8. Desarrollo y Mantenimiento de Sistemas

Política: Toda solución tecnológica que se implante en Banesco, debe haber sido construida de acuerdo con una metodología formal de desarrollo y mantenimiento de sistemas, que considere los requerimientos de Seguridad de la Información, durante todo su ciclo de vida, desde el diseño hasta la puesta en operación.

9. Continuidad del Negocio

Política: Todos los procesos críticos del negocio y los activos de información asociados, deben contar con un Plan de Continuidad del Negocio que permita a Banesco estar preparado para afrontar situaciones de contingencia y ataques contra la Seguridad de la Información.

10. Cumplimiento de las Políticas y de las Regulaciones vigentes

a) Cumplimiento de las Regulaciones

Política: Banesco debe cumplir con las regulaciones locales e internacionales de Privacidad y Seguridad de la Información.

b) Monitoreo de las Políticas de Seguridad de la Información

Política: Banesco debe vigilar el estricto cumplimiento de las presentes Políticas de Seguridad de la Información y alertar a la Organización en forma inmediata, cuando se detecte una violación a la misma.

c) Protección de la Propiedad Intelectual

Política: La propiedad intelectual sobre patentes, derechos de autor, invenciones o información, generada durante la operación de la Organización, permanecerá en Banesco; 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.

11. Administración del Riesgo de Seguridad

Política: Los riesgos a los cuales se encuentra expuesta la información de Banesco, deben ser identificados, evaluados y mitigados acorde con su valor, probabilidad de ocurrencia e impacto en el negocio.

Para mayor información llámenos al:
502.7041 / 502.9027/ 502.8358 / 502.9247

Banesco
BANCO UNIVERSAL

www.Banesco.com

SEGURIDAD DE LA INFORMACIÓN

PRINCIPIOS Y POLÍTICAS

La Información y la Tecnología son la clave para preservar el éxito de Banesco como Organización Financiera.

Nuestro liderazgo está basado en tradición e innovación, junto con el mejor talento humano y la más avanzada tecnología.

El programa de Seguridad de la Información, nos ayudará a ser más conscientes de nuestro deber de proteger uno de nuestros principales activos: La información.

Nos corresponde a todos asegurar que este programa sea un éxito.

Contamos con la participación de todos y cada uno de nosotros en este programa.

Principios

Se fundamentan en las mejores prácticas de Seguridad de la Información y estándares internacionalmente aceptados tales como el ISO 7498-2 e ISO 17799, que en conjunto con el Código de Ética de Banesco, definen los principios:

- Valores fundamentales de Banesco: Excelencia en el Servicio, Ética, Justicia y Equidad, Confidencialidad y Respeto Mutuo, así como los principios Institucionales establecidos al interior de la organización.
- El cumplimiento de las leyes aplicables: Venezolanas o extranjeras, regulaciones establecidas por entes gubernamentales que rigen la práctica del Sector Financiero Venezolano, así como las relacionadas con delitos y fraude informático.
- La protección de los bienes y activos de la organización, tanto físicos como de información, es una responsabilidad fundamental de aquellos a quienes se ha conferido la facultad de administrarlos o usarlos, constituye un deber disponer efectiva y racionalmente de los mismos, para el beneficio exclusivo de Banesco.
- La seguridad es una responsabilidad de todos los empleados de Banesco, que debe ser ejercida acorde con el rol y funciones desempeñadas en la Organización.

Políticas

1. Políticas de Seguridad de la Información

Las Políticas de Seguridad de la Información y los elementos que la soportan, deben ser desarrollados y mantenerse actualizados en función de los riesgos a los cuales se encuentra expuesta la Organización.

2. Organización de Seguridad

a) Organización y responsabilidades

Política: La Organización de Seguridad debe establecerse y mantenerse, acorde a las mejores prácticas, a fin de apoyar la implantación de un Modelo de Seguridad de la Información efectivo a lo largo del tiempo.

b) Terceros que acceden recursos de cómputo de Banesco local o remotamente

Política: Los Terceros que utilizan local o remotamente recursos de cómputo de Banesco deben cumplir con las Políticas de Seguridad de la información.

3. Clasificación y Control de Activos de Información

a) Responsables de los Activos de Información

Política: Todo activo de información de Banesco requiere la asignación de un Propietario, quien es responsable de velar por su adecuada seguridad, en función de su clasificación y los riesgos a los cuales se encuentra expuesto.

b) Clasificación de la información

Política: La información de Banesco 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.

c) Protección de la Información

Política: La información del negocio es un activo primordial de Banesco, por lo tanto debe ser protegida.

d) Uso de los recursos de cómputo de la Organización

Política: Los recursos de cómputo son provistos a los usuarios para uso exclusivo del negocio.

4. Seguridad del Personal

a) Capacitación y transformación de la cultura en Seguridad de la Información

Política: Banesco debe establecer un programa permanente de capacitación y transformación de la cultura en Seguridad de la Información.

b) Capacitación y transformación de la cultura en Seguridad de la Información de los Clientes de Banesco

Política: Banesco dentro de su programa capacitación y transformación de la cultura en Seguridad de la Información, debe incluir acciones específicas orientadas a sus Clientes.

c) Cumplimiento de las responsabilidades sobre la Seguridad de la Información

Política: Banesco debe proveer los mecanismos necesarios para asegurar que sus empleados cumplan con sus responsabilidades en Seguridad de la Información.

d) Reporte de Incidentes de Seguridad

Política: Banesco debe establecer un procedimiento para reportar incidentes de seguridad, el cual debe ser conocido por todos los usuarios de Banesco, quienes tienen la responsabilidad de utilizarlo cuando se presente una situación que comprometa los activos de información de la Organización.

5. Seguridad Física y Ambiental

a) Áreas Seguras

Política: Todas las áreas físicas del negocio deben tener un nivel de seguridad acorde con el valor de la información que se procesa y administra en ellas.

b) Manejo de Información clasificada

Política: La información clasificada debe ser mantenida en forma segura durante su uso en la operación diaria de Banesco, y permanecer en lugares con acceso restringido cuando no es utilizada.

6. Administración de Operaciones y Comunicaciones

Política: Los procesos para la Administración de las Operaciones y Comunicaciones deben cumplir con los requerimientos de mejores prácticas y estándares definidos por Banesco, con el fin de garantizar la continuidad de las plataformas operativas que soportan los procesos de gestión del negocio, dentro de los niveles de seguridad requeridos.

7. Control de Acceso a los Activos de Información

a) Identificación y Autenticación Individual

Política: Todos los usuarios que acceden a la información de Banesco deben disponer de 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.

b) Control y Administración del Acceso a la Información

Política: El acceso a los activos de información de Banesco 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.