BANCO CENTRAL DE COSTA RICA

Políticas Específicas para la Seguridad de la Información

Políticas Específicas para la Seguridad de la Información

HISTORICO DE VERSIONES Y CONTROL DE CAMBIOS A LA POLITICA.

Versión:	**Fecha de creación:**	**Aprobado por:**	**Cambios realizados:**
7.0	30 de enero de 2025	Aprobación de la Gerente del Banco Central de Costa Rica	Se modifican las políticas P-2. a P-7., P-12., P-13. y P-15. a P-18., en línea con los requisitos de la norma INTE/ISO/IEC 27001:2023, la actualización a la política de alto nivel y para mejorar la redacción. Además, se amplía el alcance del sistema para incluir los activos de la División Transformación y Estrategia y se documentan los objetivos específicos del sistema, según lo aprobado en el informe de labores del Equipo de Seguridad de la Información (GER-0137-2024). Se incluye la política P-28. relacionada con el uso de herramientas de inteligencia artificial, carpetas compartidas, enlaces externos y otros que puedan comprometer la confidencialidad de la información. Finalmente, se realizan ajustes para mantener un lenguaje neutro y se estandariza el nombre del sistema como Sistema de Gestión de Seguridad de la Información.
6.0	13 de mayo de 2024	Aprobación del Gerente del Banco Central de Costa Rica	A partir de una revisión de las políticas, se actualizan las políticas P-26., P-28., P-29. y P-30., con mejoras en redacción y uso de términos. Ajustes en el nombre de la anterior División Gestión de Información.

5.0	24 de setiembre de 2022	Aprobación del Gerente del Banco Central de Costa Rica	Se modifica el nombre de las dependencias y se actualiza el alcance, en línea con los cambios aprobados en el acuerdo de Junta Directiva de la sesión 6038-2021, artículo 11, celebrada el 9 de diciembre del 2021 relacionados con la propuesta de cambio organizacional titulada "Transformación Organizacional de seis dependencias del Banco Central". En la política P-3, se actualiza el nombre de las Políticas específicas de gestión documental y se agregan las Políticas Específicas de Seguridad Tecnológica PCI-DSS. Se actualizan las políticas P-9 y P-19, con la nomenclatura vigente para los procesos y metodologías de capacitación. Se actualiza la numeración a partir de la política P-21. Se modifican las políticas P-4, P-16 y P-21, y se incorpora la política P25, en atención a la implementación del etiquetado de activos. Se eliminan los controles C-20.1, C-23.1, C-23.2 y C-23.3 y se incluye lo pertinente en las políticas P-21 y P-24.
4.0	17 de enero del 2022	Aprobación del Gerente del Banco Central de Costa Rica	Se incorpora la política P-25 incluyendo la referencia a la necesidad de que algunos funcionarios firmen un acuerdo de confidencialidad. Además, se ajusta la numeración de las siguientes políticas. En la política P-26, se amplía la descripción del nivel de confidencialidad "máxima seguridad" indicando que la información relacionada con tarjetas de crédito debe ser definida en dicho nivel.
3.0	5 de noviembre de 2018	Aprobación del Gerente del Banco Central de Costa Rica	Se incorporan las políticas P-25, P-26 y P-27, donde se incluyen la especificación de los niveles de confidencialidad, integridad y disponibilidad en la valoración de los activos de información.
2.0	4 de mayo de 2017	Aprobación del Director de la División Gestión y Desarrollo	Modificación de la redacción del control **C-20.1.,** para ser consistente con las políticas específicas de Gestión de Riesgos No Financieros.
1.0	11 de enero de 2016	Aprobación del Gerente del Banco Central de Costa Rica	Oficialización y publicación de las políticas.

Consideraciones que sustentan la emisión de estas políticas específicas:

A. La Junta Directiva aprobó las Políticas de Alto Nivel para seguridad de la información mediante el artículo 16 del acta de la sesión 5441-2009.

B. La Gerencia es la responsable de la aprobación de las políticas específicas derivadas de las políticas de alto nivel aprobadas por la Junta Directiva.

C. Estas políticas responden a la norma internacional ISO/IEC 27001.

D. Se deroga la Resolución de Gerencia 30-2014 en donde se estableció el Comité del Sistema de Gestión de Seguridad de la Información y se designó a la División Transformación y Estrategia como responsable de coordinar con las demás divisiones y desarrollar las políticas requeridas.

E. Las políticas específicas aquí contenidas han sido revisadas y aprobadas por sus responsables; satisfacen el esquema definido para la creación de políticas específicas, controles y lineamientos y cuentan con el visto bueno de la División Transformación y Estrategia en cuanto a forma y estandarización.

Políticas Específicas para la Seguridad de la Información

I. Aspectos generales

P-1. La Gerencia del Banco Central de Costa Rica establece estas políticas específicas de Seguridad de la Información para atender el marco de gestión que responde a la política de alto nivel, sobre Seguridad de la Información, establecida por la Junta Directiva.

P-2. La Gerencia del Banco Central de Costa Rica instaura la estructura para establecer, operar, evaluar y mejorar el Sistema de Gestión de Seguridad de la Información institucional mediante una estructura de gobierno basada en las mejores prácticas internacionales, con el fin de asegurar la protección de los activos de información del Banco Central de Costa Rica de usos no autorizados, modificación, daños o destrucción accidental o intencional.

P-3. Debido a la amplitud de los elementos que componen el Sistema de Gestión de Seguridad de la Información, el marco normativo se complementa con las siguientes políticas y elementos, adicionales a la presente política:

- **Políticas específicas para la seguridad tecnológica**: en cuanto a la gestión de la seguridad de la infraestructura tecnológica.
- **Políticas específicas de gestión de riesgos no financieros**: en cuanto a la identificación, valoración y tratamiento del riesgo asociado a los activos de información.
- **Políticas específicas de continuidad del negocio**: en cuanto a aspectos relacionados con la continuidad del negocio.
- **Código de Ética**: en cuanto al tratamiento de la información por parte de las personas funcionarias.
- **Políticas específicas de gestión de información**: para la adecuada gestión de la información.
- **Políticas específicas de gestión documental** para la adecuada conservación de los recursos de información.
- **Políticas específicas de capacitación**: para el desarrollo y actualización de conocimientos asociados al tema.
- **Políticas Específicas de Seguridad Tecnológica PCI-DSS:** para los servicios de la División de Servicios Tecnológicos que soportan la gestión del ambiente sujeto a cumplimiento de la certificación PCI Council PCI-DSS.
- **Políticas Específicas para la Seguridad Administrativa del Banco Central de Costa Rica:** relacionadas con los controles de seguridad física dentro de las instalaciones.

P-4. Con el fin de garantizar la adecuada interpretación de los aspectos relacionados con Seguridad de la Información se definen los siguientes términos:

- **Activo de información:** todo aquello que tenga valor informativo, para la organización, con respecto a la seguridad de la información.
- **Disponibilidad:** la cualidad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Confidencialidad:** la cualidad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Seguridad de la información:** la preservación de la confidencialidad, integridad y disponibilidad de los activos de información.

- **Etiqueta de confidencialidad:** es un sello que se aplica a un activo de información para declarar su nivel de confidencialidad. De acuerdo con el nivel de confidencialidad que posea el activo, podrá contener elementos adicionales de protección.
- **Evento de seguridad de la información:** la ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de salvaguardas, o una situación previamente desconocida que pueda ser relevante para la seguridad.
- **Gestor o cogestor del grupo de acceso:** es la persona designada por cada dependencia para administrar las etiquetas y los grupos autorizados para acceder a cada activo de información.
- **Grupo de acceso:** son las personas que cada dependencia define que están autorizadas para utilizar el activo de información.
- **Sistema de gestión:** el conjunto de elementos (personas, sistemas manuales o automatizados, normativa y otros) que interactúan de manera sistémica para el logro de la adecuada gestión institucional en términos de eficiencia y eficacia.
- **Sistema de gestión de la seguridad de la información:** la parte del sistema de gestión global, basada en un enfoque hacia los riesgos del Banco, para establecer, implementar, operar, dar seguimiento, evaluar, mantener y mejorar la seguridad de la información.
- **Integridad:** la cualidad de salvaguardar la exactitud y estado completo de los activos.
- **Aceptación del riesgo:** la decisión de asumir un riesgo.

P-5. La Gerencia del Banco Central de Costa Rica declara como alcance del Sistema de Gestión de Seguridad de la Información y de estas políticas la cobertura de los activos de información de las divisiones: Gestión de Activos y Pasivos, Sistemas de Pago, Económica y Análisis de Datos y Estadísticas, y Transformación y Estrategia, valorados como críticos en términos de confidencialidad, correspondiendo a los niveles máxima seguridad y confidencial, con el fin de hacer un uso estratégico de la inversión de fondos públicos en el aseguramiento de los activos de información más valiosos de la organización, de conformidad con la declaración de aplicabilidad de los controles vigente. Los límites de este alcance incluyen el edificio central del Banco Central de Costa Rica y las instalaciones ubicadas en Moravia.

P-6. La Gerencia del Banco Central de Costa Rica declara como objetivo del Sistema de Gestión de Seguridad de la Información la implementación de un enfoque sistémico para establecer, operar, evaluar y mejorar la seguridad de la información de la organización para ayudar a alcanzar los objetivos organizacionales. Para lo cual establece como objetivos específicos:

- Identificar y clasificar los activos de información, con el fin de protegerlos de acuerdo con su nivel de confidencialidad y preservar la información vital de la organización.
- Prevenir, reducir o mitigar a niveles aceptables los riesgos de uso no autorizado a los que está expuesta la información del BCCR, contribuyendo al cumplimiento de los objetivos de la organización y a mantener la confianza de las partes interesadas.
- Fortalecer la cultura en seguridad de la información, por parte de las personas funcionarias y terceros que tengan acceso a información confidencial del BCCR, con el fin de contribuir a la aplicación correcta de las políticas de seguridad de la información.
- Prevenir incumplimientos normativos, legales o contractuales a través del monitoreo del cumplimiento de las políticas en materia de seguridad de la información.
- Mantener la mejora continua del SGSI a través de la atención oportuna y eficaz de los planes de acción, con el fin de fortalecer la conformidad del sistema.

P-7. La Gerencia del Banco Central de Costa Rica brinda el apoyo necesario para lograr la

asignación de los recursos presupuestarios requeridos para el adecuado establecimiento, operación, evaluación y mejora del Sistema de Gestión de Seguridad de la Información.

P-8. La Gerencia del Banco Central de Costa Rica establece que estas políticas son de acatamiento obligatorio para todas las personas funcionarias de la institución, a fin de garantizar el logro de los objetivos establecidos para el Sistema de Gestión de Seguridad de la Información, así como para asegurar que todas las actividades dentro de la organización se ejecutan de acuerdo con lo establecido por estas políticas. Su no cumplimiento será sancionado de acuerdo con lo que establece el Reglamento Autónomo de Servicios.

P-9. Los incidentes de seguridad se gestionan de acuerdo con lo establecido en el proceso Atención de incidentes de seguridad tecnológica disponible en el Sitio de Calidad.

P-10. Los cambios a estas políticas deben ser comunicados y difundidos a toda la organización por parte de la División Transformación y Estrategia para su conocimiento y acatamiento.

II. Aspectos organizativos

P-11. La Gerencia del Banco Central de Costa Rica establece el Comité Gerencial como responsable de velar por la adecuada gestión de la seguridad de la información del Banco.

P-12. La Gerencia del Banco Central de Costa Rica establece que el Comité Gerencial para atender temas relacionados con Seguridad de la Información está integrado por la Gerencia y por los Directores de las divisiones, Gestión de Activos y Pasivos, Sistemas de Pago, Económica, Servicios Tecnológicos, Transformación y Estrategia y Análisis de Datos y Estadísticas, con el objetivo de velar por el adecuado establecimiento, operación, evaluación y mejora continua del Sistema de Gestión de Seguridad de la Información a nivel institucional.

P-13. Las responsabilidades del Comité Gerencial son:

- Velar que los objetivos de la seguridad de información sean identificados, relacionarlos con las exigencias organizacionales y que sean integrados en procesos relevantes.
- Velar por la revisión y actualización de las políticas específicas de seguridad de la información al menos cada dos años para mantener la vigencia del sistema, con respecto a cambios en el entorno y las necesidades de las partes interesadas, así como otros requerimientos de mejora que se detecten.
- Validar la actualización de políticas específicas de Gestión de la seguridad de la información, así como de los controles y lineamientos derivados de ellas.
- Revisar la efectividad del Sistema de Gestión de Seguridad de la Información en términos de reducción de incidentes relacionados.
- Revisar el desempeño del Sistema de Gestión de Seguridad de la Información con respecto al logro de los objetivos, al menos una vez al año, y retroalimentar al Equipo de Apoyo en Seguridad de la Información.
- Proveer direcciones claras y un visible apoyo en la gestión para iniciativas de seguridad de la información.

- Apoyar planes y programas para mantener la concientización y actualización en seguridad de la información.
- Velar porque el Sistema de Gestión de Seguridad de la Información esté alineado con el Plan Estratégico del Banco Central de Costa Rica, así como de la Gestión Integral de Riesgos.
- Gestionar revisiones independientes, de tercera parte, de la Seguridad de la Información cuando se considere necesario.
- Gestionar contacto con grupos de interés especial de expertos o con amplio conocimiento en el área de Seguridad de la Información cuando se considere necesario.

P-14. La Gerencia del Banco Central de Costa Rica establece el Equipo de Apoyo en Seguridad de la Información como apoyo al Comité Gerencial, para coordinar la implementación de las acciones necesarias para la adecuada gestión de la seguridad de la información dentro de la organización.

P-15. El Equipo de Apoyo en Seguridad de la Información está integrado por un representante de cada una de las divisiones del Banco, y es coordinado por la División Transformación y Estrategia, con el objetivo de articular las acciones necesarias para el establecimiento, operación, evaluación y mejora continua del Sistema de Gestión de Seguridad de la Información a nivel institucional.

P-16. Las responsabilidades del Equipo de Apoyo en Seguridad de la Información son:

- Identificar los objetivos de la seguridad de la información, según las exigencias organizacionales, e integrarlos en los procesos relevantes.
- Proponer, revisar y mantener actualizadas las políticas específicas de seguridad de la información y presentarlas a la Gerencia para su aprobación y oficialización, al menos cada dos años.
- Evaluar y proponer para aprobación del Comité Gerencial los controles derivados del abordaje de los riesgos del Sistema de Gestión de Seguridad de la Información.
- Evaluar el Sistema de Seguridad de la Información acorde con las políticas específicas de seguridad de la información y las buenas prácticas internacionales, e informar anualmente al Comité Gerencial sobre su desempeño.
- Implementar las directrices e iniciativas de seguridad de la información que respondan a las directrices establecidas por el Comité Gerencial.
- Proponer y ejecutar planes y programas para mantener la concientización y actualización de las personas funcionarias del Banco Central de Costa Rica en seguridad de la información.
- Asegurar la implementación de los controles de la seguridad de información, incluyendo la gestión de las etiquetas de confidencialidad para los activos de información dentro del alcance.
- Velar por que en la contratación de servicios con terceros se incluya como parte de los acuerdos los aspectos de confidencialidad, y el cumplimiento de controles y lineamientos que aseguren los requerimientos de Seguridad de la Información que se deben satisfacer.

- Establecer la frecuencia de reuniones, la cual no debe ser inferior a una por año.
- Coordinar la ejecución de una campaña de refrescamiento sobre aspectos de Seguridad de la Información al menos una vez al año con el fin de mantener el apego de la ejecución de tareas al cumplimiento de los aspectos relacionados con seguridad de la información.
- Informar al Comité Gerencial sobre las necesidades de recursos, formación u otras relacionadas con el desarrollo de competencias en el personal, para el adecuado funcionamiento del Sistema de Gestión de Seguridad de la Información.

P-17. La División Transformación y Estrategia, mediante el Departamento de Calidad y Mejora Continua, es responsable de:

- Coordinar la implementación de los esfuerzos organizacionales acordados por el Comité Gerencial a fin de mantener la adecuación del Sistema de Gestión de Seguridad de la Información a los requerimientos del BCCR.
- Actualizar la declaración de aplicabilidad de los controles, cuando surjan cambios en estos, presentarla a la Gerencia para su aprobación y oficialización, y coordinar su comunicación a todas las personas funcionarias.
- Establecer la metodología para evaluar y mejorar el Sistema de Gestión de Seguridad de la Información, para aprobación de la Gerencia, y definir una guía para su aplicación.

III. Aspectos de implementación y gestión

P-18. La División Transformación y Estrategia incluye como parte de la Intranet institucional un espacio exclusivo para el Sistema de Gestión de Seguridad de la Información a fin de conservar toda aquella información relacionada con el sistema, entre otra, la declaración de aplicabilidad de los controles, el inventario de activos controlados, los informes de labores y las minutas de reunión de los comités.

P-19. La División Transformación y Estrategia debe impartir una capacitación básica sobre seguridad de la información como parte del proceso de inducción al personal de nuevo ingreso a fin de que estas personas conozcan el marco normativo aplicable y las facilidades relacionadas con el Sistema de Gestión de Seguridad de la Información.

P-20. La División Transformación y Estrategia brinda los mecanismos necesarios para realizar la clasificación de los recursos de información correspondientes a los registros generados por la ejecución de los procesos dentro del alcance establecido y que se custodian en la Intranet institucional, en términos de confidencialidad, integridad y disponibilidad, así como el plazo de conservación del recurso con el fin de facilitar a los dueños de los activos su clasificación.

P-21. Los dueños de los procesos dentro del alcance establecido aseguraran la consideración de los siguientes aspectos en su definición para el cumplimiento de la seguridad de la información:

- Los riesgos asociados a los activos de información se gestionan considerando lo dispuesto en las Políticas Específicas para la Gestión de Riesgos no Financieros.

- La especificación del periodo de conservación de cada uno de los activos de información identificados.
- Especificar claramente el responsable de cada activo de información.
- Especificar los controles del proceso que garantizan el cumplimiento de los niveles de confidencialidad, integridad y disponibilidad de cada activo de información.
- Para aquellos activos cuyo nivel de confidencialidad corresponda a los niveles de máxima seguridad y confidenciales, asegurar que se incluyen como parte del inventario de activos de Seguridad de la Información, que se designe a un gestor y cogestor de los grupos acceso y se determine el grupo de acceso para cada activo de información.
- Coordinar con el gestor y cogestor la actualización de los grupos de acceso para cada activo de información.
- Como parte de la revisión anual de los procesos solicitada por la División Transformación y Estrategia se debe hacer una revisión de los aspectos anteriores.

P-22. Las divisiones y departamentos definidos en el alcance de esta política establecen y comunican a la División Servicios Compartidos los requerimientos de control de acceso físico, protección de áreas y las personas autorizadas para acceder a estos espacios a fin de que esta última implemente los controles y mecanismos necesarios para asegurar las áreas de trabajo.

P-23. La División Servicios Compartidos establece los mecanismos necesarios para la vigilancia y revisión de los servicios públicos y del abastecimiento de combustible para la operación del generador alterno, con el fin de garantizar la continuidad en la prestación de estos servicios.

P-24. Las divisiones y departamentos definidos en el alcance de esta política establecen y comunican a la División Servicios Tecnológicos los requerimientos de seguridad de acceso y protección lógica de los recursos de información a fin de que esta última implemente los controles y las políticas necesarios para asegurar su debida protección. Incluyendo los mecanismos necesarios para el uso adecuado de los equipos móviles que se facilitan al personal, los mecanismos necesarios para la devolución de equipos a los proveedores, y los lineamientos necesarios para prevenir el daño a los equipos tecnológicos de procesamiento de información por consumo de alimentos y bebidas cerca de ellos, con el fin de prevenir posibles daños o pérdida de información valiosa.

P-25. Las dependencias definidas en el alcance de esta política establecen y comunican a la División Transformación y Estrategia, las personas gestoras y cogestoras de los grupos de acceso, así como las personas que pertenecen a cada grupo de acceso, a fin de que esta última coordine la implementación de las etiquetas necesarias para asegurar la debida protección de los activos declarados como máxima seguridad y confidencial.

P-26. Los directores de división cubiertos por el alcance instruyen al personal a su cargo para no dejar información de acceso restringido a la vista de terceros de manera que se prevenga la fuga de información valiosa.

P-27. El personal del Banco o terceros que tengan acceso a información confidencial por medio de los diferentes canales de Atención al Cliente, deben suscribir un acuerdo de confidencialidad comprometiéndose de esta manera a no divulgar datos o información a terceros, ni utilizarla

para beneficio personal. La División Transformación y Estrategia llevará el control de todos los acuerdos de confidencialidad firmados como parte de la gestión de Seguridad de la Información.

P-28. El personal del BCCR no deberá compartir o gestionar datos o información en cualquier formato, que se encuentren clasificados de acuerdo con el nivel de confidencialidad, como: de uso interno, propietario, confidencial o de máxima seguridad; mediante aplicaciones en línea como servicios de inteligencia artificial, carpetas compartidas, enlaces externos, o cualquier otro medio que no corresponda con las herramientas oficiales de la institución.

P-29. El Banco Central de Costa Rica establece los niveles de confidencialidad para especificar el nivel requerido en el análisis de los activos de información, para lo cual se aplica la siguiente escala:

- Público: El activo es de dominio público. No hay ningún impacto si hay acceso ilimitado. La seguridad a este nivel es mínima.
- Uso interno: El acceso al activo no aprobado de manera generalizada fuera de la organización, de suceder, la situación incomodaría a la organización o a la Gerencia, pero es poco probable que dé lugar a pérdidas financieras o a un daño serio a la credibilidad o imagen de la organización. La seguridad a este nivel debe ser controlada pero normal.
- Propietario: El acceso al activo es normalmente para el uso del personal autorizado solamente. La seguridad a este nivel es alta.
- Confidencial: Activos que se consideran críticos para las operaciones de la organización y podría impedirlas si se comparten o se publican. Estos activos no deben ser duplicados (en caso de ser posible) y jamás deben salir del control de la organización sin una autorización previa. La seguridad para estos activos debe ser muy alta.
- Máxima seguridad: Activos de uso interno de acceso altamente restringido. Los activos clasificados como de "Máxima Seguridad" siempre se deben proteger. La seguridad a este nivel es la más alta posible. La información relacionada con tarjetas de crédito debe ser catalogada en este nivel.

P-30. El Banco Central de Costa Rica establece los niveles de integridad para especificar el nivel requerido en el análisis de los activos de información, para lo cual se aplica la siguiente escala:

- Baja: La alteración o modificación de los datos en este activo representa un riesgo bajo. No importa si los datos son alterados o modificados. En caso de alteración o modificación no se tendrán consecuencias de ningún tipo para la organización.
- Media: La alteración o modificación de los datos en este activo representa un riesgo medio. Tiene importancia la alteración o modificación de datos, pero no representa un riesgo elevado para la organización. En caso de alteraciones, se pueden afectar algunos servicios, pero no de manera generalizada.
- Alta: La alteración o modificación de los datos en este activo representa un alto riesgo para la organización. En caso de alteraciones la organización puede llegar a serios incumplimientos legales, sufrir pérdidas patrimoniales o de imagen considerables o experimentar una afectación considerable de los objetivos.

P-31. El Banco Central de Costa Rica establece los niveles de disponibilidad para especificar el nivel requerido en el análisis de los activos de información, para lo cual se aplica la siguiente

escala:

- Baja: El activo puede no estar disponible hasta por una semana sin que exista ninguna afección en los servicios en donde se utiliza.
- Media: El activo puede no estar disponible hasta por un día completo sin que exista ninguna afectación en los servicios en donde se utiliza.
- Alta: El activo puede no estar disponible hasta por un máximo de 4 horas sin que se produzcan fallas o incumplimientos críticos para la organización.
- Muy alta: Bajo ninguna circunstancia el activo puede dejar de estar disponible ya que cualquier fallo o retraso en la prestación del servicio en que se utiliza podría llevar a la organización a serios incumplimientos legales, pérdidas patrimoniales, de imagen considerables o afectación ostensible de objetivos.