Política de Seguridad Cibernética y de la Información

Código	PO-SI-0001
Edición Nº	04
Fecha	19-mar-2020

Contenido

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 a los controles de seguridad establecidos por la Norma ISO /IEC 27000, la cual provee mejores prácticas en el ámbito internacional y proporcionan las directrices requeridas para establecer un sistema confiable y flexible.

2. Objetivo y Alcance

La presente política ha sido diseñada con el objetivo de hacer de conocimiento a todos los Colaboradores de la organización de **BANESCO BANCO MÚLTIPLE, S. A.,** el compromiso acceso, uso y manejo de las informaciones de la Organización.

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.
- Proyectos OWASP, referente a las consideraciones de seguridad en los software de información.
- 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.

II. Políticas

A. Generales.

1. 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.

2. La información del negocio es un activo primordial de **BANESCO BANCO MÚLTIPLE S.A.** por lo tanto deberá ser protegida de acuerdo a la ón asignada.

3. Estará prohibido la captura, grabación, reproducción o extracción de informaciones de **BANESCO BANCO MÚLTIPLE S.A.** a terceros o a equipos personales de colaboradores no autorizados para tales fines.

4. 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 Seguridad de la Información.

5. **BANESCO BANCO MÚLTIPLE S.A.** suministrará a sus colaboradores los equipos necesarios (computadoras, celulares, u otros) para el uso y conexión de la red local en aras de satisfacer los requerimientos de seguridad establecidos al respecto, y velar por el aseguramiento de la información corporativa.

6. Los dispositivos de almacenamiento (CD o DVD ROM, USB u otros) de los equipos de **BANESCO BANCO MÚLTIPLE S.A.** estarán bloqueados para la entrada y salida de datos, con la finalidad de velar por el aseguramiento de la información dentro de la corporación, salvo justificación establecida y aprobada indicada en la **NR-SI-0006 Norma Excepción de Políticas de Seguridad.**

7. 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.

8. **BANESCO BANCO MÚLTIPLE S.A.** deberá cumplir con las regulaciones locales e internacionales de Privacidad y Seguridad de la Información.

9. La propiedad intelectual sobre patentes, derechos de autor, invenciones o información, generada durante la operación de la Organización, permanecerá en **BANESCO BANCO MÚLTIPLE S.A.**; de igual forma, la Institución respetará los derechos de autor y licencias de uso, para lo cual solamente software licenciado y aprobado debe ser cargado en los sistemas de la Organización.

10. Los sistemas y aplicaciones contratados por **BANESCO BANCO MÚLTIPLE S.A.** como servicios en la nube deberán garantizar aspectos de protección a la información en cuanto a niveles de clasificación, establecer el modelo de servicio (SAAS, IAAS, PAAS), modelos de implementación, protección de la información, gestión administrada y acuerdos de servicio.

11. Todo proyecto de aplicación o software desarrollado tanto interno como externo para **BANESCO BANCO MÚLTIPLE S.A.**, deberá tener definido los alcances de los roles y perfiles establecidos por los propietarios del requerimiento, los cuales deberán documentar a través de la Matriz de Perfiles de Usuario para revisión por parte de seguridad de la información.

12. No deberán existir roles aprobadores por parte de usuarios que no formen parte de la misma área de trabajo. Así mismo, un usuario no deberá tener dentro de su perfil el rol de aprobador y gestor a la vez.

B. Responsabilidades de Seguridad Cibernética y de la Información

13. 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.

14. Asegurar que los terceros que utilizan recursos de cómputo de **BANESCO BANCO MÚLTIPLE S.A.** cumplan con los lineamientos de confidencialidad y seguridad de la información.

15. Establecer los programas de capacitación y transformación de la cultura en Seguridad cibernética y de la Información para todos los colaboradores de **BANESCO BANCO MÚLTIPLE S.A.**

16. Dentro de su programa de capacitación y transformación de la cultura en Seguridad cibernética y de la Información, deberá desarrollar e incluir acciones específicas orientadas a sus clientes externos.

17. Proporcionar a los usuarios que acceden a la información de **BANESCO BANCO MÚLTIPLE S.A.**, un medio de identificación personal, que permita su autenticación en los recursos de cómputo, previo al uso de los activos de información de la institución.

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 está regida por el **RE-DIS-0001 Reglamento Disciplinario por Incumplimiento de los Reglamentos, Normas, Procedimientos Y Políticas De La Organización**.

19. Los riesgos a los cuales se encuentra expuesta la información de **BANESCO BANCO MÚLTIPLE S.A.**, deberán ser identificados, evaluados y mitigados acorde con su valor, probabilidad de ocurrencia e impacto en el negocio, por parte del área de Seguridad de la Información.

20. 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.**
21. Realizar mesa de trabajo conjuntamente con Capital Humano, Riesgo, y el usuario experto, para evaluar solicitudes o casos específicos 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.

    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.

22. Informar al Vicepresidente del área que corresponda el usuario experto citado en el artículo anterior, el resultado de la mesa de evaluadora.

23. Contemplar la gestión de los accesos de los colaboradores a los sistemas e infraestructura tecnológica, estableciendo los límites y controles para los accesos.

24. Limitar el acceso a las personas autorizadas, utilizando mecanismos de control de acceso que contemple los principios de menor privilegios y separación de funciones.

25. 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.**

26. Implementar soluciones tecnológicas o mecanismos de prevención y detección de intrusos, a fin de proteger los sistemas de **BANESCO BANCO MÚLTIPLE S.A**

C. Responsabilidades del Colaborador Banesco.

27. 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.

28. 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.

29. Las áreas deberán reportar al buzón de Seguridad de la Información las situaciones que comprometan los activos de la información de la Organización.

30. No abrir correos electrónicos de remitentes desconocidos o sospechosos.

31. No compartir información sensible o confidencial a través de las redes de la organización a personal interno o externo.

D. Seguridad Física y Ambiental

32. 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.

33. La protección de los equipos será necesaria para reducir el riesgo de acceso no autorizado a la información y proteger contra perdida o daño.

34. Estará prohibido ingresar con líquidos, alimentos u otro elemento no necesario para desarrollar las actividades en el centro de datos.

35. 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.

E. Comunicaciones y Operaciones

36. Se deberán establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de información.

37. Los sistemas operacionales y de software de aplicación deberán estar sujetos a un estricto control gerencial del cambio.

38. 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 auditoria conteniendo toda la información relevante.

39. 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.

40. 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.

41. 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.

42. Las redes deberán ser protegidas por controles físicos de seguridad, con el apoyo de documentación actualizada y el etiquetado de los componentes esenciales.

43. 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.

44. 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

45. Los requerimientos del negocio, incluidos los de Seguridad Cibernética y de la Información, deberán ser contemplados durante la fase de especificaciones de requerimientos.

46. 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.

47. 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.

48. 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.

49. 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.

50. 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

51. Se establecerán procedimientos formales de reporte y de la intensificación de un evento. 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.

52. 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.

53. 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:

    - Preparación, detección, análisis, contención, erradicación, recuperación, y actividad posterior al incidente.

54. 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.

55. Los incidentes de Seguridad Cibernética y de la Información serán respondido con los procedimientos apropiados basados en procesos organizacionales documentados.

56. 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.

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 contemple 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 para evitar cambios o accesos no autorizados, previniendo la interrupción de los servicios como resultado de una sobrecarga del sistema.

62. Los sistemas informáticos y equipos de la infraestructura tecnología, deben ser registrados en un repositorio, el cual deberá permanecer actualizado.

I. Responsabilidad de Seguridad Física

63. Definirá 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.

64. Definirá, documentará y actualizará los perfiles de seguridad de las localidades físicas, de los colaboradores internos, procesos, tecnologías utilizadas y ubicación asociados a sus localidades físicas.

J. Responsabilidades del Capital Humano.

65. Solicitar los permisos correspondientes de los Colaboradores que ingresen al Banco, de acuerdo a su rol establecido en la Matriz de Perfiles de Usuario.

66. Cualquier cambio de rol y/o permiso no contemplado será revisado por las áreas de Capital Humano, Riesgo y Seguridad de Información para que evalúe y apruebe.

67. Informar al área de Seguridad 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.

68. Notificar las salidas de colaboradores de **BANESCO BANCO MÚLITPLE S,A.,** al área de Seguridad de la Información, con la finalidad de establecer controles extras que aseguren las informaciones dentro de la institución.

    - Para los despidos, deberá informarlo desde que tenga su formalización.
    - Para las salidas voluntaria (renuncias), desde que la misma sea colocada.

K. Privacidad de la Información

69. Las informaciones recibidas por parte de nuestros clientes y usuarios podrán ser recopiladas, procesadas y conservadas en las bases de datos de **BANESCO BANCO MÚLITPLE 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.

70. Las informaciones recibidas por parte de los clientes podrán ser de utilidad para:

    - 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

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

71. 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.**

72. La presente política aplica para todos los servicios de contratación en la nube privada, publica e hibrida, 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.

73. 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,
    - Evaluación y tratamiento de riesgo.

74. 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.

75. 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.

76. 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.

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 auditorias 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,
- 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.

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:		
Dirección Planificación Estratégica y Excelencia de Procesos	Nicole M. Martínez T.	10-feb-2019
Revisado por:		
Vicepresidente de Administración Integral de Riesgo y GPPCN	Rolando Losada	12-feb-2020
Vicepresidente Canales, Inteligencia de Negocios y Tecnología	Deiniel Cárdenas	11-feb-2020
Comité de Riesgos	-	19-feb-2020
Aprobado por:		
Consejo de Administración	-	19-mar-2020

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.** • 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.	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
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	Consejo de Administración 20-Jul-2018

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
				VP Capital Humano y Excelencia Organizacional 13-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. - 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 perdida 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.	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
			- 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 auditoria 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 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.		

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
			- 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. • 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. 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. - 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.		

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
			- 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 tecnología, deben ser registrados en un reportorio, 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 MÚLITPLE 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. - Como usamos las informaciones recibidas por parte de nuestros clientes: o Personalización de contenido y experiencia de usuario o Identificar al cliente cuando utilice nuestra banca en línea o Configuración y administración de cuentas o Realizar encuestas, contenidos, etc. o Investigaciones de fraude y desarrollo interno o Recopilación de comentarios y opiniones sobre nuestros servicios o Notificación de cambios en nuestros productos/servicios o Notificación de ofertas de productos de créditos o 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.		

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
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 hibrida, 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, • 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,	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
			• El banco puede revisar las auditorias 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, • 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.		