documentación, especificación, prueba, control de calidad e implementación manejada.

G. Gestión de incidentes de seguridad Cibernética y de la Información

49. Se deberán establecer y mantener procedimientos formales para el reporte, registro y escalamiento de eventos y debilidades de seguridad de la información. Todos los empleados deberán conocer y cumplir dichos procedimientos, garantizando que cualquier evento o debilidad que pueda afectar la seguridad de los activos organizacionales sea reportado de manera oportuna y conforme a los canales establecidos.
50. La capacidad de respuesta ante incidentes de Seguridad Cibernética y de la Información deberá sustentarse en un plan formalmente definido, el cual deberá contemplar las siete etapas del ciclo de gestión de incidentes:
 - Preparación, detección, análisis, contención, erradicación, recuperación, y actividad posterior al incidente.
51. Los incidentes de Seguridad Cibernética y de la Información deberán identificarse y clasificarse en diferentes niveles de gravedad para que el proceso de respuesta a incidentes sea más efectivo.
52. Los incidentes de Seguridad Cibernética y de la Información serán respondidos con los procedimientos apropiados basados en procesos organizacionales documentados.
53. Los eventos de Seguridad Cibernética y de la Información deberán ser reportados oportunamente a través de los canales oficiales establecidos. Todos los incidentes deberán ser registrados, monitoreados y rastreados durante todo su ciclo de vida, desde su detección hasta su resolución y cierre.
54. Establecer un equipo especializado para la gestión de incidentes, con roles y responsabilidades definidas. Este equipo debe tener autoridad para la toma de decisiones en situaciones críticas.
55. Se deberán utilizar múltiples fuentes internas y externas confiables para la obtención, análisis y actualización de información sobre amenazas, incluyendo aquellas de

alcance global, con el fin de fortalecer la capacidad de detección y respuesta ante posibles riesgos de seguridad.

56. La organización deberá mantener un esquema formal de recolección de información interna que incluya registros de eventos de sistemas operativos, alertas de soluciones de seguridad y datos proporcionados por las áreas de negocios, legales y de operaciones, con el fin de respaldar la gestión de riesgos y la seguridad de la información.

H. Responsabilidad de Tecnología

57. Implementar procesos y plataformas para la gestión segura de los componentes en las redes de información de **BANESCO BANCO MÚLTIPLE S.A.**
58. Registrar las aplicaciones de estaciones de trabajo en un inventario actualizado.
59. Establecer un proceso de gestión de desarrollo de sistemas, el cual contempla una metodología de desarrollo documentada y apegada a las mejores prácticas internacionales, tales como las Normas ISO, Proyectos OWASP, Normas NIST entre otras.
60. Adoptar un ciclo de vida para el desarrollo seguro de los sistemas y aplicaciones de Banesco Banco Múltiple.
61. Configurar los servidores físicos y virtuales de manera que se prevengan cambios y accesos no autorizados, garantizando la continuidad de los servicios y minimizando el riesgo de interrupciones derivadas de sobrecargas o fallas del sistema.
62. Los sistemas informáticos y equipos de la infraestructura tecnológica, deben ser registrados en un repositorio, el cual deberá permanecer actualizado.

I. Responsabilidad de Seguridad Física

63. Definir e implementar los mecanismos necesarios para garantizar la seguridad física y del entorno en las instalaciones críticas de BANESCO BANCO MÚLTIPLE, S.A., incluyendo aquellas que albergan sistemas de información, centros de datos, redes, equipos de telecomunicaciones, material físico sensible y demás activos relevantes.
64. Definir, documentar y mantener actualizado el Perfil de Seguridad de Localidad Física para cada una de sus ubicaciones operativas que contengan activos críticos.
65. Mantener un registro de entrada y salida, uso obligatorio de identificación, acceso limitado y bajo supervisión a áreas autorizadas, y el retorno obligatorio de los mecanismos de acceso físico (tarjetas, llaves).

J. Responsabilidades del Capital Humano.

66. Solicitar los accesos de todos los colaboradores que ingresen a BANESCO BANCO MÚLTIPLE, S.A., conforme a su posición, unidad organizativa y nivel organizacional.
67. Cualquier cambio de rol y/o permiso no contemplado en la Matriz de Perfiles de Usuario deberá ser revisado y evaluado por las áreas de Capital Humano, Riesgo y SCI, quienes serán responsables de su aprobación formal antes de su implementación, garantizando la adecuada segregación de funciones y el cumplimiento de los controles de acceso establecidos.
68. Informar al área de Seguridad Cibernética y de la Información sobre los cambios en roles, responsabilidades de los colaboradores de las distintas áreas, Vacaciones o Licencias, a fin de que mantengan actualizadas las informaciones, perfiles y permisología de los colaboradores en los diferentes sistemas de seguridad de información.
69. Notificar al área de Seguridad Cibernética y de la Información sobre la salida de cualquier colaborador de BANESCO BANCO MÚLTIPLE, S.A., con el fin de implementar los controles necesarios que garanticen la protección y resguardo de la información institucional, incluyendo la revocación oportuna de accesos y permisos en los sistemas y activos tecnológicos del banco.

K. Privacidad de la Información

70. Banesco Banco Múltiple, S.A. y todos sus colaboradores deberán cumplir con los lineamientos establecidos en la política **PO-SI-0002 Política Privacidad de la Información** relativos a la protección y privacidad de los datos, garantizando el tratamiento adecuado y seguro de la información bajo su responsabilidad.

L. Uso y Contratación de Servicios de Computación en la Nube

71. Los sistemas y aplicaciones contratados por BANESCO BANCO MÚLTIPLE, S.A. bajo modalidad de servicios en la nube deberán garantizar la protección de la información de acuerdo con los niveles de clasificación definidos por la organización. Asimismo, deberán especificar claramente el modelo de servicio (SaaS, IaaS, PaaS), el modelo de implementación, los mecanismos de seguridad y protección de la información, la gestión administrativa y los acuerdos de nivel de servicio (SLA) aplicables, asegurando el cumplimiento de los lineamientos institucionales de seguridad y control.
72. La presente Política de Uso Seguro de las Plataformas en la Nube aplica a todos los procesos, datos comerciales, sistemas de información, componentes tecnológicos, personal y áreas operativas de BANESCO BANCO MÚLTIPLE, S.A., que hagan uso, administración o gestión de servicios y recursos en entornos de computación en la nube.

73. La presente política aplica para todos los servicios de contratación en la nube privada, pública e híbrida, por Banesco Banco Múltiple S.A. Esto incluye todos los servicios de correo electrónico basados en la nube, hospedaje de servicios web, almacenamiento de documentos, Software como Servicio (SaaS), Plataforma con Servicio (PaaS), Infraestructura con Servicio (IaaS), entre otros.
74. La Gerencia de Seguridad Ciberseguridad y de la Información será responsable de revisar, analizar y comprender las políticas de seguridad del proveedor de servicios en la nube, con el fin de verificar su cumplimiento con los requerimientos de **BANESCO BANCO MÚLTIPLE, S.A.**, así como con las regulaciones locales y lo establecido en el Reglamento de Seguridad Cibernética y de la Información (RSCI).
75. Definir políticas y controles técnicos que impidan el uso de servicios de almacenamiento en la nube no aprobados por **BANESCO BANCO MÚLTIPLE, S.A.**, garantizando que únicamente se utilicen plataformas autorizadas y alineadas con los estándares de seguridad y cumplimiento establecidos por la institución.
76. Todo servicio contratado en la nube por **BANESCO BANCO MÚLTIPLE, S.A.** deberá contar con planes de continuidad del negocio y recuperación ante desastres, que aseguren la disponibilidad y operatividad del servicio en caso de incidencias o interrupciones, conforme a los requerimientos de resiliencia y seguridad establecidos por la institución.
77. El servicio contratado por **Banesco Banco Múltiple S.A.** deberá contar con mecanismos o herramientas que permitan realizar pruebas periódicas, a fin de validar la eficacia y eficiencia de los planes de continuidad establecidos o realizar los ajustes pertinentes según sea necesario.
78. Requerimientos a considerar para la contratación de servicio en la nube.
- Realizar auditorías de seguridad de manera regular,
 - Definir Acuerdo de Nivel de Servicios (SLA) ante incidentes presentadas,
 - Devolver la data del Banco y sus clientes en formato legible mediante medios seguros, en caso de terminación de contrato,
 - El banco puede revisar las auditorías y/o pruebas de seguridad que garanticen el cumplimiento de los controles de seguridad,
 - Brindar documentación a **Banesco Banco Múltiple S.A.** de los resultados de las pruebas de continuidad (BCP, DRP) y respuesta ante incidentes,
 - Ofrecer información en qué jurisdicción reposa la data del banco,
 - Disponer de una política de actualización y parches,
 - Garantizar servicios de autenticación robustos, con doble factor,

- Tener controles para la identidad y control de acceso en las cuentas de usuarios,
- La información debe estar cifrada para el tráfico desde y hacia la nube, o en el almacenamiento,
- Disponer de procedimientos de borrado o destrucción segura de los datos
- Tener productos de antimalware o detección de intrusos escaneado sus servidores,
- Política de divulgación responsable publicada por el proveedor,
- Habilitar los registros de eventos que pudieran permitir un análisis forense ante un incidente de seguridad.

M. Inteligencia Artificial y Ciberseguridad

79. El uso de tecnologías de Inteligencia Artificial (IA) en los procesos de ciberseguridad deberá estar alineado con los principios éticos institucionales de **BANESCO BANCO MÚLTIPLE, S.A.**, garantizando en todo momento el respeto a la privacidad, la transparencia, la imparcialidad y la no discriminación en su diseño, implementación y uso.
80. Se implementarán medidas estrictas para proteger la privacidad y los datos sensibles al utilizar la IA, especialmente en el análisis de grandes conjuntos de datos.
81. Los procedimientos para la transferencia de información entre los sistemas de IA y la infraestructura de seguridad vigente deben ser establecidos y verificados, garantizando que la comunicación esté protegida, verificada y permitida para preservar la integridad y privacidad de los datos.
82. La organización debe proporcionar capacitación y concientización a los empleados sobre el uso seguro y ético de la IA en ciberseguridad, así como sobre los riesgos asociados.

III. Glosario de Términos

N/A

IV. Anexos

- NR-SI-0002 Uso de Correo y Drive en Dispositivos Móviles y Estaciones de Trabajos
([ver aquí](#))

V. Aprobación del Documento

Unidad	Nombre, Apellido y Firma	Fecha
Elaborado por:		
Analista Optimización de Procesos	Danyeli Castro	04-nov-2025
Revisado por:		
Comité de Riesgos	-	17-nov-2025
Aprobado por:		
Consejo de Administración	-	20-nov-2025

VI. Historia de Cambios

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
01	Gerencia GPPC	Creación	N/A	-	Consejo de Administración 19-Jun-2015
02	GPPCN	Actualización	Se agrega: - La prohibición de la captura, grabación, reproducción o extracción de informaciones de BANESCO BANCO MÚLTIPLE S.A. a terceros o a equipos personales de colaboradores no autorizados. BANESCO BANCO MÚLTIPLE S.A. suministrará a sus colaboradores los equipos necesarios para el uso y conexión de la red local, en aras de satisfacer los requerimientos de seguridad establecidos, y velar por el aseguramiento de la información corporativa. - El bloqueo de los dispositivos de almacenamiento (CD o DVD ROM, USB u otros) de los equipos suministrados por BANESCO BANCO MÚLTIPLE S.A. - La prohibición del uso de equipos personales para la conexión a la red local de BANESCO BANCO MÚLTIPLE S.A.	Gerente GPPCN 12-Jul-18 VP Adm. Integral de Riesgo y GPPCN 13-Jul-2018 VP Capital Humano y Excelencia Organizacional 13-Jul-2018	Consejo de Administración 20-Jul-2018

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
			- La restricción de roles aprobadores por parte de usuarios que no formen parte de la misma área de trabajo. Igualmente, se priva a un usuario de no tener dentro de su perfil el rol de aprobador y gestor a la vez. - La realización de mesa de trabajo por parte de Seguridad de la Información junto a Capital Humano, Riesgo y el usuario experto para evaluar solicitudes o casos que presenten diferencias desde la óptica de seguridad de información, basado en análisis de la no segregación de funciones de roles y la generación de conflictos. - Las responsabilidades de Capital Humano de: - Solicitar los permisos correspondientes a los Colaboradores que ingresen al Banco, de acuerdo a la Matriz de Perfiles de Usuarios. - Revisión de cualquier cambio de rol y/o permiso no contemplado. - Informar al área de Seguridad de la Información sobre cualquier renuncia, despido, cambio de roles o responsabilidades de los colaboradores, a fin de mantener actualizadas las informaciones de perfiles y permisos.		
02	GPPCN	Actualización	Se elimina: Las responsabilidades de aseguramiento de la información asignadas al área de Continuidad del Negocio, quedando como responsable el área de Seguridad de la Información.	Gerente GPPCN 12-Jul-18 VP Adm. Integral de Riesgo y GPPCN 13-Jul-2018 VP Capital Humano y Excelencia Organizacional 13-Jul-2018	Consejo de Administración 20-Jul-2018
03	Gerencia GPPCN 01-Oct-2019	Actualización conforme Reglamento de Seguridad Cibernética y de la Información	Se adiciona: - Como responsabilidad del área de Seguridad Cibernética y de la Información. - Contemplar la gestión de los accesos de los colaboradores a los sistemas e infraestructura tecnológica, estableciendo los límites y controles para los accesos. - Limitar el acceso a las personas autorizadas, utilizando mecanismos de control de acceso que contemple los principios de menor privilegios y separación de funciones. - Implementar soluciones tecnológicas para el control y protección de software malicioso en los sistemas de información e infraestructura tecnológica de BANESCO BANCO MÚLTIPLE S.A. - Implementar soluciones tecnológicas o mecanismos de prevención y detección de intrusos, a fin de proteger los sistemas de BANESCO BANCO MÚLTIPLE S.A. - Como responsabilidad del Colaborador Banesco.	Gerencia de GPPCN y Continuidad del Negocio/ Vicepresidente de Administración Integral de Riesgo y GPPCN/ Comité de Riesgos	Consejo de Administración 20-nov-2019

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
			- No abrir correos electrónicos de remitentes desconocidos o sospechosos. - No compartir información sensible o confidencial a través de las redes de la organización a personal interno o externo. • En cuanto a la Seguridad Física y Ambiental: - Los medios de procesamiento de información crítica o confidencial deberán ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Deberán estar físicamente protegidos del acceso no autorizado, daño e interferencia. - La protección de los equipos será necesaria para reducir el riesgo de acceso no autorizado a la información y proteger contra pérdida o daño. - Estará prohibido ingresar con líquidos, alimentos u otro elemento no necesario para desarrollar las actividades en el centro de datos. - Estará restringido el ingreso de equipos electrónicos como radios, televisores o equipo de audio personales en las cercanías de los equipos del centro de datos. • En cuanto a las comunicaciones y operaciones. - Se deberán establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de información. - Los sistemas operacionales y de software de aplicación deberán estar sujetos a un estricto control gerencial del cambio. - Se deberán establecer las responsabilidades y procedimientos gerenciales formales para asegurar un control satisfactorio de todos los cambios en el equipo, software o procedimientos. Cuando se realizan los cambios, se deberán mantener un registro de auditoría conteniendo toda la información relevante. - Las actividades de desarrollo de sistemas se realizarán en los entornos de desarrollo especializados, los cuales deben estar separados de los ambientes de producción y preproducción, y protegido contra el acceso no autorizado. - Se deberán proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y software se pueda recuperar después de un desastre o falla. - Los dispositivos de red deberán ser configurados para funcionar de acuerdo a su rol		

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
			y se establecerán controles de seguridad para evitar cambios no autorizados. - Las redes deberán ser protegidas por controles físicos de seguridad, con el apoyo de documentación actualizada y el etiquetado de los componentes esenciales. - El acceso desde y hacia redes inalámbricas, será limitado a los usuarios y dispositivos autenticados y autorizados. El canal de transmisión debe ser cifrado para salvaguardar la información sensible en tránsito. - Todas las contraseñas y cuentas predeterminadas se deberán cambiar antes de la implementación del sistema. • En cuanto a la adquisición, desarrollo y mantenimiento de los sistemas de información - Los requerimientos del negocio, incluidos los de Seguridad Cibernética y de la Información, deberán ser contemplados durante la fase de especificaciones de requerimientos. - Los requisitos de Seguridad Cibernética y de la Información para los sistemas que estén en el ciclo de desarrollo, deberán ser considerados en el diseño de dichos sistemas y aplicaciones. - Los sistemas y aplicaciones en desarrollo deberán ser probados en una zona dedicada de pruebas que simulen el entorno de producción, antes de que el sistema o aplicación sea publicado en ambiente de producción. - Los sistemas y aplicaciones en desarrollo deberán ser sometidos a pruebas de Seguridad Cibernética en las fases requeridas dentro del ciclo de desarrollo, previo a su publicación en los ambientes de producción. - El acceso al código fuente de los sistemas y los paquetes asociados se deberán controlar estrictamente para evitar la introducción de una funcionalidad no autorizada y para evitar cambios no intencionados. - Se deberán documentar y hacer cumplir los procedimientos formales de control de cambio para minimizar la corrupción de los sistemas de información. La introducción de sistemas nuevos y los cambios importantes a los sistemas deberán realizarse después de un proceso formal de documentación, especificación, prueba, control de calidad e implementación manejada. • En cuanto a la gestión de incidentes de seguridad cibernética y de la información - Se establecerán procedimientos formales de reporte y de la intensificación de un evento.		

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
			Todos los empleados y terceros deberán estar al tanto de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener un impacto en la seguridad de los activos organizacionales. - Todos los empleados y terceros reportarán cualquier evento y debilidad de la seguridad de la información lo más rápido posible en el punto de contacto designado. - La capacidad de respuesta a incidentes de Seguridad Cibernética y de la Información deberá incluir un plan definido el cual debe abordar las siete etapas de respuestas a incidentes: - o Preparación, detección, análisis, contención, erradicación, recuperación, y actividad posterior al incidente. - Los incidentes de Seguridad Cibernética y de la Información deberán identificarse y clasificarse en diferentes niveles de gravedad para que el proceso de respuesta a incidentes sea más efectivo. - Los incidentes de Seguridad Cibernética y de la Información serán respondido con los procedimientos apropiados basados en procesos organizacionales documentados. - Los eventos de Seguridad Cibernética y de la Información deberán informarse a través de los canales adecuados. Los incidentes serán rastreados a medida que ocurran. ● Responsabilidad de Tecnología - Implementar procesos y plataformas para la gestión segura de los componentes en las redes de información de BBM. - Registrar las aplicaciones de estaciones de trabajo en un inventario actualizado.		

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
			- Establecer un proceso de gestión de desarrollo de sistemas, el cual contemple una metodología de desarrollo documentada y apegada a las mejores prácticas internacionales, entre ellas Normas ISO, Proyecto OWASP, Normas NIST, entre otras. - Adoptar un ciclo de vida para el desarrollo seguro de los sistemas y aplicaciones de Banesco Banco Múltiple. - Configurar los servidores físicos y virtuales para evitar cambios o accesos no autorizados, previniendo la interrupción de los servicios como resultado de una sobrecarga del sistema. - Los sistemas informáticos y equipos de la infraestructura tecnológica, deben ser registrados en un repertorio, el cual deberá permanecer actualizado. • Responsabilidad de Seguridad Física - Definir los mecanismos que provean las condiciones de seguridad física y del entorno adecuado de las instalaciones críticas, incluyendo lugares que albergan los sistemas de información, tales como centro de datos, redes, equipos de telecomunicaciones, material físico sensible y otros activos importantes. Deben ser protegidos contra accidente, ataques y accesos no autorizados. - Definir, documentar y actualizar los perfiles de seguridad de las localidades físicas, de los colaboradores internos, procesos, tecnologías utilizadas y ubicación asociados a sus localidades físicas. • Privacidad de la Información - Las informaciones recibidas por parte de nuestros clientes y usuarios podrán ser recopiladas, procesadas y conservadas en las bases de datos de BANESCO BANCO MÚLTIPLE S.A. siempre que se hayan recibido mediante los servicios y diferentes canales de comunicación que provea (Sucursales, BanescoOnline, CAT, Cajeros Automáticos, etc),		

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
			de manera que el Banco pueda tener registro de las transacciones realizadas. - Como usamos las informaciones recibidas por parte de nuestros clientes: ○ Personalización de contenido y experiencia de usuario ○ Identificar al cliente cuando utilice nuestra banca en línea ○ Configuración y administración de cuentas ○ Realizar encuestas, contenidos, etc. ○ Investigaciones de fraude y desarrollo interno ○ Recopilación de comentarios y opiniones sobre nuestros servicios ○ Notificación de cambios en nuestros productos/servicios ○ Notificación de ofertas de productos de créditos ○ Procesar sus transacciones Se modifica: ● Se amplía el alcance de la presente Política, adicionalmente criterios de la seguridad cibernética. En se sentido se cambia el nombre del documento a Política de Seguridad Cibernética y de la Información. Anteriormente solo poseía lineamientos de la seguridad de la información.		
04	Vicepresidencia Adm. Integral de Riesgos y GPPCN 10-feb-2020	Actualización	Se incluyen los siguientes lineamientos referentes al Uso y Contratación de Servicios de Computación en la Nube: - La presente política de uso seguro de las plataformas en la nube aplica a todos los procesos y datos comerciales, sistemas de información, componentes, y al personal y áreas físicas de Banesco Banco Múltiple S.A. - La presente política aplica para todos los servicios de contratación en la nube privada, publica e híbrida, por Banesco Banco Múltiple S.A. Esto incluye todos los servicios de correo electrónico basados en la nube, hospedaje de servicios web, el almacenamiento de documentos, Software como Servicio (SaaS), Plataforma con Servicio (PaaS), Infraestructura con Servicio (IaaS), entre otros. - La Unidad de Ciberseguridad será responsable de contemplar el desarrollo de un análisis de riesgo de Seguridad Cibernética y de la Información a los servicios contratados que incluya: ● Identificación de amenazas, ● Identificación de vulnerabilidades,	Vicepresidencia Adm. Integral de Riesgos y GPPCN/ Vicepresidencia Canales, Inteligencia de Negocios y Tecnología/ Comité de Riesgos 19-feb-2020	Consejo de Administración 19-mar-2020

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
			• Evaluación y tratamiento de riesgo. - La Unidad de Ciberseguridad será responsable de leer y comprender las políticas de seguridad del proveedor de servicios para asegurar que cumpla con las necesidades de Banesco Banco Múltiple S.A. y regulaciones locales de acuerdo a lo establecido en el Reglamento de Seguridad Cibernética y de la Información. - La Unidad de Ciberseguridad será responsable de elaborar y difundir una lista de los servicios de almacenamiento en la nube que estén permitidos y prohibidos por Banesco Banco Múltiple S.A. De esta forma se evitará el uso de servicios de almacenamiento que no se consideren seguros. - El servicio contratado por Banesco Banco Múltiple S.A. deberá contar con planes de continuidad del negocio, como garantía de disponibilidad en caso de incidencias. - El servicio contratado por Banesco Banco Múltiple S.A. deberá contar con mecanismos o herramientas que permitan realizar pruebas periódicas, a fin de validar la eficacia y eficiencia de los planes de continuidad establecidos o realizar los ajustes pertinentes según sea necesario. - Requerimientos a considerar para la contratación de servicio en la nube. • Realizar auditorías de seguridad regularmente, • Definición de Acuerdo de Nivel de Servicios (SLA) ante incidentes presentados, • En caso de terminación de contrato, la data del banco y sus clientes deberá ser devuelta a Banesco Banco Múltiple S.A. en formato legible mediante medios seguros, • El banco puede revisar las auditorías y/o pruebas de seguridad que garanticen el cumplimiento de los controles de seguridad, • Brindar documentación a Banesco Banco Múltiple S.A. de los resultados de las pruebas de continuidad (BCP, DRP) y respuesta ante incidentes, • Ofrecer información en que jurisdicción reposa la data del banco, • Disponer de una política de actualización y parches, • Garantizar servicios de autenticación robustos, con doble factor, • Tener controles para la identidad y control de acceso en las cuentas de usuarios, • La información debe estar cifrada para el tráfico desde y hacia la nube, o en el almacenamiento,		

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
			• Disponer de procedimientos de borrado o destrucción segura de los datos • Tener productos de antimalware o detección de intrusos escaneado sus servidores, • Política de divulgación responsable publicada, • Habilitar los registros de eventos que pudieran permitir un análisis forense ante un incidente de seguridad.		
05	Gerencia de Seguridad de la Información 04-nov-2025	Actualización	Se incluye: La gestión de la ciberseguridad y de la seguridad de la información en la organización se alinea con los marcos y metodologías de arquitectura empresarial, tales como TOGAF, con el fin de garantizar la integración coherente de la seguridad en todos los dominios tecnológicos y de negocio. La Arquitectura de seguridad de la organización podrá desarrollarse tomando como referencia la metodología TOGAF, asegurando la integración de los principios de ciberseguridad dentro del ciclo de vida de la arquitectura empresarial. BANESCO BANCO MÚLTIPLE S.A. mantendrá e implementará estrictamente el principio de Segregación de Funciones (SoD) en todos los procesos de negocio y sistemas críticos garantizando que un mismo colaborador no tenga en su perfil de usuario, la capacidad de ser Gestor (creador/ejecutor) y Aprobador I(autorizado) de una misma transacción o proceso de control. Todo colaborador de BANESCO BANCO MÚLTIPLE, S.A. deberá participar de manera obligatoria en los programas continuos de cultura y sensibilización sobre Seguridad Cibernética y de la Información, con el propósito de fortalecer la conciencia, responsabilidad y cumplimiento de las políticas y buenas prácticas establecidas por la institución. Todo colaborador de BANESCO BANCO MÚLTIPLE, S.A. es responsable de identificar, gestionar y reportar los riesgos asociados al uso de los sistemas de información e infraestructura tecnológica dentro de su ámbito de trabajo, asegurando el cumplimiento de las políticas, procedimientos y controles de seguridad establecidos por la institución. Banesco Banco Múltiple, S.A. y todos sus colaboradores deberán cumplir con los lineamientos establecidos en la política PO-SI-0002 Política Privacidad de la Información relativos a la protección y privacidad de los datos, garantizando el tratamiento adecuado y seguro de la información bajo su responsabilidad.	Especialista II Gobierno/Cumplimiento SCI y administración Ciberseguridad 04-Nov-2025 Analista Optimización de Procesos 13-Nov-2025	Comité de Riesgo 17-Nov-2025 Consejo de Administración 20-Nov-2025

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
			Inteligencia Artificial y Ciberseguridad El uso de tecnologías de Inteligencia Artificial (IA) en los procesos de ciberseguridad deberá estar alineado con los principios éticos institucionales de BANESCO BANCO MÚLTIPLE, S.A., garantizando en todo momento el respeto a la privacidad, la transparencia, la imparcialidad y la no discriminación en su diseño, implementación y uso. Se implementarán medidas estrictas para proteger la privacidad y los datos sensibles al utilizar la IA, especialmente en el análisis de grandes conjuntos de datos. Los procedimientos para la transferencia de información entre los sistemas de IA y la infraestructura de seguridad vigente deben ser establecidos y verificados, garantizando que la comunicación esté protegida, verificada y permitida para preservar la integridad y privacidad de los datos. La organización debe proporcionar capacitación y concientización a los empleados sobre el uso seguro y ético de la IA en ciberseguridad, así como sobre los riesgos asociados. Se modifica: Para los proyectos de desarrollo de aplicaciones o software, se sustituyó la referencia a los "propietarios del requerimiento" por "propietarios del proyecto" y se estableció que la información deberá ser documentada en la Matriz de Perfiles de Usuario, sometida a revisión y validación por el área de Seguridad de la Información antes de la puesta en producción. Asimismo, se incorporó la obligación de cumplir con los principios de segregación de funciones y control de accesos, reforzando los controles de seguridad en el proceso de desarrollo de aplicaciones o software. Establecer programas de capacitación y de transformación de la cultura en Seguridad Cibernética y de la Información dirigidos a todos sus colaboradores, incluyendo acciones específicas orientadas a concienciar y guiar a sus clientes externos sobre buenas prácticas de seguridad. Estos programas deberán garantizar la adopción de comportamientos seguros y la difusión de la importancia de la protección de la información tanto dentro como fuera de la organización. Anteriormente solo se indicaba a quienes estaba dirigido los programas.		

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
			Se deberá conformar una mesa de trabajo integrada por el área experta solicitante y las áreas correspondientes de apoyo, con el propósito de evaluar solicitudes o casos específicos que presenten posibles conflictos o desviaciones en materia de segregación de funciones o asignación de roles. Dicha mesa será responsable de analizar los riesgos asociados desde la perspectiva de Seguridad de la Información y de definir las medidas correctivas o controles compensatorios necesarios para mitigar los impactos identificados. Todos los colaboradores de BANESCO BANCO MÚLTIPLE, S.A. Son responsables de garantizar la seguridad de la información bajo su manejo, considerando su clasificación, los riesgos asociados y las medidas de protección aplicables, asegurando que los activos de información se utilizan y gestionan de manera segura y conforme a los lineamientos institucionales, anteriormente Los Vicepresidentes o Gerentes Funcionales tendrán la responsabilidad de velar por la adecuada seguridad de la información, en función de clasificación y los riesgos a los cuales se encuentran expuestos. Todos los colaboradores de BANESCO BANCO MÚLTIPLE, S.A. deberán reportar de manera inmediata al buzón del equipo de Seguridad Cibernética y de la Información cualquier situación, incidente o evento que pueda comprometer los activos de información de la organización, garantizando así la detección oportuna y la protección de la información corporativa, Las áreas deberán reportar al buzón de Seguridad de la Información las situaciones que comprometan los activos de la información de la Organización. Se prohíbe abrir correos electrónicos provenientes de remitentes desconocidos o sospechosos, con el objetivo de prevenir la exposición a amenazas cibernéticas, incluyendo phishing, malware y otros ataques dirigidos. En caso de recibir un correo sospechoso, los colaboradores deberán: • No interactuar con enlaces, archivos adjuntos o solicitudes contenidas en el mensaje. • Reportar inmediatamente el correo al buzón o canal oficial del área de SCI. • Eliminar el correo de manera segura siguiendo los procedimientos establecidos por la organización. Se fortalece las medidas de seguridad física aplicables a los medios de procesamiento de información crítica o confidencial. Se modificó la redacción para enfatizar el mantenimiento en áreas seguras, se incluyó la prohibición expresa del acceso		

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
			no autorizado y se amplió la protección a la pérdida de equipos. Además, se incorporaron los principios de confidencialidad, integridad y disponibilidad de la información, y se añadió la obligación de supervisión y auditoría periódica por las áreas correspondientes, con el fin de reforzar el control y la trazabilidad del cumplimiento. Se elimina: Las informaciones recibidas por parte de nuestros clientes y usuarios podrán ser recopiladas, procesadas y conservadas en las bases de datos de BANESCO BANCO MÚLTIPLE S.A. siempre que se hayan recibido mediante los servicios y diferentes canales de comunicación que provea (Sucursales, BanescOnline, CAT, Cajeros Automáticos, etc), de manera que el Banco pueda tener registro de las transacciones realizadas.		