Política Corporativa de Ciberseguridad Banesco (Panamá), S.A. y Subsidiarias

Edición Nº	2
Fecha	13/08/2020 (Comité de Cumplimiento, GC y Ética) 18/08/2020 (Junta Directiva)

Contenido

I. Introducción

Banesco (Panamá), S.A., como parte de sus medidas preventivas y correctivas en torno a situaciones que pudieran incidir en el buen funcionamiento del Banco, ha elaborado la presente Política Corporativa de Ciberseguridad, estableciendo los lineamientos para su gestión.

Lo anterior, considerando el auge que ha tenido la digitalización de los servicios financieros en los últimos años, la mayor interconectividad de los mismos; y la masificación en el uso de canales electrónicos, entre otros elementos, que han derivado en un incremento de la exposición a riesgos cibernéticos.

La presente Política es una disposición de la Junta Directiva de Banesco (Panamá), S.A. – Casa Matriz, la cual tiene alcance obligado tanto a sus Subsidiarias, así como a los colaboradores de la Organización.

Cualquier modificación y/o cambio a la misma, deberá ser aprobado por la Junta Directiva/Consejo de Administración y a su vez comunicado a la Casa Matriz. De igual forma, cualquier cambio y/o modificación a la misma por parte de Casa Matriz, deberá ser comunicado a las Subsidiarias, para su ratificación.

II. Información General de la Política

1. *Objetivo*

Esta política tiene como objetivo principal establecer los lineamientos y servir como marco de referencia para la gestión de asuntos de ciberseguridad, que permitan prevenir o mitigar los posibles eventos que se presenten; está alineada a la estrategia y a los objetivos del negocio procurando la protección de clientes y terceros que interactúan en el entorno del Grupo, tomando las mejores prácticas.

2. *Alcance*

Es aplicable a Banesco (Panamá), S.A. y Subsidiarias, en adelante el Grupo Bancario, respetando y tomando en consideración los lineamientos propios según la regulación y

jurisdicción propia de cada actividad desempeñada tanto por Banesco (Panamá), S.A. como por sus Subsidiarias.

III. Lineamientos

a. Generales

1. Promover la cultura y gestión en temas de ciberseguridad que involucre actividades relacionadas con la prevención de posibles eventos o acciones que puedan afectar o influir en los procesos internos o externos de la Organización.

2. Contar con lineamientos asociados a la gestión de ciberseguridad, que permitan prevenir posibles afectaciones, a través de los diferentes medios

3. Informar a la Junta Directiva y/o Consejo de Administración, así como a la Alta Gerencia, a través del Comité de Riesgo de las empresas del Grupo, con la periodicidad que éste considere; cualquier tema relacionado a ciberseguridad, especialmente, en la identificación de ciber-amenazas, resultados de la evaluación de efectividad de los programas de ciberseguridad, propuestas de mejora en materia de ciberseguridad, resumen de los incidentes de ciberseguridad, que hayan afectado de alguna manera el funcionamiento de la Organización, así como orientar sobre esta materia.

   Contar con la Estructura Organizativa necesaria, que se encargue o realice la gestión, relacionada a temas de ciberseguridad, y que la misma cuente con los mecanismos y recursos necesarios para sus funciones.

4. Considerar en los contratos que se celebren con terceros, las medidas y consideraciones pertinentes que permitan prevenir y/o mitigar que la Organización se vea afectada por temas de ciberseguridad.

5. Gestionar la ciberseguridad en cualquier iniciativa que involucre cambios tecnológicos.

b. Gestión de Prevención

Cada empresa debe contar con los controles adecuados para velar por la gestión de la ciberseguridad, conforme se dispone en los párrafos anteriores. Esto implica la capacidad de limitar o contener el impacto de un posible incidente de ciberseguridad, para lo cual deberá estimar:

1. Definir una estrategia de Seguridad y Ciberseguridad a través del establecimiento del portafolio de proyectos de seguridad que basados en el perfil de riesgo de la organización y su nivel de madurez permitan apoyar los objetivos de negocio, fortaleciendo paralelamente aspectos como gobierno, procesos, gestión de riesgos, prevención de fraude y la gestión de seguridad & ciberseguridad.

2. Establecer, documentar y brindar seguimiento a los controles de entrada y salida de información y gestión de identidades, bajo la premisa que las personas solo pueden disponer de los recursos que demande sus funciones, durante el tiempo que ello sea necesario o por duración de sus servicios en la Organización.

   Los colaboradores de la Organización deberán procurar el cumplimiento y aplicación de los lineamientos descritos en la presente política con lo cual se mitiga o se previene cualquier proceso de vulnerabilidad que afecte su gestión.

3. Identificar e informar, en la medida de lo posible, una vez detectados, cualquier riesgo cibernético emergente que pueda llegar a afectar al Grupo Bancario.

4. Considerar dentro de los Planes de Continuidad y Contingencia del Negocio, la respuesta y recuperación oportuna de la Organización frente a ataques cibernéticos.

   La Unidad de Auditoría de cada empresa deberá incluir dentro de sus procesos, la evaluación periódica de los procesos relacionados a ciberseguridad.

5. Incluir en los planes de Continuidad del Negocio pruebas (de intrusión o de cualquier otra que consideren), que simulen la materialización de posibles ataques.

6. Contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad.

7. De acuerdo a la estructura, canales de atención, volumen transaccional y número de clientes, monitorear diferentes fuentes de información; tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la entidad.

8. Informar periódicamente a los clientes, sobre las medidas de seguridad y recomendaciones que deberán adoptar para su ciberseguridad.

c. Protección y detección

El Grupo Bancario, conforme a las disposiciones de cada país donde mantiene presencia, debe desarrollar e implementar actividades que permitan identificar la ocurrencia de un evento de ciberseguridad. La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos, considerando:

1. Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de ciberseguridad que se presenten.

2. Gestionar las vulnerabilidades de aquellas plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.

3. Realizar un monitoreo continuo a su plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar posibles ciberataques contra el Grupo Bancario.

d. Respuesta y comunicación

Aún con las medidas de seguridad adoptadas, se deben desarrollar e implementar actividades para mitigar los incidentes relacionados con ciberseguridad. Para hacerle frente a esta situación el Grupo Bancario debe:

1. Establecer procedimientos de respuesta a incidentes cibernéticos tales como: desconexión automática de equipos, cambios de contraseñas, actualizar la base de firmas del antivirus, bloqueo de direcciones IP, entre otros.

2. Evaluar los elementos de la red para identificar otros dispositivos que pudieran haber resultado afectados.

3. Adoptar los mecanismos necesarios para recuperar los sistemas de información al estado en que se encontraban antes del ataque cibernético.

4. En la medida de lo posible, preservar las evidencias digitales para que las áreas de seguridad o las autoridades puedan realizar las investigaciones correspondientes.

IV. Cadena de valor de gestión de Prevención de Pérdidas

V. Glosario

- **Activo de información**

Conocimiento o datos que tienen valor para el Grupo Bancario o el individuo.

- **Ciber-amenaza o amenaza cibernética**

Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

- **Ciberataque o ataque cibernético**

Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.

- **Ciberespacio**

Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.

- **Ciber-riesgo o riesgo cibernético**

Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.

- **Ciberseguridad**

Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación del banco.

- **Evento de ciberseguridad**

Ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones del banco y que son esenciales para el negocio.

- **Grupo Bancario**

El constituido por una propietaria de acciones bancarias y sus subsidiarias de cualquier nivel cuyas actividades predominantes consisten en proveer servicios en el sector bancario o financiero, incluyendo las subsidiarias no bancarias de estas últimas que, a juicio de la Superintendencia, operen bajo gestión común, ya sea a través de esta propietaria de acciones bancarias o mediante distintas participaciones o convenios.

- **Incidente de ciberseguridad**

Ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de las empresas del Grupo Bancario y que son esenciales para el negocio.

- **Terceros críticos**

Terceros con quien se vincula el Grupo Bancario y que, de acuerdo con los parámetros establecidos por cada una de las empresas del Grupo, pueden tener incidencia directa en la seguridad de su información.

- **Vulnerabilidad**

Debilidad de un activo o control que puede ser explotado por una amenaza. Se tienen en cuenta todas aquellas amenazas que surgen por la interacción de los sistemas en el ciberespacio.

VI. Aprobación del Documento

Unidad	Nombre y Apellido	Fecha
Elaborado por:		
Especialista de Gobierno Corporativo	Ana Sofía Vega	29/07/2020
Revisado por:		
Gerente de Cumplimiento Normativo y Gobierno Corporativo Gerente de Seguridad de Información	Yaritsel Cruz Ian Pérez	29/07/2020 28/07/2020
Aprobado por:		
Comité de Cumplimiento, Gob. Corp. y Ética Junta Directiva	n/a	13/08/2020 18/08/2020

VII. Historial de Cambios

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
1	Vicepresidencia de Cumplimiento y Gobierno Corporativo	Con el objeto de robustecer las buenas prácticas en materia de Gobierno Corporativo, se consideró establecer una Política Corporativa de Ciberseguridad.	Elaboración de la Política.	Yaritsel Cruz Gerente de Cumplimiento Normativo y Gobierno Corporativo 29/10/2019	Junta Directiva 19/11/2019

Edición	Unidad Solicitante Fecha	Motivo	Descripción del Cambio	Revisado por Fecha	Aprobado por Fecha
2	Vicepresidencia de Cumplimiento y Gobierno Corporativo	Revisión anual 2020	Sección III Lineamientos, literal b. Gestión de Prevención, se incluyó el siguiente punto: 1. Definir una estrategia de Seguridad y Ciberseguridad a través del establecimiento del portafolio de proyectos de seguridad que basados en el perfil de riesgo de la organización y su nivel de madurez permitan apoyar los objetivos de negocio, fortaleciendo paralelamente aspectos como gobierno, procesos, gestión de riesgos, prevención de fraude y la gestión de seguridad & ciberseguridad.	Ian Pérez Gerente de Seguridad de Información 28/07/2020	Comité de Cumplimiento, Gob. Corp. y Ética 13/08/2020 Junta Directiva 18/08/2020