CUARTO SUPLEMENTO

REGISTRO OFICIAL®
ÓRGANO DE LA REPÚBLICA DEL ECUADOR

**CORPORACIÓN FINANCIERA NACIONAL**
**BANCA PÚBLICA**

**REGULACIÓN DIR-054-2022**

# APRUÉBESE LA REFORMA DE LAS POLÍTICAS INSTITUCIONALES PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, CON LA MODIFICACIÓN EN EL TEXTO DEL ANEXO 1

Año I - Nº 166 - 110 páginas
Quito, martes 11 de octubre de 2022

**REGULACIÓN DIR-054-2022**

**EL DIRECTORIO DE LA**
**CORPORACIÓN FINANCIERA NACIONAL BANCA PÚBLICA**

**CONSIDERANDO:**

Que, el artículo 226 de la Constitución establece el principio de legalidad, mismo que señala: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley."*

Que, el artículo 2 del Decreto Ejecutivo 868, publicado en el Registro Oficial N° 676 de fecha 25 de enero del 2016, con el que se reorganiza a la Corporación Financiera Nacional B.P., señala que dicha institución es: *"una entidad financiera pública, dedicada al financiamiento del sector productivo de bienes y servicios, así como proyectos de desarrollo en el ámbito nacional e internacional. Buscará estimular la inversión productiva e impulsar el crecimiento económico sostenible, a través de apoyo financiero o no financiero a los sectores productivos, de bienes y servicios; así como de proyectos que contribuyan a la mejora de la competitividad nacional*."

Que, el numeral 12 del artículo 375 del Código Orgánico Monetario y Financiero, señala que es competencia del Directorio: "Aprobar los reglamentos internos".

Que, la Gerencia de Seguridad de la Información, mediante memorando Nro. CFN-B.P.-GDSI-2022-0363-M de 14 de septiembre de 2022, señala:

> *"Mediante Regulación No. DIR-032-2020, publicada el 5 de febrero de 2021, se oficializó la creación de la Gestión de Seguridad de la Información, en la Corporación Financiera Nacional B.P., dentro del "PROYECTO DE REDISEÑO DE ESTRUCTURA ORGANIZACIONAL Y ACTUALIZACIÓN DEL ESTATUTO ORGANIZACIONAL POR PROCESOS".*
>
> *La Gerencia de Seguridad de la información cuya misión es: "Dirigir y administrar la normativa, procedimientos en materia de Seguridad de la información estableciendo mecanismos y ejecutando controles para su cumplimiento contribuyendo al desarrollo de los procesos que se realizan en la Corporación Financiera Nacional B.P", debe hacer esfuerzos a fin de alinearse a los objetivos institucionales mediante el establecimiento de las disposiciones normativas y buenas prácticas en materia de seguridad de la información.*
>
> *El CASI (Comité de Administración de seguridad de la información) en sesión celebrada del 25 al 30 de agosto de 2022, aprobó por unanimidad, mediante correo electrónico, los 4 temas propuestos de la agenda. Los miembros con voz y voto que constituyen el CASI son: el Eco. Iván Andrade, Presidente; Eco. Virna Rossi, Gerente General (e) e Ing. Steven Ganchozo, Gerente de Riesgos (e) y miembros con voz y sin voto, el Ing. Jorge Carvajal, Gerente de Tecnologías de la información y como Secretaria del Comité, la Ing. Ilse Ycaza, Gerente de seguridad de la información (e). constan sus firmas en Acta.*

***MARCO NORMATIVO***

*Estatuto Orgánico de Gestión Organizacional por Procesos de la CFN B.P., para la Gerencia de seguridad de la información, Atribuciones y responsabilidades.*

*1. Proponer y ejecutar mejoras en el proceso de Gestión de Seguridad de la Información*

*2. Elaborar y presentar al Comité de Seguridad de la Información para su posterior aprobación por parte del Directorio, las estrategias, políticas, procesos y*

*3. procedimientos alineados al negocio y a los organismos de control desde la perspectiva de la confidencialidad, integridad y disponibilidad de la información*

*4. Planificar, organizar y proponer cambios en la Política de seguridad de la información, desde la perspectiva de la confidencialidad, integridad y disponibilidad de la información, así como controlar que los procedimientos de la Política de Seguridad de la Información se cumplan por parte de los funcionarios de la CFN B.P. a nivel nacional.*

*5. Revisar y aprobar los planes de acción para la mitigación de riesgos y su presentación al Comité de Seguridad de la Información;*

*6. Convocar regularmente o cuando la situación lo amerite al Comité de Seguridad de la Información así como llevar registros de asistencia y actas de las reuniones*

***Política Institucional para la Administración de la normativa CFN B.P.**, Libro Preliminar: Generalidades de la Normativa CFN B.P., Título I: Disposiciones Normativas CFN B.P., Subtítulo I: Política Institucional para la Administración de la Normativa CFN B.P., Capítulo III: De las Responsabilidades: Artículo 8. PARA LA NORMATIVA GENERAL: Serán responsables las siguientes instancias:*

***8.1. Área promotora:** Motivará el requerimiento de eliminación, modificación o inclusión al instrumento normativo vigente, generando para el efecto el informe técnico con la argumentación e insumos técnicos pertinentes; requerirá informes dentro de sus respectivas competencias a la Gerencia Jurídica y Gerencia de Calidad. Una vez obtenidos los mismos con carácter de favorables, procederá a remitir la documentación a la Gerencia General y secretaría General, junto con el memorando de solicitud para aprobación del Directorio de la Corporación Financiera Nacional B.P. En caso que la normativa general deba ser aprobada por un Comité, delegado por el Directorio de la Corporación Financiera Nacional B.P., procederá a dirigir la documentación el Secretario del Comité.*

***DESARROLLO***

*En cumplimiento de la normativa institucional antes citada, la Gerencia de Seguridad de la información, ha gestionado la revisión de las políticas, procesos y procedimientos alineados al negocio y a los organismos de control desde la perspectiva de la confidencialidad, integridad y disponibilidad de la información y puestas a consideración del Comité de Administración de seguridad de la información, lo que se indica a continuación:*

***Actualización de la Política institucional del sistema de Gestión de Seguridad de la Información, con la modificación del texto del Anexo 1 – Acuerdo de confidencialidad (interno)***

*Mediante memorandos CFN-B.P.-GEJU-2022-0515-M, CFN-B.P.-GERI-2022-0495-M y CFN-B.P.-GECA-2022-0341-M, las gerencias Jurídica, Riesgos y Calidad respectivamente, proceden a ratificar la conformidad de la propuesta a la reforma de la Política institucional del sistema de gestión de seguridad de la información, con la modificación del texto del anexo 1 – acuerdo de confidencialidad (interno) planteada por parte de la Gerencia de Seguridad de la Información. En la sesión del CASI, del 25 al 30 de agosto de 2022, se dio por conocido y aceptado este punto de la agenda, por todos los miembros del Comité."*

Que, la economista Virna Rossi Flores, Gerente General (E), dispone dentro de la agenda de Directorio, se presente para conocimiento y aprobación del Directorio, la Reforma de las Políticas Institucionales para el Sistema de Gestión de Seguridad de la Información con la modificación en el texto del Anexo 1, contenido mediante memorando de recomendación Nro. CFN-B.P.-GDSI-2022-0363-M de 14 de septiembre de 2022.

Debidamente motivado, en ejercicio de sus atribuciones.

**RESUELVE:**

**Artículo 1.-** Aprobar la Reforma de las Políticas Institucionales para el Sistema de Gestión de Seguridad de la Información, con la modificación en el texto del Anexo 1.

## SUBTITULO I: POLÍTICAS INSTITUCIONALES PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

### INDICE

CAPÍTULO I: GENERALIDADES .....
CAPÍTULO II: DE LA SEGURIDAD DE LOS RECURSOS HUMANOS.....
CAPÍTULO III: DE LA SEGURIDAD FÍSICA Y DEL ENTORNO.....
CAPÍTULO IV: DE LA GESTIÓN DE COMUNICACIONES Y OPERACIONES .....
CAPÍTULO V: DEL CONTROL DE ACCESOS .....
CAPÍTULO VI: DE LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS .....
CAPÍTULO VII: SOBRE EL USO DE FIRMAS ELECTRÓNICAS.....
CAPÍTULO VIII: DE LA GESTIÓN DE LA CONTINUIDAD DE LOS NEGOCIOS .....
CAPÍTULO IX: DEL CUMPLIMIENTO.....
CAPÍTULO X: DEL ACUERDO DE PRIVACIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES .....
CAPÍTULO XI: DE LA ADMINISTRACIÓN DE CONTRASEÑAS .....
CAPÍTULO XII: MONITOREO PERIÓDICO DE ACCESOS, OPERACIONES PRIVILEGIADAS E INTENTO DE ACCESOS NO AUTORIZADOS.....
CAPÍTULO XIII: RELACIÓN CON PROVEEDORES ASOCIADOS AL TRATAMIENTO DE INFORMACIÓN EN SITUACIONES DE CONTRATAR SERVICIOS DE TRATAMIENTO O RESGUARDO DE ACTIVOS DE INFORMACIÓN .....
CAPÍTULO XIV: IDENTIFICACIÓN Y DOCUMENTACIÓN DE LOS REQUERIMIENTOS Y CONTROLES MÍNIMOS DE SEGURIDAD PARA CADA ACTIVO DE INFORMACIÓN EN BASE A UNA EVALUACIÓN DE RIESGOS.....
CAPÍTULO XV: DEFINICIÓN Y VERIFICACIÓN DE REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA NUEVOS SISTEMAS O SU MANTENIMIENTO.....
CAPÍTULO XVI: DETECTAR Y EVITAR LA INSTALACIÓN DE SOFTWARE NO AUTORIZADO O SIN LICENCIA; Y, PARA INSTALAR Y ACTUALIZAR PERIÓDICAMENTE APLICACIONES DE DETECCIÓN Y DESINFECCIÓN DE VIRUS INFORMÁTICOS Y DEMÁS SOFTWARE .....
CAPÍTULO XVII: TRAER SU PROPIO DISPOSITIVO (BYOD, BRING YOUR OWN DEVICE).....

CAPÍTULO XVIII: ELIMINACIÓN DE LA INFORMACIÓN CRÍTICA DE LA ENTIDAD, DE MANERA SEGURA Y CONSIDERANDO LOS REQUERIMIENTOS LEGALES Y REGULATORIOS .....
CAPÍTULO XIX: PROTEGER LA INFORMACIÓN CONTENIDA EN: DOCUMENTOS, MEDIOS DE ALMACENAMIENTO U OTROS DISPOSITIVOS EXTERNOS E INTERCAMBIO ELECTRÓNICO, CONTRA: ROBO, UTILIZACIÓN O DIVULGACIÓN NO AUTORIZADA DE INFORMACIÓN .....
CAPÍTULO XX: SEGMENTACIÓN DE LA RED DE DATOS, SELECCIÓN/AJUSTES DE SISTEMAS Y CONTROL DE ACCESOS. .....
CAPÍTULO XXI: CIFRAR INFORMACIÓN REQUERIDA COMO RESULTADO DEL ANÁLISIS DE RIESGOS. .....
CAPÍTULO XXII: TELETRABAJO.....
CAPÍTULO XXIII: SEGURIDAD DEL ALMACENAMIENTO EN LA NUBE .....
CAPÍTULO XXIV: DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN .....
CAPÍTULO XXV: DEL INTERCAMBIO DE INFORMACIÓN INTERNA Y CON TERCEROS .....
CAPÍTULO XXVI: DE LA GESTIÓN DE ACTIVOS DE INFORMACIÓN Y SU USO ACEPTABLE.....
CAPÍTULO XXVII: DE LA GESTIÓN DE CAMBIOS DE TI .....
CAPÍTULO XXVIII: DISEÑAR, MONITOREAR, PISTAS DE AUDITORÍA EN APLICATIVOS Y BASES DE DATOS.....
CAPÍTULO XXIX: CONTROL DEL ESCANEO AUTOMATIZADO DE VULNERABILIDADES EN CÓDIGO FUENTE .....
CAPÍTULO XXX: MONITOREAR LA EFECTIVIDAD DE LOS NIVELES DE SEGURIDAD IMPLEMENTADOS EN HARDWARE, SOFTWARE, REDES Y COMUNICACIONES.....
CAPÍTULO XXXI: PRINCIPIO DE INGENIERÍA EN SISTEMAS SEGUROS .....
CAPÍTULO XXXII: GESTIÓN DE LOS REPORTES DE MONITOREO EMITIDO POR SOC Y ALARMAS ANTIMALWARE – ANTIVIRUS - ANTIPHISHING .....
CAPÍTULO XXXIII: MONITOREAR, CONTROLAR Y EMITIR ALARMAS EN LÍNEA QUE INFORMEN OPORTUNAMENTE SOBRE EL ESTADO DE LOS CANALES ELECTRÓNICOS .....
CAPÍTULO XXXIV: ANEXOS .....

## CAPÍTULO I: GENERALIDADES

**Artículo 1.- OBJETIVO:**

Preservar la información y garantizar su integridad, confidencialidad y disponibilidad, a través de reglas, normas o directrices “marco” que se deben respetar para proteger los recursos de información de la CFN B.P. y la tecnología utilizada para su procesamiento, de tal manera de minimizar los riesgos que le afectan.

A continuación se detallan los objetivos específicos de las Políticas Institucionales de Seguridad de la Información:

1. Establecer los lineamientos de alto nivel con respecto al correcto uso de los recursos de información (tanto en la creación, almacenamiento, uso, procesamiento, transferencia y destrucción), así como de las medidas que se deben adoptar para su protección.
2. Determinar las medidas de alto nivel de seguridad de la información que la institución debe adoptar, para protegerse apropiadamente contra riesgos o amenazas que podrían afectar a la confidencialidad, integridad y disponibilidad de la información, como por ejemplo:

- Pérdida o mal uso de los activos de información.
- Pérdida de imagen corporativa.
- Interrupción a la continuidad del negocio.

3. Proteger los recursos de información de la CFN B.P. y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información, así como, contribuir a la continuidad del negocio.
4. Asegurar la consecución de los objetivos de seguridad contemplados en esta Política mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).
5. Hacer patente el compromiso de la Gerencia General en relación a la seguridad de la información, en consonancia con la estrategia del negocio.
6. Brindar un tratamiento adecuado a los riesgos de Seguridad de la Información que se identifiquen, de tal manera que se ejecuten los planes respectivos hasta llegar al nivel de aceptación del riesgo establecido por la Institución.

7. Definir, desarrollar e implantar los controles técnicos y organizativos que resulten necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada por la CFN B.P.
8. Garantizar el cumplimiento de la legislación vigente en materia de protección de datos de carácter personal y sociedad dela información, así como de todos los requerimientos legales, reglamentarios, normativos y contractuales que resulten aplicables.
9. Crear una cultura de seguridad de la información y concientizar a todo el personal de la Institución, como externamente, en relación con los clientes y proveedores de CFN B.P., de tal manera que conozcan las responsabilidades para su cumplimiento
10. Considerar la seguridad de la información como un proceso de mejora continua, que permita alcanzar niveles de seguridad cada vez más avanzados.

**Artículo 2.- ALCANCE:**

Las disposiciones de la presente Política son de aplicación obligatoria en todo el ámbito de la Corporación Financiera Nacional B.P., al personal y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o convenios con terceros; son de aplicación obligatoria para todos los responsables de acuerdo a la estructura orgánica por procesos de la Institución.

Los principios y acciones de esta Política deben ser reconocidos y de estricto cumplimiento por todo el personal que produce, gestiona, administra y resguarda activos de información en el ejercicio de sus funciones.

La política debe ser concienciada, observada, comunicada y cumplida por todos los funcionarios y colaboradores, sean estos empleados directos, externalizados o servicios profesionales, y por entidades externas como proveedores o entidades de control los cuales tengan relación con los prestadores de servicios.

**Artículo 3.- RESPONSABLES:**

a) Todos los responsables de las unidades administrativas, deben dar cumplimiento a las Políticas Institucionales de Seguridad de la Información y fomentar su cumplimiento dentro de sus equipos de trabajo, de tal manera de garantizar un adecuado manejo de la seguridad de la información en lo que se refiere a la confidencialidad, integridad y disponibilidad de la información.

b) El Comité de Administración de la Seguridad de la Información, es responsable de evaluar las políticas Institucionales de seguridad de la información y someterlas a aprobación del Directorio; proponer al Directorio modificaciones a las Políticas Institucionales de Seguridad de la Información que sean del caso; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación de incidentes relativos a la seguridad; recomendar la aplicación de las principales iniciativas, estrategias y metodologías para incrementar la seguridad de la información.

c) El Comité de Tecnología es responsable del control y mantenimiento del plan estratégico de tecnología de información, el cual entre otros debe observar las Políticas Institucionales de Seguridad de la Información, a fin de garantizar la continuidad de las operaciones, el proceso de adquisición, desarrollo, implementación y mantenimiento de aplicaciones, la infraestructura tecnológica, la provisión de recursos y servicios informáticos de terceros y, la integridad, confidencialidad y disponibilidad de información de la CFN B.P.

d) La Gerencia de Seguridad de la Información, es responsable de dirigir y administrar la normativa, procedimientos en materia de Seguridad de la Información, estableciendo mecanismos y ejecutando controles para su cumplimiento, contribuyendo al desarrollo sostenido de los procesos que se realizan en la Corporación Financiera Nacional B.P.

e) Los propietarios de la información son responsables de identificar y clasificar la información acorde al grado de sensibilidad y protegerla adecuadamente; deben documentar y mantener actualizada la clasificación efectuada; definir, aprobar y revisar periódicamente los roles de acceso a las aplicaciones de su responsabilidad, y especificar la asociación de dichos roles con los diferentes cargos y competencias de los funcionarios; adicionalmente deben aprobar los permisos de acceso a los sistemas e información de acuerdo a las funciones o roles especiales de los usuarios, independientemente del cargo; autorizar la creación, mantenimiento y/o eliminación de funcionalidad (controles de cambios) que involucren a las aplicaciones de su responsabilidad; complementariamente deben supervisar y aplicar estrategias y controles para que la información contenida en los sistemas de aplicación y datos, sean de óptima calidad (la Gerencia de Seguridad de la Información puede hacer recomendaciones orientadas en mejorar la calidad de la información).

f) La Gerencia de Talento Humano es responsable de notificar a todo el personal que ingresa a prestar sus servicios profesionales en la CFN B.P., sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y todas las normas, procedimientos y prácticas que de ella surjan. De igual manera, tiene a su cargo la notificación de la presente Política a todo el personal, los cambios que en ella se produzcan, la suscripción de los Acuerdos de Confidencialidad (Anexos 1 y 3); y, las tareas de capacitación continua en materia de seguridad en coordinación con la Gerencia de Seguridad de la Información.

g) La Gerencia de Tecnologías de la Información es responsable de implementar los requerimientos de seguridad de la información establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnologías de la información de la Corporación Financiera Nacional B.P. Por otra parte, tiene la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

h) La Gerencia Jurídica debe asesorar en el cumplimiento de las normas del ordenamiento jurídico vigente, nacionales e internas aplicables en operaciones, actos y contratos, emitiendo los criterios jurídicos que fueran necesarios y en el cumplimiento de las directrices y políticas, que estén relacionadas con la Seguridad de la Información.

i) Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente dentro del ámbito de sus competencias.

j) La Gerencia de Auditoría Interna Bancaria y la Gerencia de Auditoría Interna Gubernamental son responsables de practicar auditorias periódicas sobre los sistemas de información y actividades vinculadas con la tecnología de información, debiendo comunicar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

***Acceso de Terceros***

a) Las personas de la Institución que tengan relación con "terceros", deben poner en conocimiento las Políticas Institucionales, para su cumplimiento obligatorio, por ejemplo la gestión de contraseñas; gestión de activos; de la seguridad de los recursos humanos; de la seguridad física y del entorno; gestión de comunicaciones y operaciones, del control de accesos; de la adquisición, desarrollo y mantenimiento de sistemas; de la gestión de incidentes de seguridad de la información y de todos los aspectos de esta política.

b) Cuando exista necesidad de acceso físico de terceros a las instalaciones de procesamiento de información, el acceso debe ser controlado y las acciones supervisadas todo el tiempo por personal de la Institución. No se dará acceso mientras no se hayan implementado los controles apropiados y se haya firmado un contrato que defina las condiciones de reserva y sigilo para la conexión, acceso y manipulación de información.

c) Cuando exista necesidad del negocio que involucre una conexión con un sitio externo, debe llevarse a cabo una evaluación de riesgos para identificar los requerimientos de controles específicos. Ésta debe tener en cuenta el tipo de acceso requerido, el valor de la información, los controles empleados por la tercera parte y la incidencia de este acceso en la seguridad de la información de la Institución.

d) No se debe otorgar a terceros acceso a la información ni a las instalaciones de procesamiento mientras no se hayan implementado los controles apropiados y se haya firmado un contrato que defina las condiciones de reserva y sigilo para la conexión, acceso y manipulación de información.

**Artículo 4.- BASE LEGAL:**

- Constitución de la República del Ecuador, Registro Oficial No 449 del 20 de octubre de 2008.
- Ley de Comercio Electrónico, Firmas y Mensajes de Datos, Ley No 67 publicada en el Registro Oficial Suplemento No 557 del 17 de abril de 2002.
- Codificación de las Normas de la Superintendencia de Bancos. LIBRO I Normas de Control para las Entidades de los Sectores Financieros Públicos y Privado. TITULO IX De la Gestión y Administración de Riesgos. Capítulo V Norma de Control para la Gestión del Riesgo Operativo (Capítulo sustituido por la Resolución No. SB-2018-771 de 30 de julio de 2018; reformado por Resolución No. SB-2018-814 de 13 de agosto de 2018; reformado por Resolución No. SB-2019-497 de 29 de abril de 2019, sustituido por la resolución No. SB-2021-2126 de 2 de diciembre de 2021).
- Ley Orgánica de Transparencia y Acceso a la Información Pública, Ley No 24 publicada en el Registro Oficial Suplemento No 337 del 18 de mayo de 2004.

- Código de Ética de la Corporación Financiera Nacional B.P.
- NORMA ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información Requerimientos –
- NORMA ISO/IEC 17799:200527002 Tecnología de la información - Técnicas de seguridad - Código de práctica para la gestión de seguridad de la información.
- INEN ISO/IEC 27005 Gestión del Riesgo en la Seguridad de la Información.
- EGSI–Esquema Gubernamental de Seguridad de la Información. Acuerdo Ministerial 025-2019 publicado en el Registro Oficial Edición Especial No 228 del 10 de enero de 2020.
- Código Orgánico Monetario y Financiero, Registro Oficial No 332 del 12 de septiembre de 2014, Libro I, Sección 16 del Sigilo y Reserva. Ley orgánica de protección de datos personales, Registro Oficial del 26 de mayo de 2021, Quinto Suplemento.
- Ley orgánica del sistema nacional de contratación pública, reformado el 17 de febrero de 2021.

**Artículo 5.- GLOSARIO DE TÉRMINOS:**

**a) Activo de información:**
Se refiere a toda información generada por la CFN B.P. en el desarrollo de sus actividades y procesos.

**b) Administración de Riesgos**
Es el proceso de identificación, control, medición y mitigación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

**c) Anti Phishing:**

Es un método que permite evitar que los ciberdelincuentes consigan información no autorizada, a través del engaño (como por ejemplo a través de páginas web que aparentan ser de una empresa, correos electrónicos falsos, etc.).

**d) Anti-spyware:**

Herramienta tecnológica que detecta y elimina programas maliciosos o amenazantes en un computador.

**e) Antivirus:**

Herramienta tecnológica que detecta y elimina software malicioso de equipos y dispositivos.

**f) Autenticación:**
Es garantizar el origen de la transacción, validando al emisor para evitar suplantación de identidades.

**g) Autorización:**
Es asegurar que la transacción sea ejecutada por quién está legalmente facultado.

**h) Canales electrónicos**
Se refiere a todas las vías o formas a través de las cuales los clientes o usuarios pueden efectuar transacciones, consultas, entre otros, con las instituciones del sistema financiero, mediante el uso de elementos, dispositivos electrónicos o tecnológicos.

**i) Ciberseguridad:**
Conjunto de medidas de protección de la infraestructura tecnológica y de la información, a través del tratamiento de las amenazas que ponen en riesgo la información procesada por los diferentes componentes tecnológicos interconectados.

**j) Confiabilidad:**
Es asegurar que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las funciones.

**k) Datos Personales:**
Datos que identifican o hacen identificable a una persona natural, directa o indirectamente.

**l) Dispositivos BYOD (Bring your own device):**
Dispositivos personales que son utilizados por las personas en una Empresa. Son sus propios dispositivos, los cuales no son provistos por las Empresas.

**m) Evaluación de Riesgos**
Es el análisis de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento (centro de cómputo) de la misma, la probabilidad de que ocurran y su potencial impacto en la operatividad de la entidad.

**n) Incidente de Seguridad**
Es un evento adverso inesperado o no deseado que amenaza la confidencialidad, integridad, disponibilidad y/o confiabilidad de la información, y tiene una probabilidad significativa de comprometer las operaciones del negocio.

**o) Información:**
Se refiere a toda forma de registro electrónico, óptico, magnético, o en otros medios, previamente procesado a partir de datos, que pueden ser almacenados, distribuidos y sirven para análisis, estudios y toma de decisiones.

**p) Instalaciones de procesamiento:**
Se refiere a la infraestructura que permite alojar los recursos físicos relacionados con la tecnología de información.

**q) Malware:**

O “software malicioso” es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.

**r) No repudio:**
Es garantizar que el uso y/o modificación de la información por parte de un usuario sea irrefutable, es decir, que el usuario no pueda negar dicha acción.

**s) Propietario de la Información**
Se refiere al funcionario al cual se la ha asignado la responsabilidad administrativa para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término “propietario” no significa que la persona tenga realmente algún derecho de propiedad sobre el activo de información.

**t) Seguridad de la Información**

Se entiende por seguridad de la información a la preservación de las siguientes características:

- **Confidencialidad:** garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** salvaguardar la totalidad y exactitud de la información, así como, los métodos de procesamiento.
- **Disponibilidad:** garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, siempre que lo requieran.

**u) Sistema de Información:**

Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

**v) Tecnología de Información:**

Se refiere al hardware y software operado por la CFN B.P. o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad.

**w) Teletrabajo:**

El teletrabajo es un modelo laboral en donde el empleado realiza sus funciones desde su casa y que utiliza las tecnologías de la información para acceder a los recursos tecnológicos institucionales.

**x) Terceros:**

Se refiere a toda persona externa a la CFN B.P. que interactúa de alguna manera con información de la CFN B.P., sean proveedores, auditores externos, personal de organismos de control, entre otros.

**Artículo 6.- INCUMPLIMIENTOS:**

Todo funcionario que tiene acceso a los sistemas informáticos debe suscribir el Acuerdo de Confidencialidad de la Información Anexos 1 y 3, en el cual el usuario se compromete a mantener la integridad, calidad y confidencialidad de la información institucional, de los clientes, y/o terceros; así como, el cumplimiento de las disposiciones contempladas en el artículo 7, literal a) del título III del Reglamento de Régimen Disciplinarios de la institución.

El Código de Ética de CFN B.P., contempla la sección VII de la Información y Confidencialidad, por tanto:

En caso de incumplimiento de la presente política, la Corporación Financiera Nacional B.P. debe aplicar las medidas disciplinarias según se determina en la Ley Orgánica de Servicio Público (LOSEP) y su Reglamento; y Reglamento Interno de Administración del Talento Humano de la Corporación Financiera Nacional B.P.

**Artículo 7.- SOBRE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:**

**Importancia**

Debido al cambio constante de tecnología, personas y procesos, la seguridad de la información se vuelve un reto, de ahí la importancia de establecer lineamientos de alto nivel para que todas las personas involucradas

con la institución conozcan las normas y reglas que se deben cumplir para garantizar la confidencialidad, integridad y disponibilidad de la información.

Es importante adelantarnos y prevenir posibles riesgos o amenazas que puedan afectar a la Seguridad de la Información y además saber cómo actuar cuando se presenten incidentes. El objetivo principal es proteger los datos de la organización y otros activos valiosos.

La información es un recurso que, como el resto de los activos, tiene valor importante y estratégico para la entidad y por consiguiente debe ser debidamente protegida.

Las Políticas y Procedimientos de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la Institución.

La Política de Seguridad debe formar parte de la cultura organizacional, es por ello que existe el compromiso manifiesto de las máximas Autoridades y de los Gerentes, Subgerentes, Jefes y Designados de las Unidades Administrativas, para la difusión, consolidación y cumplimiento de la presente Política.

**Principios**

a) Las políticas de Seguridad de la Información son definidas bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento; las cuales definan claramente la posición de la CFN B.P. respecto a la seguridad de la información.

b) Las políticas, procedimientos y normas de seguridad son elaboradas, revisadas y evaluadas periódicamente; en especial, ante cambios significativos en la tecnología de información promulgados por marcos referenciales como: normas de mejores prácticas, resoluciones de organismos de control, cambios institucionales o procesos que puedan afectar la base original de evaluación de riesgos.

c) La Gerencia de Seguridad de la Información será la encargada de proponer al Comité de Administración de la Seguridad de la Información, las diferentes políticas y procedimientos relacionados con la seguridad de la información, incluyendo la ciberseguridad (para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos); mientras que la Gerencia de Tecnologías de la Información, será la encargada de las implementaciones tecnológicas que se requieran para su cumplimiento.

d) CFN B.P. tiene el derecho de ver, editar y borrar todos los datos e información de la Institución que se encuentran almacenados, transferidos o procesados si considera que es necesario para la protección de los datos e información de la empresa, sin el consentimiento del propietario del dispositivo.

e) CFN B.P. no asume responsabilidad alguna por los datos e información personal contenida en los dispositivos a cargo de los usuarios; o por la información personal proporcionada por los empleados o terceros a través de los accesos permitidos en las diferentes plataformas tecnológicas, a través de los activos de información o a través de la red; o por los datos e información personal que estén contenidos en los sistemas y/o aplicaciones de la entidad; por los datos e información personal contenida en los dispositivos BYOD; o por los datos e información personal que estén almacenados en los activos de información y que hayan sido eliminados sin notificación previa; o por los datos e información personal que estén contenidos en los documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico.

f) CFN B.P. tiene la facultad de analizar, modificar, actualizar, restringir y eliminar los accesos a los sistemas, información relevante y/o recursos tecnológicos; cuando considere necesario o cuando evidencie que existan vulnerabilidades que puedan afectar el buen desenvolvimiento de las operaciones de la institución.
g) CFN B.P. tiene la facultad de analizar, modificar, actualizar y eliminar las relaciones con los proveedores de servicios que presten servicios asociados con el tratamiento o resguardo de los activos de información; cuando considere necesario o cuando evidencie que existan debilidades que puedan afectar el buen uso de los activos de la entidad.
h) CFN B.P. tiene la facultad de analizar y efectuar actualizaciones de manera automática para resolver errores en los sistemas; cuando considere necesario o cuando evidencie que existan vulnerabilidades que puedan ser explotadas y comprometan el buen desenvolvimiento de las operaciones de la institución.
i) CFN B.P. tiene la facultad de analizar, instalar, desinstalar y actualizar software que permitan detectar y/o evitar la instalación de software no autorizado o sin la respectiva licencia; cuando considere necesario o cuando evidencie que existan vulnerabilidades que puedan ser explotadas y comprometan el buen desenvolvimiento de las operaciones de la entidad.
j) CFN B.P. tiene el derecho de ver, editar y borrar todos los datos e información de la empresa que se encuentran almacenados, transferidos o procesados en dispositivos BYOD si considera que es necesario para la protección de los datos e información de la empresa, sin el consentimiento del propietario del dispositivo.
k) CFN B.P. tiene la facultad de analizar, restringir y eliminar la información relevante almacenada en los activos de información y/o recursos tecnológicos; cuando considere necesario o cuando evidencie que existan vulnerabilidades que puedan afectar el buen desenvolvimiento de las operaciones de la institución.
l) CFN B.P. tiene la facultad de analizar, modificar y restringir los accesos a la información contenida en documentos, medios de almacenamientos u otros dispositivos externos e intercambio electrónico contra: robo, utilización o divulgación no autorizada de información; cuando considere necesario o cuando evidencie que existan vulnerabilidades que puedan afectar el buen desenvolvimiento de las operaciones de la institución.
m) CFN B.P. tiene la facultad de analizar, editar, bloquear y cambiar los accesos a la red de datos y/o aplicativos; cuando considere necesario o cuando evidencie que existan vulnerabilidades que puedan ser explotados por software malicioso o atacantes de la red.
n) CFN B.P. tiene la facultad de analizar, revisar y catalogar eventos de seguridad como incidentes de seguridad; cuando considere necesario o cuando evidencie que se vulneran los sistemas de información y/o servicios del sistema de Seguridad de la Información.

**Niveles de Revisión y Aprobación**

El Comité de Administración de la Seguridad de la Información debe evaluar las políticas Institucionales de Seguridad de la Información, normas y procedimientos recomendadas por la Gerencia de Seguridad de la Información, y proponer su aprobación.

El Directorio de la Corporación Financiera Nacional B.P. aprobará las políticas de Seguridad de la Información.

## CAPÍTULO II: DE LA SEGURIDAD DE LOS RECURSOS HUMANOS

**Artículo 8.-:**

**Funciones y Responsabilidades**
a) La Gerencia de Talento Humano debe tener documentado las funciones y responsabilidades de los empleados, contratistas y terceros de acuerdo con la Política de Seguridad de la Información de la Institución.
b) La Gerencia de Talento Humano es la responsable de entregar formalmente a los nuevos empleados sus funciones y responsabilidades a cumplir dentro de la Unidad Administrativa a la cual fueron asignados.

c) La Gerencia de Talento Humano debe notificar a la Gerencia de Seguridad de la Información los permisos necesarios para activación y acceso a los activos de información a los usuarios que se integran a la Institución, de manera coordinada con el superior jerárquico de la Unidad Administrativa respectiva al que se va a integrar el usuario.
d) Es responsabilidad de todos los funcionarios de la Institución informar a la Gerencia de Seguridad de la Información sobre los eventos potenciales, intentos de intrusión u otros riesgos que pueden afectar la Seguridad de la Información de la CFN B.P.

**Selección**

e) La Gerencia Administrativa y/o Gerencia de Talento Humano, dentro del ámbito de su competencia, debe cumplir y realizar las siguientes actividades:

i. Comprobar los antecedentes de todos los candidatos a empleados, contratistas y terceros de acuerdo con las legislaciones, normativas y códigos éticos que sean de aplicación para el efecto.

ii. Definir los criterios y las limitaciones para las revisiones de verificación de personal actual (por motivos de designación o promoción), potenciales empleados y de terceras partes.
iii. Informar del procedimiento de revisión y solicitar el consentimiento al personal actual (por motivos de designación o promoción), potenciales empleados y de terceras partes

**Términos y Condiciones Laborales**

f) La Gerencia Jurídica asesora a las Unidades Administrativas que gestionen contratos con empleados, contratistas y terceros para que se incorporen la firma de un acuerdo de confidencialidad o no divulgación (Anexos 1 <personal interno>, 2 <personal externo> y 3 <utilización de herramientas tecnológicas>, según corresponda), antes de que tengan acceso a la información. En el contrato se debe establecer los parámetros de vigencia del acuerdo, información confidencial referida, formas de acceso, responsabilidades y funciones.
g) La Gerencia Administrativa y/o Gerencia de Talento Humano debe solicitar como parte de su obligación contractual que los empleados, contratistas y terceros, en caso de ser seleccionados, acepten, firmen los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información, así mismo debe responsabilizar al personal sobre el manejo y creación de la información resultante durante el contrato laboral con la Institución.

**Empleados y puestos de trabajo**

h) A fin de prevenir los riesgos de error humano, robo, fraude, uso inadecuado de los recursos, etc., la Gerencia de Talento Humano debe incluir en sus procesos y procedimientos lineamientos que aseguren una apropiada planificación y administración del capital humano con respecto a la seguridad de la información.
i) Los términos y condiciones del contrato de empleo establecen la responsabilidad del funcionario con respecto a la seguridad de la información, durante y después de la relación laboral con la CFN B.P.
j) Todos los empleados y usuarios externos de las instalaciones de procesamiento de información deben mantener el sigilo y confidencialidad de la información que maneja la Institución para lo cual deben suscribir el acuerdo de confidencialidad (Anexos 1 <personal interno>, 2 <personal externo> y 3 <utilización de herramientas tecnológicas>, según corresponda).

**Capacitación del personal**

k) Todo el personal de la CFN B.P. debe recibir periódicamente una adecuada capacitación y actualización en relación con los procedimientos de seguridad, la respuesta a incidentes de seguridad, las responsabilidades legales y el correcto uso de las instalaciones de procesamiento de información, a fin de minimizar eventuales riesgos de seguridad. También se debe capacitar a aquellos funcionarios y empleados que estén a cargo de responsabilidades de seguridad de la información, específicamente en administración y tecnología de seguridad.
l) El Programa de Capacitación debe ser llevado a cabo por la Gerencia de Seguridad de la Información de acuerdo a la planificación operativa anual y con la colaboración de la Gerencia de Talento Humano, quien se encargará de coordinar y comunicar a la personal de CFN B.P.
m) Es responsabilidad y obligación de cada empleado de la Corporación Financiera Nacional B.P. asistir a los cursos o talleres de capacitación en seguridad de la información, registrar su asistencia y rendir la evaluación correspondiente.

**Durante el Empleo**

n) La Gerencia de Seguridad de la Información debe lograr la concienciación del funcionario sobre la Seguridad de la Información correspondiente a sus funciones y responsabilidades dentro de la CFN B.P.
o) La Gerencia Administrativa y/o Gerencia de Talento Humano deben exigir a los empleados, contratistas y terceros que apliquen aspectos de seguridad de acuerdo con la Política de Seguridad de la Información y procedimientos establecidos en la CFN B.P.
p) La Gerencia de Seguridad de la Información debe verificar el cumplimiento de las funciones y responsabilidades respecto a la Seguridad de la Información mediante la utilización de reportes e informes.
q) La Gerencia de Talento Humano debe aplicar el Régimen Disciplinario de a LOSEP en concordancia con la normativa interna para los empleados que hayan provocado alguna violación de la Política de Seguridad de la Información.
r) La Gerencia de Talento Humano debe considerar sanciones graduales, dependiendo de factores tales como naturaleza, cantidad y la gravedad de la violación, así como su impacto en el negocio, el nivel de la capacitación del personal, la legislación correspondiente (Ley orgánica de protección de datos personales, Ley de Comercio Electrónico, Firmas electrónicas, Mensajes de datos y demás leyes conexas) y demás factores existente en los procedimientos propios de la Corporación Financiera Nacional B.P.

**Finalización del Empleo o cambio de puesto de trabajo**

s) La Gerencia de Talento Humano debe comunicar oficialmente al personal las responsabilidades para la terminación de su relación laboral, lo cual debe incluir los requisitos permanentes para la seguridad de la información y las responsabilidades legales o contenidas en cualquier acuerdo de confidencialidad (Anexos 1, y 3). Además debe informar de esta situación a la Gerencia de Seguridad de la Información (para gestionar la inactivación de los usuarios en los sistemas informáticos) y a la Gerencia Administrativa.
t) Los cambios en la responsabilidad o en el contrato laboral de un funcionario deben ser gestionados por la Gerencia de Talento Humano, que incluye la terminación de la responsabilidad o el contrato laboral respectivo y la nueva responsabilidad o contrato laboral.
u) Previo a la terminación de un contrato es obligación del funcionario realizar la transferencia de la documentación e información de la que fue responsable al nuevo funcionario a cargo, jefe inmediato y/o responsable de la Unidad Administrativa; en caso de ausencia, a la Gerencia de Seguridad de la información.

v) La Gerencia Administrativa y/o Gerencia de Talento Humano deben garantizar que los contratos del empleado, el contratista o el usuario de terceras partes, incluyan las responsabilidades válidas aún después de la terminación del contrato laboral.

w) Para personal externo, es responsabilidad del superior jerárquico de la Unidad Administrativa notificar las desvinculaciones a la Gerencia de Seguridad de la Información para proceder a inactivar los usuarios, de no hacerlo se considera una falta grave, porque se pone en riesgo a los activos de información ya que se pueden dar accesos no autorizados.

x) La Gerencia de Talento Humano debe garantizar que los empleados devuelvan todos los activos (dispositivos de cómputo móviles, tarjetas de acceso, token USB con certificados de electrónicos, pendrive, entre otros) de la organización que estén inventariados, al finalizar su empleo, contrato o acuerdo.

y) La Gerencia de Talento Humano debe coordinar con el superior jerárquico de la unidad administrativa correspondiente, de tal manera que se apliquen los debidos procesos para garantizar que toda la información generada por el empleado, contratista o usuario de terceras partes dentro de la CFN B.P, sea transferida, archivada o eliminada con seguridad y de manera coordinada con la Gerencia de Seguridad de la Información.

z) La Gerencia de Talento Humano debe solicitar al jefe inmediato del funcionario saliente que certifique que se ha realizado el proceso de traspaso de conocimientos por parte del empleado, contratistas o terceras partes al nuevo funcionario, y en caso de ausencia se puede realizar dicha transferencia a un funcionario delegado para esta actividad, de tal forma que se asegure la continuación de las operaciones importantes dentro de la CFN B.P.

## CAPÍTULO III: DE LA SEGURIDAD FÍSICA Y DEL ENTORNO

### Artículo 9.- CARACTERÍSTICAS DE LAS CONTRASEÑAS:

**Áreas seguras**

a) Las instalaciones de procesamiento de la CFN B.P. deben estar ubicadas en sitios resguardados por un perímetro de seguridad con controles de acceso y físicamente protegidas contra daños e intrusiones.

b) Los espacios físicos que administrativamente se definan como Áreas Seguras deben estar protegidas por controles adecuados, para asegurar que únicamente se permita el acceso de personal autorizado.

**Seguridad del equipamiento y documentación**

c) El equipamiento de tecnología de información y comunicaciones debe estar físicamente protegido de amenazas de seguridad y peligros ambientales, para reducir el riesgo de acceso no autorizado a los datos y para prevenir pérdidas o daños. Además, estará protegido con respecto a posibles fallas en el suministro de energía eléctrica.

d) El equipamiento es provisto de mantenimiento adecuado para asegurar que su disponibilidad e integridad sean permanentes.

e) Las instalaciones de procesamiento de información y la información deben ser protegidas contra divulgación, modificación o robo por parte de personas no autorizadas, debiéndose implementar controles para minimizar pérdidas o daños.

f) El equipamiento, la información o el software no deben ser retirados de la sede de la organización sin autorización.

g) El cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de

información debe estar protegido frente a interceptaciones o daños.

h) La Gerencia de Seguridad de la Información, debe generar una política General sobre este tema, en la cual se detallen políticas más específicas.

## CAPÍTULO IV: DE LA GESTIÓN DE COMUNICACIONES Y OPERACIONES

**Artículo 10.- Generalidades:**

i) La Gerencia de Tecnologías de la Información debe establecer políticas, procedimientos y responsabilidades formales para la gestión y operación de los recursos de procesamiento de la información y el control de cambios en los sistemas e instalaciones, los cuales estén bajo la coordinación con la Gerencia de Seguridad de la Información.

j) La Gerencia de Tecnologías de la Información, debe separar los ambientes de desarrollo, pruebas, contingencia y producción para reducir los riesgos de acceso no autorizado o los cambios en los sistemas e instalaciones. La Gerencia de Seguridad de la Información debe hacer el control correspondiente.

k) La Gerencia de Tecnologías de la Información, de manera periódica (de acuerdo a lo establecido por los Organismos de Control) debe presentar el plan de capacidad, el cual debe incluir las oportunidades de mejoras y acciones oportunas a fin de garantizar la disponibilidad de la capacidad de procesamiento y almacenamiento adecuados, en función de los nuevos requerimientos del negocio y sistemas de la Institución.

l) La Gerencia de Tecnologías de la Información debe implementar controles de detección y prevención para la protección contra software malicioso, en coordinación con la Gerencia de Seguridad de la Información.

m) Con el fin de mantener la disponibilidad de los servicios de procesamiento y comunicación de información, la Gerencia de Tecnologías de la Información, debe establecer procedimientos formales de respaldo de equipos, datos y software esencial, que incluyan pruebas de restablecimiento oportuno y el registro de eventos y fallas, en coordinación con la Gerencia de Seguridad de la Información.

n) La Gerencia de Tecnologías de la Información, debe implementar mecanismos de control adecuados a fin de garantizar la seguridad de la información en las redes (y su segmentación) y la protección de la infraestructura de soporte, bajo la coordinación con la Gerencia de Seguridad de la Información.

o) La Gerencia de Tecnologías de la Información, debe implementar mecanismos que protejan los medios de almacenamiento contra daño, robo y acceso no autorizado, con el fin de impedir la interrupción de las actividades de la Institución, bajo la coordinación de la Gerencia de Seguridad de la Información.

p) La Gerencia de Tecnologías de la Información, debe implementar mecanismos para que la información incluida en transacciones en línea, así como la información puesta a disposición pública esté protegida para evitar actividades fraudulentas, disputas contractuales, transmisión incompleta o modificaciones no autorizadas, en coordinación con la Gerencia de Seguridad de la Información.

q) La Gerencia de Tecnologías de la Información debe asegurar que los sistemas de información incluyan los registros de auditoría de las actividades de los usuarios, las excepciones y eventos de seguridad de la información, y deben mantener los registros durante un periodo acordado para servir como prueba en investigaciones futuras y en la supervisión del control de acceso, de manera coordinada con los propietarios de la información y la Gerencia de Seguridad de la Información.

**Artículo 11.- Responsabilidades y Procedimientos de Operación:**

r) Es responsabilidad de los usuarios de las Unidades Administrativas de los sistemas de información, el documentar sus procedimientos de operación, mantenerlos actualizadas y puestos en conocimiento de todos los usuarios que los necesiten, conforme a lo establecido en el Sistema de Gestión de Calidad de la CFN B.P.
s) La Gerencia de Tecnologías de la Información, debe mantener un procedimiento formal y único de la gestión de cambios para todo recurso tecnológico y sistema de tratamiento de la información que garantice la correcta continuidad de la operatividad.
t) A fin de reducir la posibilidad de que se produzcan modificaciones no autorizadas o usos indebidos de los activos Institucionales, debe existir una adecuada segregación de tareas.
u) Los diferentes ambientes de procesamiento de información deben estar separados a fin de reducir los riesgos de acceso o cambios no autorizados, tales ambientes deben ser de desarrollo, pruebas - control de calidad y producción.

**i. Ambiente de Desarrollo de Sistemas de información**

Este ambiente debe servir para realizar las tareas de análisis, desarrollo, mantenimiento y pruebas parciales o técnicas de los sistemas y plataformas.

En este ambiente residen las herramientas de desarrollo (utilitarios, compiladores y similares), los programas fuentes, bases de datos y archivos para desarrollo y pruebas parciales o técnicas.

El ambiente de desarrollo debe operar con muestras de archivos y base de datos parciales o con información despersonalizada. Cuando sea necesario el archivo total y real, se debe solicitar la correspondiente autorización a la Gerencia de Seguridad de la Información.

La Gerencia de Seguridad de la Información en coordinación con los propietarios de la Información son los responsables de definir la información que debe despersonalizarse previo a su carga en este ambiente por parte de la Gerencia de Tecnologías de la Información.

Al ambiente de desarrollo solo pueden acceder los servidores (personal) de la Gestión Interna de Desarrollo de Sistemas de la Gerencia de Tecnologías de la Información y servidores (personal) que deba efectuar tareas de administración de los equipos de la Gerencia de Tecnologías de la Información o terceros con accesos controlados y contratos debidamente firmados, bajo la supervisión y control de la Gerencia de Tecnologías de la Información y la Gerencia de Seguridad de la Información.

**ii. Ambiente de Pruebas - Control de Calidad**

Este ambiente sirve para realizar pruebas integrales certificables de los sistemas y plataformas previos a implementarse en producción.

En este ambiente residen los aplicativos y versiones fuentes aprobadas por los usuarios para su compilación y posterior pase a producción.

Al ambiente de pruebas solo pueden acceder los servidores (personal) de la Gerencia de Tecnologías de la Información encargados de la Administración de Pruebas, servidores de la Gerencia de Seguridad de la Información, los usuarios responsables definidos para probar y autorizar el pase a producción y servidores (personal) encargados de efectuar tareas de administración de los equipos con el perfil que corresponda.

**iii. Ambiente de Producción**

En el ambiente de producción están datos reales, programas fuentes con restricciones de acceso, ejecutables e instaladores de las diferentes plataformas, por ningún motivo deben residir herramientas de desarrollo.

La Gerencia de Tecnologías de la Información debe asegurar la uniformidad de todas las versiones instaladas en producción en todos los equipos de procesamiento de la CFN B.P.

En el ambiente de producción solo deben acceder los usuarios finales de plataformas y servidores (personal) de la Gerencia de Tecnologías de la Información encargados de la administración de los equipos del centro de cómputo.

Los servidores (personal) de la Gestión Interna de Desarrollo de Sistemas de la Gerencia de Tecnologías de la Información solo pueden acceder a los programas y datos reales para dar soporte y solución a problemas en las plataformas.

Antes de la salida a producción de una nueva plataforma, la Gerencia de Seguridad de la Información debe validar el cumplimiento de las políticas de seguridad de la información, así como también los requerimientos de seguridad definidos en la etapa de conceptualización de los proyectos de desarrollo, y validar el informe de vulnerabilidades de código ejecutado por la Gerencia de Tecnologías de la Información, con el fin de minimizar la posibilidad que la nueva plataforma ingrese en producción con huecos de seguridad, dicho análisis se debe realizar de manera conjunta con el Administrador de Pruebas de la Gerencia de Tecnologías de la Información.

Para el caso de nuevas versiones, cambios a las plataformas, la Gerencia de Seguridad de la Información, puede evaluar, dependiendo si los cambios introducidos en las nuevas versiones podrían haber afectado al cumplimiento de las normas de seguridad.

**Artículo 12.- Gestión de la provisión de servicios por terceros:**

v) La Gerencia Jurídica debe asesorar a las Unidades Administrativas que gestionen contratos de prestación de servicios o adquisición de bienes por parte de terceros las cláusulas que definan:

i. La propiedad de la información y de las aplicaciones;
ii. La responsabilidad de la empresa proveedora de la tecnología en caso de ser vulnerables sus sistemas, a fin de mantener la integridad, disponibilidad y confidencialidad de la información; y,
iii. Que las aplicaciones sean parametrizables, que exista una transferencia del conocimiento y que se entregue documentación técnica y de usuario, a fin de reducir la dependencia la Corporación Financiera Nacional B.P. con proveedores externos y los eventos de riesgo operativo que esto origina.

w) Las Unidades Administrativas que reciban servicios prestados por terceros, deben supervisar y revisar periódicamente el servicio, los informes y registros proporcionados por el proveedor a fin de asegurar que se encuentren enmarcados en los ámbitos contractuales, complementariamente y de ser necesario, se deben llevar a cabo auditorias de los servicios prestados.

**Artículo 13.- Planificación y aceptación del sistema:**

x) La Gerencia de Tecnologías de la Información es la responsable de evaluar la capacidad instalada, así como de realizar las proyecciones de los requisitos futuros de capacidad en función de las necesidades del negocio y en base a la información suministrada por los usuarios de las Unidades Administrativas de los sistemas de información.

y) Los usuarios de las Unidades Administrativas deben realizar todas las pruebas necesarias y dejar por escrito la aceptación de nuevos sistemas de información o de la actualización y nuevas versiones de los mismos.

**Artículo 14.- Protección contra código malicioso y descargable:**

z) La Gerencia de Tecnologías de la Información en coordinación con la Gerencia de Seguridad de la Información debe implantar los controles de detección, prevención y recuperación que sirvan como protección contra código malicioso.

aa) La Gerencia de Talento Humano en coordinación con la Gerencia de Seguridad de la Información, debe emplear mecanismos adecuados para la concienciación de los servidores (personal) con el fin de reducir las exposiciones al código malicioso.

bb) El usuario debe abstenerse de ejecutar un programa si no se tiene la certeza de los resultados o si no se conoce el origen del programa, especialmente si son programas y/o archivos que provengan de fuentes externas y no confiables como: CD, unidades externas de almacenamiento, correos externos, Internet, entre otros.

cc) Los programas de control de virus deben ser instalados, configurados y actualizados por la Gerencia de Tecnologías de la Información, en los puntos de acceso a redes externas, los equipos centralizados de procesamiento y en las estaciones de trabajo de modo residente para que estén activados durante su uso a fin prevenir y eliminar las consecuencias de la acción de los virus informáticos.

dd) Las actualizaciones deben aplicarse solamente en el servidor central donde reside el programa master antivirus, el mismo que debe distribuir dichas actualizaciones a los demás equipos de la Institución.

ee) Los programas antivirus deben monitorear y detectar los posibles virus y spams en tiempo real, así como, analizar los archivos recibidos vía el servicio de correo electrónico o desde otras redes de datos / Internet.

ff) Ante la sospecha de la existencia de un virus, el servidor (personal) debe desconectar el computador de la red en forma inmediata, y reportar dicho incidente a la Gerencia de Tecnologías de la Información y a la Gerencia de Seguridad de la Información.

gg) Se prohíbe la utilización de CD's o unidades externas de almacenamiento de origen desconocido, los medios a ser utilizados deben ser revisados previo a su uso, por el programa antivirus instalado en cada computador, para la cual, la Gerencia de Tecnologías de la Información debe implementar los mecanismos necesarios para facilitar el control del uso de los dispositivos señalados, en función de las necesidades del negocio.

hh) No se debe introducir a propósito virus en las computadoras de la institución.

ii) La Gerencia de Tecnologías de la Información debe implementar los mecanismos necesarios para revisar que los computadores externos (de proveedores) que se conecten a la red Institucional, cuenten con un programa antivirus, en caso de no tenerlo, debe solicitar al proveedor la instalación del mismo.

jj) La Gerencia de Tecnologías de la Información y la Gerencia de Seguridad de la Información deben revisar los reportes de antivirus y antispam a fin de tomar acciones preventivas o correctivas según el caso, para lo cual la Gerencia de Tecnologías de la Información debe desarrollar el procedimiento que corresponda el cual debe incluir la periodicidad de su revisión, cuyos resultados deben ser remitidos a la Gerencia de Seguridad de la Información.

**Artículo 15.- Copias de Seguridad:**

kk) La Gerencia de Tecnologías de la Información es responsable por la obtención de copias de seguridad (backups) de la configuración e información residente en los equipos del centro de cómputo, software, log's de seguridad, pistas de auditoría y aplicaciones que soportan el procesamiento de la información, para lo cual, debe establecer procedimientos formales de respaldo, restauración y recuperación de equipos, datos, software, bajo la coordinación de la Gerencia de Seguridad de la Información.

ll) A fin de garantizar que las copias de seguridad se obtienen y conservan adecuadamente, la Gerencia de Tecnologías de la Información es responsable de ejecutar pruebas de legibilidad de dichas copias, cuyos resultados deben ser reportados a la Gerencia de Auditoría Interna Bancaria y/o la Gerencia de Auditoría Interna Gubernamental, así como también a la Gerencia de Seguridad de la Información y Gerencia de Riesgo – Subgerencia de Riesgo Operativo, sobre la base del procedimiento que para el efecto haya definido la Gerencia de Tecnologías de la Información, en el cual debe determinar su periodicidad y la forma de escoger la muestras para dichas pruebas.

mm) Es de responsabilidad de los usuarios realizar respaldos frecuentes de la información de trabajo que considere importante y que reside en su equipo, de acuerdo a las políticas de Control de Accesos.

nn) El espacio destinado en el servidor central para almacenar copias de respaldo de información de los usuarios es definido por la Gerencia de Seguridad de la Información y la Gerencia de Tecnologías de la Información en función de la disponibilidad de recursos (plan de capacidad). En caso de requerir mayor espacio, el usuario debe depurar sus datos, dando prioridad a los de mayor importancia; las excepciones de espacio deben ser autorizadas por la Gerencia de Seguridad de la Información.

oo) La información que el usuario respalde en el servidor central, está sujeta a verificación de cumplimiento de políticas por la Gerencia de Seguridad de la Información o la Gerencia de Tecnologías de la Información, en el caso de no dar fiel cumplimiento con las normas estipuladas, se puede proceder a eliminar los archivos sin

pp) previo aviso, incluso se podrá quitar el privilegio de respaldar información en caso de incumplimientos reiterados.

**Artículo 16.- Gestión de Seguridad de las Redes:**

qq) Se deben implementar los mecanismos necesarios a fin de asegurar la protección de la información en las redes y la infraestructura que la soporta, para lo cual se debe considerar:

iv. La Administración de la seguridad perimetral está a cargo de la Gerencia de Tecnologías de la Información, sin embargo, la Gerencia de Seguridad de la Información debe tener acceso de modo consulta a las plataformas/herramientas que la conforman, de tal manera de validar posibles eventos que pongan en riesgo la seguridad de la información.

v. Separación lógica o física de las redes de acuerdo a las necesidades del negocio que es de responsabilidad de la Gerencia de Tecnologías de la Información, así como, la aplicación de mecanismos que permitan asegurar la confidencialidad de la información en el tráfico de redes

vi. La administración de equipos en forma remota debe ser restringida al personal estrictamente necesario y de competencia con sus funciones del cargo (establecido por la Gerencia de Tecnologías de la Información), bajo la coordinación de la Gerencia de Seguridad de la Información.

vii. Se puede tomar control de equipos únicamente para casos de soporte técnico y con la autorización explícita del dueño del mismo, su incumplimiento es considerado como falta grave.

viii. La optimización de los enlaces de comunicación en cuanto a rendimiento y seguridad.

ix. Las redes institucionales deben estar protegidas con los mecanismos de seguridad necesarios (software o hardware) a fin de garantizar la confidencialidad, integridad y disponibilidad de la información

y de los servicios informáticos. La implementación está a cargo de la Gerencia de Tecnologías de la Información, bajo la coordinación de la Gerencia de Seguridad de la Información.

**Artículo 17.- Manipulación de los soportes:**

rr) Los servidores públicos (personal) no deben mantener información confidencial o activos de la institución sin la debida protección y accesible a otras personas cuando estén fuera de su lugar de trabajo. Esto incluye CD, unidades externas de almacenamiento u otros medios externos.

ss) La Gerencia Administrativa debe contar con procesos formales para la asignación y retiro de equipos de procesamiento / almacenamiento.

tt) Cuando un equipo sea retirado del puesto de trabajo de un usuario por parte de la Gerencia Administrativa, previo a la entrega del mismo a otro usuario o previo a su bodegaje para futuras acciones, éste debe ser entregado a la Gerencia de Tecnologías de la Información, para realizar el proceso de sanitización del equipo, en base a los procedimientos que dicha Unidad Administrativa defina para el efecto en coordinación con la Gerencia de Seguridad de la Información.

**Artículo 18.- Intercambio de información:**

uu) Cuando por necesidades institucionales se requiera intercambiar información con otras organizaciones, sean gubernamentales, privadas o proveedores, se debe vigilar la disponibilidad, confidencialidad e integridad de la información, para lo cual, la Gerencia de Tecnologías de la Información debe implementar los mecanismos necesarios que lo garanticen, en coordinación con la Gerencia de Seguridad de la Información.

vv) Los mensajes de correo electrónico que salieren de la CFN B.P. deben contener una nota adjunta de descargo que delinee el manejo de la información enviada por este medio.

ww) La Gerencia de Tecnologías de la Información debe garantizar la confidencialidad e integridad en el envío y recepción de mensajes de correo electrónico que contengan información sensible, para lo cual debe aplicar los mecanismos que den cumplimiento a las políticas de seguridad que correspondan.

**Artículo 19.- Servicios de Comercio Electrónico:**

xx) Las Unidades Administrativas que por sus necesidades operacionales, incluyan transacciones de comercio electrónico en sus actividades, deben coordinar con las diferentes Unidades Administrativas de la CFN B.P. la implementación de los controles necesarios a fin de prevenir actividades fraudulentas, disputas contractuales y revelación o modificación no autorizada de la información.

yy) Se debe implementar certificados digitales o controles similares en los servicios de transaccionalidad en línea prestado por la CFN B.P.

zz) La Gerencia de Tecnologías de la Información debe implementar cualquier mecanismo que garantice la identificación, autenticación y autorización de transacciones realizadas en línea, considerando un doble factor de autenticación, tales como tokens, tarjetas de coordenadas, OTP - one time password, biométricos, pines, entre otros.

aaa) La integridad de la información puesta a disposición pública debe estar protegida para evitar modificaciones no autorizadas, garantizando la buena reputación e imagen Institucional, para lo cual, la Unidad Administrativa responsable de publicar información debe coordinar con las diferentes Unidades Administrativas de la CFN B.P. la implementación de controles según el caso.

bbb) La Gerencia de Seguridad de la Información debe mantener permanentemente informados y capacitados a los clientes internos y externos de la CFN BP, sobre los riesgos derivados del uso de canales electrónicos, y sobre las medidas de seguridad que se deben considerar al momento de hacer uso de dichos canales. Se debe considerar en la capacitación entre otros servicios, la plataforma de correo seguro, y Files&ProFiles. Las cápsulas informativas deben ser publicadas a través de las redes sociales de la CFN B.P. afiches o flyers y correos electrónicos enviados a las cuentas personales de los clientes de la CFN, BP. El diseño y publicación de esta información debe ser realizada en coordinación con la Gerencia de Mercadeo.

**Artículo 20.- Supervisión:**

ccc) Todo sistema de información debe mantener pistas de auditoria de acuerdo a los requerimientos funcionales y necesidades de los propietarios de la información, cuidando el cumplimiento de las políticas relacionadas con este tema.

ddd) Las pistas de auditoría y log's de seguridad deben mantenerse por el período dispuesto por los organismos de control, a fin de poder ser revisados, monitoreados y servir como prueba en investigaciones futuras.

eee) La Unidad Administrativa de Secretaría General, es la responsable de mantener e informar a las demás Unidades Administrativas sobre los períodos de retención de las pistas de auditoría y log's de seguridad de acuerdo a lo establecido por los organismos de control.

fff) En caso de ser necesario vaciar las pistas de auditoría y log's de seguridad, el propietario de la información debe emitir la autorización respectiva y poner en conocimiento de la Gerencia de Seguridad de la Información.

ggg) La Gerencia de Tecnologías de la Información debe garantizar e implementar mecanismos seguros para avalar que las pistas de auditoría y log's de seguridad son protegidos contra manipulaciones indebidas y accesos no autorizados.

hhh) La Gerencia de Seguridad de la Información debe hacer revisiones periódicas de la existencia de información en las pistas de auditoria de las aplicaciones de negocio, de acuerdo a la periodicidad establecida.

iii) A fin de encontrar tempranamente fraudes o anomalías en el procesamiento de la información, los usuarios de las Unidades Administrativas y/o propietarios de la información son los responsables de la revisión de las pistas de auditoria de las aplicaciones de negocio, quienes deben informar de sus resultados a la Gerencia de Auditoría Interna Bancaria y/o la Gerencia de Auditoría Interna Gubernamental, así como también a la Gerencia de Seguridad de la Información.

jjj) La Gerencia de Auditoría Interna Bancaria y la Gerencia de Auditoría Interna Gubernamental deben realizar revisiones a las pistas de auditoria suministrados por los sistemas de procesamiento de información.

kkk) La Gerencia de Seguridad de la Información debe realizar revisiones periódicas de los log's de seguridad de los equipos, herramientas tecnológicas y actividades de usuarios privilegiados de la Gerencia de Tecnologías de la Información, sobre la base de las políticas y/o procedimientos de Seguridad de la Información definida para el efecto, de acuerdo a la periodicidad establecida y los el tipo de logs a ser monitoreados. Auditoria Interna puede solicitar la revisión de los log's en cualquier momento de considerarlo así necesario.

lll) La Gerencia de Tecnologías de la Información debe garantizar que los fallos e interrupciones de los sistemas/servicios sean registrados de acuerdo a los procedimientos de Gestión de Incidentes y/o Problemas y analizados a fin de tomar las correspondientes acciones.

mmm)Los relojes de todos los sistemas de procesamiento de la información deben estar sincronizados con una fuente oficial de tiempo.

**Artículo 21.- Gestión de los Medios removibles**

nnn) Los funcionarios que por sus actividades laborales porten información confidencial en dispositivos de almacenamiento removibles, son los únicos responsables de evitar el acceso no autorizado a la información contenida en el medio.

ooo) Es responsabilidad de cada funcionario tomar las medidas de seguridad adecuadas para el almacenamiento y resguardo de los medios removibles, de tal forma que se evite accesos no autorizados, daños, pérdida de información o robo del medio.

ppp) Los medios removibles no deben ser considerados por ningún motivo como alternativa para realizar respaldos de información.

qqq) La Gerencia de Tecnologías de la Información debe implementar las herramientas tecnológicas que consideren pertinentes para evitar la fuga de información a través de medios removibles institucionales, asignados a los funcionarios mediante el empadronamiento, en coordinación con la Gerencia de Seguridad de la Información.

## CAPÍTULO V: DEL CONTROL DE ACCESOS

**Artículo 22.-: Generalidades:**

a) La Gerencia de Tecnologías de la Información debe implementar en los sistemas de información, una Administración de Roles/Grupos y sus accesos, así como también una Administración de Usuarios, que sean amigables, bajo la coordinación de la Gerencia de Seguridad de la Información y con el cumplimiento de las políticas respectivas.
b) La Gerencia de Seguridad de la Información debe implementar procedimientos formales para controlar la asignación de derechos de acceso de usuarios a los sistemas y servicios de información, contemplando el registro de usuarios, la administración de privilegios, la administración de contraseñas de usuario, la revisión periódica de derechos de acceso de los usuarios y el registro de auditoría.
c) El plan de capacitación en materia de seguridad, es responsabilidad de la Gerencia de Seguridad de la Información y está enfocado en concienciar a los usuarios acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas, seguridad del equipamiento y buenas prácticas para precautelar la seguridad de la información.
d) Todos los usuarios deben seguir las buenas prácticas de seguridad en la selección y uso de contraseñas y seguridad del equipamiento. Las contraseñas son de uso personal e intransferible en todo momento; manejadas por el usuario como información confidencial, el compartir o divulgar las contraseñas se considera falta grave sancionable.
e) La Gerencia de Tecnologías de la Información debe implementar mecanismos para controlar el acceso a los servicios de red, sistemas operativos y aplicaciones, mientras que la Gerencia de Seguridad de la Información, es la responsables de validar los controles mediante la verificación en el cumplimiento de políticas de uso, autenticación de usuarios y mecanismos de protección, con el fin de garantizar que los usuarios no comprometan la seguridad de estos servicios.
f) El acceso a las herramientas de auditoria, monitoreo y administración de los sistemas de información es autorizado por la Gerencia de Seguridad de la Información, únicamente a las Unidades Administrativas relacionadas, a fin de evitar cualquier peligro o uso indebido.
g) Los funcionarios deben aplicar la política de pantallas y escritorios limpios determinada por la CFN B.P. para proteger documentos en papel, dispositivos de almacenamiento removibles, información en las estaciones de trabajo, entre otros, a fin de reducir los riesgos de acceso no autorizado, pérdida y/o daño de la información.

**Requisitos de negocio para el control de accesos**

h) Los roles o perfiles en los sistemas de información en forma general se clasificarán como: ingreso, modificación o registro de información, aprobación de transacciones, consulta, parametrización, administración de accesos y otros de acuerdo con el tipo de aplicación.
i) Los usuarios de los sistemas de información que soportan las actividades diarias de los diferentes procesos institucionales, no deben tener roles o perfiles de administración en los sistemas base.
j) Los perfiles de acceso de los funcionarios deben ser estandarizados de acuerdo a las funciones y actividades del cargo.
k) La autorización para la creación o modificaciones de roles únicamente la puede realizar el propietario de la información.
l) Por ningún motivo se puede otorgar a un mismo funcionario perfiles que tengan conflicto de intereses.
m) La Gerencia de Talento Humano de manera coordinada con la Unidad Administrativa requirente, deben presentar el formulario de accesos RPSI-12 en la cual se detallen todos los accesos requeridos para los nuevos usuarios, de tal manera de proceder con la creación de usuarios y accesos.
n) Cuando existan desvinculaciones, es responsabilidad de la Gerencia de Talento Humano, notificar a la Gerencia de Seguridad de la Información, de tal manera de gestionar las inactivaciones de usuarios y accesos.
o) De manera periódica, la Gerencia de Talento Humano debe comunicar a la Gerencia de Seguridad de la Información las novedades del personal, de tal manera de validar que se encuentren habilitados únicamente los usuarios activos.
p) Es responsabilidad de cada Unidad Administrativa de la Institución gestionar la creación de usuarios externos mediante el formulario de accesos RPSI-12 y además notificar de sus salidas cuando ya no colaboren en la Institución. De no hacerlo, se podría considerar una falta grave porque se corre el riesgo de mantener usuarios vigentes en los sistemas y servicios de personas que ya no colaboran con la Institución.
q) Es responsabilidad de cada usuario gestionar el formulario de accesos RPSI-12 cuando se requieran añadir o eliminar roles, con las autorizaciones del superior jerárquico y del propietario de la información.

r) Debido a sus funciones, la Gerencia de Seguridad de la Información debe verificar los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.
s) La Institución debe contar con una póliza de seguros para cubrir posibles riesgos informáticos, según resolución JB-2012-2090 y reformada mediante SB-2021-2126.

**Gestión de Accesos de Usuario**

t) Los niveles de seguridad de acceso a las aplicaciones en producción, deben ser controlados (validados) por la Gerencia de Seguridad de la Información.
u) Se otorgan accesos a las aplicaciones a los funcionarios de la CFN B.P. que tengan nombramiento, contrato de servicios ocasionales, contrato por honorarios profesionales o en comisión de servicios, acorde a las funciones que vayan a desempeñar en la institución. Se otorga el acceso a pasantes, auditores externos o de organismos de control a las diferentes aplicaciones que se manejan en la CFN B.P., solamente de consulta, se puede excepcionar los accesos de modificación a sistemas a pasantes de acuerdo a solicitud expresa de la jefatura, debidamente fundamentada y por tiempo limitado, con la autorización de la Gerencia de Seguridad de la Información.
v) El usuario es el único responsable por su correcto uso dentro de los aplicativos y servicios informáticos disponibles, por lo que se debe registrar los logs correspondientes en las estructuras definidas como críticas por los propietarios de la información y/o Seguridad de la Información.

w) Cuando el sistema informático o el servicio correspondiente lo permita, se puede habilitar más de una sesión de trabajo, a los usuarios, por pedido del superior jerárquico y una vez se tenga la autorización de la Gerencia de Seguridad de la Información.

x) Se debe restringir el uso de la cuenta de usuario a determinados días y horas, conforme la operatividad y requerimientos del negocio, siempre y cuando el servicio o el sistema informático lo permita.

y) Se debe cerrar automáticamente la sesión del usuario en el aplicativo o servicio informático que se detecte inactividad durante un lapso de hasta 60 minutos.

z) Los roles de acceso a las aplicaciones deben ser definidos por el responsable de la Unidad Administrativa correspondiente (propietario de la información) con el apoyo de la Gerencia de Tecnologías de la Información y la Gerencia de Seguridad de la Información. Los roles existentes, deben ser validados por los propietarios de la información mínimo cada 12 meses.

aa) Únicamente cuando se traten de usuarios masivos (más de 20) en lugar de presentar los formularios de accesos RPSI-12 de manera individual, el superior jerárquico de la Unidad Administrativa puede hacer la solicitud mediante memorando dirigido a la Gerencia de Seguridad de la Información.

bb) La Gerencia de Talento Humano debe notificar los permisos / novedades de usuarios a la Gerencia de Seguridad de la Información para proceder a inactivar los usuarios por los períodos establecidos.

cc) Es responsabilidad de los superiores jerárquicos gestionar con la anticipación debida la solicitud de accesos, mediante el formulario RPSI-12 del personal alterno, cuando los titulares se encuentran con permisos.

dd) Los funcionarios de la Gerencia de Tecnologías de la Información deben tener roles y/o permisos únicamente de consulta a las aplicaciones que soportan las actividades diarias de los diferentes procesos institucionales. En caso de requerir otro tipo de roles deben ser autorizados por el propietario de la información y la Gerencia de Seguridad de la Información.

ee) El funcionario dispone de n oportunidades para ingresar correctamente la contraseña (parámetro debe iniciar con el valor de 3 pero puede modificarse por la Gerencia de Seguridad de la Información), luego de las cuales el sistema bloquea automáticamente la cuenta.

ff) No se pueden crear usuarios genéricos de ingreso a los aplicativos, red o correo, salvo alguna excepción justificada y debidamente autorizada por la Gerencia de Seguridad de la Información.

**Responsabilidades del Usuario**

gg) El usuario de los recursos informáticos es responsable por el uso que dé a su cuenta, está obligado a mantener la confidencialidad y reserva de su contraseña y a cambiarla periódicamente.

hh) Los usuarios de las diferentes aplicaciones y de la red son los únicos responsables del ingreso, actualización y calidad de los datos, controlados por las aplicaciones informáticas en producción.

ii) Todas las transacciones en los sistemas de información realizados con una cuenta de usuario y contraseña, son de responsabilidad del funcionario propietario de la cuenta.

jj) La contraseña inicial otorgada por el Administrador de Usuarios, debe ser cambiada inmediatamente por una contraseña personalizada por el usuario. Las contraseñas deben tener un tiempo de caducidad definido por la Gerencia de Seguridad de la Información.

kk) Las contraseñas son de uso personal e intransferible en todo momento; manejadas por el funcionario como información confidencial, en caso de compartir o divulgar las claves se considera como falta grave.

ll) Los usuarios de los recursos informáticos deben utilizar contraseñas fuertes, que no puedan ser adivinadas por otros, de acuerdo a la política de Administración de contraseñas.

mm) Es responsabilidad del usuario si considera que su clave ha perdido confidencialidad, cambiar su contraseña o solicitar al Administrador de Usuarios la asignación de una nueva clave.

nn) Las contraseñas no deben ser escritas o registradas en documentos o lugares donde puedan ser observadas por otras personas.

oo) Una vez concluida la jornada laboral, es obligación de los funcionarios apagar su computadora y equipos informáticos a su cargo.

pp) El ambiente de escritorio de las computadoras debe estar estandarizado con un solo papel tapiz y protector de pantalla, en los que consta el logo de la CFN B.P.

qq) El funcionario está prohibido de cambiar cualquier tipo de configuración de la computadora.

rr) Las aplicaciones y/o utilitarios deben ser utilizados solo por los funcionarios autorizados y para realizar funciones inherentes a su cargo.

ss) El usuario debe asegurarse de respaldar frecuentemente la información considerada como crítica para el cumplimiento de sus labores y garantizar la supervivencia de la misma, por la cual responde ante la institución. Dichos respaldos deben ser efectuados con el mecanismo y procedimiento que defina la Gerencia de Tecnologías de la Información, para lo cual esta Gerencia debe tomar en cuenta la disponibilidad de la información, tanto en las oficinas locales como en el sitio alterno definido en el Plan de Continuidad del Negocio.

tt) La información considerada como crítica es la definida por el Plan de Continuidad del Negocio y la Clasificación de la Información, debe estar estrictamente relacionada con las tareas institucionales asignadas al funcionario. Los funcionarios están expresamente prohibidos de colocar información que no tenga que ver con el trabajo y/o respaldarla en cualquier medio de almacenamiento. En particular, cualquier tipo de información multimedios como audio (formato mp3, wav, y otros), imágenes (formatos jpg, bmp y otros) y video (formato avi, mpg y otros), no debe ser respaldada, a menos que cuente con la autorización expresa de la Gerencia de Seguridad de la Información.

uu) Todo usuario, sin excepción, de los servicios informáticos, debe suscribir el Acuerdo de Confidencialidad y reserva de la Información (Anexos 1 y 3), que debe ser gestionado por la Gerencia de Talento Humano.

vv) En el caso de proveedores, deben suscribir adicionalmente el Compromiso de Confidencialidad, el cual debe ser gestionado por el superior jerárquico de la Unidad Administrativa y de manera coordinada con la Gerencia de Seguridad de la Información

ww) El funcionario puede solicitar a la Gerencia de Seguridad de la Información, un reporte del uso de sus cuentas de usuario, a fin de supervisar la actividad normal, así como alertar oportunamente sobre actividades inusuales si fuere el caso.

xx) Se puede bloquear automáticamente la sesión de red del usuario del equipo si se detecta inactividad durante un lapso de hasta 10 minutos, y se desbloquea únicamente si el usuario ingresa nuevamente su clave.

yy) La Institución adopta la política de escritorios y pantallas limpias para los documentos, medios de almacenamientos removibles y para los medios de procesamiento de la información, se debe considerar las siguientes directrices para el cumplimiento de esta política:

- Cada funcionario debe mantener bajo llave la información sensible (cajas fuertes o gabinetes) que este bajo su responsabilidad, en especial cuando no la esté utilizando y/o no se encuentre en su puesto de trabajo.
- El usuario tiene la responsabilidad de desconectar de la red, servicio o sistema las computadoras personales, terminales, impresoras asignadas a funciones críticas, cuando no esté haciendo uso de las mismas.
- La Gerencia Administrativa debe mantener a través de las Unidades Administrativas de su competencia un control de acceso especial para los sitios restringidos.
- Para proteger la información de accesos no autorizados, los funcionarios deben retirar información sensible de copiadoras, impresoras, fax, entre otros, así mismo no deben tener claves pegadas en sus escritorios y/o pantallas.
- Cada funcionario es responsable de retirar los dispositivos removibles una vez que se hayan dejado de utilizar.

**Control de Accesos a la Red y Sistemas Operativos**

zz) El uso de la infraestructura y servicios de red por parte de los usuarios informáticos, debe ser consecuente con los propósitos y fines de la Corporación Financiera Nacional B.P.

aaa) El funcionario debe utilizar la infraestructura de red para el intercambio de información, cuyo contenido únicamente sea laboral.

bbb) El funcionario debe utilizar eficientemente la red, con el fin de evitar en la medida de lo posible la congestión y degradación de los servicios asociados o que dependen de la infraestructura de red.

ccc) Todo usuario al encender o reiniciar su computador en las instalaciones de la institución debe ingresar a la red con su cuenta de usuario y contraseña asignadas, no en modo estación de trabajo.

ddd) No se permite el uso de equipo de propiedad privada que no esté bajo el control y monitoreo de la institución para acceder a la red interna de la CFN B.P.

eee) En el caso de requerir la creación de una carpeta compartida en equipos centralizados, la Unidad Administrativa requirente debe solicitar mediante formulario de Accesos Informáticos, con la autorización correspondiente del propietario de la información y la Gerencia de Seguridad de la Información.

fff) La Gerencia de Seguridad de la Información (podría ser en coordinación con la Gerencia de Tecnologías de la Información), puede supervisar el tráfico de la red y el uso del servicio de todos los usuarios con el propósito de verificar su apropiado uso, operación correcta del sistema o distribución justa de los recursos de red.

ggg) La Gerencia de Tecnologías de la Información debe asegurar y mantener los sistemas operativos actualizados con los últimos parches de seguridad tanto en las estaciones de trabajo como en servidores. La Gerencia de Seguridad de la Información realizará la validación correspondiente.

hhh) La Gerencia de Tecnologías de la Información debe implementar los programas necesarios para proteger a la Institución contra software malicioso, como antivirus, anti-spyware, anti- phishing y otros, bajo la coordinación de la Gerencia de Seguridad de la Información.

iii) Es responsabilidad de la Gerencia de Tecnologías de la Información mantener actualizado y estandarizado las herramientas y utilitarios informáticos, incluyendo el antivirus.

jjj) Únicamente la Gerencia de Tecnologías de la Información puede usar programas de tipo firewall en las estaciones de trabajo o servidores de la institución, bajo la coordinación de la Gerencia de Seguridad de la Información.

kkk) Todas las estaciones las estaciones de trabajo deben disponer de un firewall local activo con el fin de evitar ataques, intrusiones y aplicaciones maliciosas que intenten establecer conexiones remotas, para lo cual la Gerencia de Tecnologías de la Información debe implementar los mecanismos técnicos y de control necesarios.

lll) La Gerencia de Tecnologías de la Información debe garantizar una adecuada administración de sitios y/o zonas de confianza a través del firewall local implementado en las estaciones de trabajo, bajo la coordinación de la Gerencia de Seguridad de la Información.

mmm) Se debe otorgar acceso al Internet a todos los funcionarios de la CFN B.P. con nombramiento, contrato de servicios ocasionales, honorarios profesionales o en comisión de servicios, pasantes o terceros de acuerdo a su cargo y roles establecidos por el propietario de la información.

nnn) La Gerencia de Seguridad de la Información es la encargada de autorizar los cambios de perfiles de internet, con el formulario de accesos, en el cual consten las firmas respectivas del superior jerárquico y/o propietario de la información.

ooo) Durante el horario habitual de labores y fuera del horario de trabajo, el acceso a Internet es con fines laborales, legales, morales y que no perjudiquen a la institución.

**Uso aceptable de servicios de red y sistemas de información**

- Usar el equipo de procesamiento de información, los servicios de red y sistemas de información solo para fines laborales.

**Uso inaceptable de servicios de red y sistemas de información (Se considera falta grave)**

- Instalar software no licenciado o no autorizado por la Gerencia de Tecnologías de la Información.
- Cambiar las configuraciones estándares de los equipos de procesamiento.
- Obtener la información de los sistemas de la CFN B.P., para uso y provecho personal.
- Colocar información que no tenga que ver con el trabajo en los directorios compartidos, de respaldo o en cualquier medio de almacenamiento.
- Ejecutar programas de escaneo de puertos TCP/UDP, uso de técnicas de enumeración, obtención de información interna de la configuración de la red, ataques de negación de servicio (DoS), obtención de contraseñas vía ataques de fuerza bruta, entre otros.
- Iniciar su PC en modo estación de trabajo

**Control de Acceso a las aplicaciones y a la información**

ppp) El acceso lógico a las aplicaciones informáticas y a la información debe estar limitado a los usuarios autorizados, los sistemas de aplicación deben controlar el acceso de usuarios a la información y a las funciones de los sistemas, de acuerdo con la política de control de accesos.

qqq) Por necesidades institucionales y luego de un análisis por parte del propietario de la información, se puede declarar a una aplicación como sensible, para el efecto, dicha aplicación puede ejecutarse en un ambiente separado.

**Monitoreo de Accesos**

rrr) La Gerencia de Seguridad de la Información debe evaluar en forma permanente el uso adecuado de las cuentas de usuario, contraseñas, roles/perfiles y otros recursos informáticos asignados.

sss) La Gerencia de Seguridad de la Información, debe realizar revisiones periódicas a la configuración de las computadoras, equipos del centro de cómputo y seguridad perimetral para evaluar la correcta aplicación de las políticas.

**Computadores Portátiles y de Escritorio**

ttt) Cada usuario es responsable por el equipo asignado, software utilizado, datos contenidos en él y utilitarios que opere.

uuu) El usuario debe salir de las aplicaciones y/o utilitarios al momento de abandonar el sitio de trabajo temporalmente o al final del día, adicionalmente, debe dejar protegida su estación de trabajo usando la contraseña de protección de pantalla.

vvv) Se prohíbe a los funcionarios de la institución usar el equipo de cómputo para realizar actos que perjudiquen el funcionamiento del mismo o deterioren la información almacenada en medios magnéticos, ópticos, etc.

www) La Gerencia de Tecnologías de la Información es la responsable de la instalación, desconexión, mantenimiento y reubicación de los equipos de la infraestructura tecnológica (de manera coordinada con la Gerencia Administrativa) de la CFN B.P.

xxx) En caso de que una Unidad Administrativa, requiera instalar aplicaciones de otras entidades (proveedoras de servicios), la instalación debe estar coordinada con la Gerencia de Tecnologías de la Información y la Gerencia de Seguridad de la Información.

yyy) La Gerencia de Seguridad de la Información debe conceder el permiso de administración de las computadoras, únicamente al personal designado por la Gerencia de Tecnologías de la Información, a fin de evitar que los usuarios cambien las configuraciones oficiales de la institución; siempre y cuando las herramientas y los aplicativos lo permitan.

zzz) En caso de requerir acceso inalámbrico en los equipos portátiles institucionales, éstos deben ser configurados para permitir solamente acceso a través de las redes inalámbricas propias de CFN B.P., fuera de las oficinas de la CFN B.P. se permite la conexión a redes inalámbricas disponibles (siempre y cuando no perjudiquen a la seguridad de la información). Para el efecto la Gerencia de Tecnologías de la Información debe implementar los mecanismos y procedimientos necesarios.

aaaa) Si un funcionario abandona su oficina, es su responsabilidad cerrarla cuando sea posible, y prever la seguridad del hardware y software, a fin de evitar o minimizar posibles robos o daños.

bbbb) Si a un funcionario se le asigna un computador portátil, es su responsabilidad guardar en un escritorio o anaquel con las seguridades correspondientes, o llevarlo consigo, si está autorizado para ello.

cccc) Todo funcionario que usa un computador portátil, en su sitio de trabajo debe tener cables y candado de seguridad para asegurar el equipo, quedando bajo su responsabilidad el mantener la seguridad del equipo asignado.

dddd) Es responsabilidad del funcionario que esté de viaje o trabaje fuera de su oficina, mantener consigo el equipo portátil que le ha sido asignado, con las seguridades y precauciones que sean del caso.

eeee) Si el funcionario necesita retirar un equipo de las oficinas (como por ejemplo, estación de trabajo, proyector, etc.), debe proceder de acuerdo a los procedimientos definidos por la Gerencia Administrativa.

ffff) La Gerencia de Tecnologías de la Información debe implementar los mecanismos de cifrados de información correspondientes en las estaciones de trabajo de los usuarios, de manera coordinada con la Gerencia de Seguridad de la Información (previamente establecidos con los propietarios de la información).

**Control de Redes Inalámbricas WIFI:**

gggg) Acceso inalámbrico para la Alta Gerencia:

- Debe ser de uso exclusivo de la Alta Gerencia (Presidente del Directorio, Gerente General, Subgerentes Generales, Gerentes Regionales, Gerentes, Subgerentes de Unidades Administrativas y asesores autorizados por el Gerente General.
- Puede acceder a la red inalámbrica por medio de cualquier dispositivo.
- Debe estar disponible únicamente en las áreas donde se ubiquen las oficinas de la Alta Gerencia.
- Debe habilitarse los servicios de acceso a la red LAN e Internet sin restricciones.

hhhh) Acceso inalámbrico para funcionarios de CFN B.P. en general, debe considerar:

- El único dispositivo autorizado para esta conexión son computadores portátiles institucionales.
- Acceso por dirección física (MAC).
- Se habilitan servicios de acceso a la red LAN e internet.
- Los funcionarios deben mantener los mismos accesos que poseen en la red LAN.
- Se debe solicitar por medio del formulario de usuarios y accesos.

iiii) Acceso inalámbrico para proveedores de CFN B.P., debe considerar:

- Se debe solicitar por medio del formulario de usuarios y accesos.
- La conexión a la red CFN B.P., debe estar limitada a los recursos o ambientes necesarios que les permita cumplir los trabajos contratados.
- El único dispositivo autorizado para esta conexión son equipos portátiles, el mismo que debe tener al menos un antivirus instalado-actualizado y parches actualizados del sistema operativo.

- En caso de detectarse que el equipo del proveedor tiene instalado programas considerados de alto riesgo para CFN B.P., no se permite el acceso, tales programas pueden ser herramientas de denegación de servicios, escaneo de puertos, sniffers, keyloggers, aplicativos p2p, entre otros.
- Se brinda servicio de Internet controlado.
- El acceso concedido a proveedores debe ser temporal. Una vez que el usuario ya no deba estar activo, debe ser notificado de manera obligatoria por el responsable de la Unidad Administrativa a la Gerencia de Seguridad de la Información.

jjjj) Acceso inalámbrico para invitados de CFN B.P., debe considerar:

- Registrar el acceso mediante enrolamiento del usuario, con el formulario de usuarios y accesos.
- El único dispositivo autorizado para esta conexión son equipos portátiles, el mismo que debe tener al menos un antivirus instalado-actualizado y parches actualizados del sistema operativo.
- En caso de detectarse que el equipo del proveedor tiene instalado programas considerados de alto riesgo para CFN B.P., no se debe permitir el acceso, tales programas pueden ser herramientas de denegación de servicios, escaneo de puertos, sniffers, keyloggers, aplicativos p2p, entre otros.
- El único servicio habilitado debe ser de Internet controlado. Las configuraciones que sean del caso, deben ser ejecutadas por la Gerencia de Tecnologías de la Información, bajo la coordinación de la Gerencia de Seguridad de la Información.
- No debe acceder a la red LAN de CFN B.P. El acceso concedido es de 1 día.

kkkk) Acceso inalámbrico para salas de reuniones, debe considerar:

- Registrar el acceso mediante contraseña establecida en la sala.
- En caso de detectarse que el equipo del proveedor tiene instalado programas considerados de alto riesgo para CFN B.P, no se permitirá el acceso, tales programas pueden ser herramientas de denegación de servicios, escaneo de puertos, sniffers, keyloggers, aplicativos p2p, entre otros.
- El único servicio habilitado debe ser de Internet controlado. No pueden acceder a la red LAN de CFN B.P.
- El acceso concedido es de 30 días.

Complementario a los tipos de usuarios que pueden acceder a los servicios de red inalámbrica de CFN B.P., la Gerencia de Tecnologías de la Información debe brindar el acceso a los dispositivos móviles bajo las siguientes características:

llll) Dispositivos PDA:

- Acceso por dirección física (MAC)
- El acceso a la red LAN de CFN B.P., está limitada a la conexión con los aplicativos de negocio que hagan uso de este dispositivo.
- No se debe habilitar el servicio de internet.

mmmm) Dispositivos móviles (teléfonos inteligentes y tablets):

- Servicio de uso exclusivo para Gerentes de Sucursal / Área, Subgerentes y Asesores autorizados por el Gerente General.
- Se permite el acceso de dispositivos móviles personales. Acceso por dirección física (MAC).
- Se permite el acceso a la red LAN de CFN B.P., para los servicios de Internet, correo electrónico institucional, sistema de video conferencia y/o comunicaciones unificadas.
- Servicio de Internet controlado.

**Consideraciones Generales:**

nnnn) Los propietarios de la Información, en coordinación con la Gerencia de Seguridad de la Información, son los responsables de categorizar los funcionarios que pueden hacer uso del correo institucional vía web, a través de dispositivos móviles tales como: Smartphone, Tablet, Laptop; entre otros, para lo cual, la Gerencia de Tecnologías de la Información con la finalidad de mantener la confidencialidad, seguridad e integridad de la información debe establecer los mecanismos de seguridad correspondientes.
oooo) Los usuarios de la red Wireless al acceder al servicio provisto por la CFN B.P., autorizan a que la Gerencia de Tecnologías de la Información, mediante los mecanismos necesarios instalen aplicativos de seguridad, gestión, control y monitoreo en los dispositivos móviles (Smartphone, Tablet, Laptop; entre otros), los cuales están orientados a fortalecer los niveles de seguridad, la administración de los dispositivos móviles (MDM) y el correcto uso de los mismos dentro de la red Wireless de la CFN B.P.; excluyéndose de lo expuesto, la red Wifi asignada a la Alta Gerencia de la Institución.

**Trabajo Remoto:**

pppp) La Gerencia de Seguridad de la Información debe monitorear los accesos realizados vía trabajo remoto.

qqqq) Los propietarios de la información, de manera conjunta con la Gerencia de Seguridad de la Información, deben autorizar el uso del servicio de "conexión remota" mediante el formulario de usuarios y accesos.
rrrr) El funcionario debe observar la seguridad física de la edificación y del entorno local existente en el sitio de trabajo remoto, protegiéndolo contra cualquier contingencia o accidente.
ssss) Cada funcionario es responsable de evitar la conexión remota a través de redes inalámbricas desconocidas/expuestas, que no presten la seguridad de acceso y autenticación adecuada.
tttt) En todo trabajo remoto debe aplicarse la confidencialidad de la información que se conserva, los sistemas y servicios internos para los cuales está autorizado
uuuu) El usuario al establecer una conexión remota, es el responsable de considerar la protección de antivirus con el fin de evitar ataques e intrusiones
vvvv) Es responsabilidad del usuario que realiza el trabajo remoto el correcto uso de este servicio

## CAPÍTULO VI: DE LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

**Artículo 23.- Generalidades:**

a) La Gerencia de Tecnologías de la Información debe establecer y mantener actualizados políticas y procedimientos formales para la adquisición, desarrollo y mantenimiento de los sistemas de información que contemplen validación de datos de entrada, de salida, control de procesamiento interno, integridad de los mensajes y control de cambios a fin de garantizar el correcto procesamiento de la información, bajo la coordinación de la Gerencia de Seguridad de la Información.
b) La Gerencia de Tecnologías de la Información, debe establecer y mantener actualizados políticas y procedimientos para separar los ambientes de los sistemas de información (producción, contingencia, pruebas, desarrollo); contemplando además la protección adecuada de los datos de producción que fueren destinados para pruebas; bajo la coordinación de la Gerencia de Seguridad de la Información.
c) La Gerencia de Tecnologías de la información, debe utilizar sistemas y técnicas criptográficas para la protección de la información que se considera en estado de riesgo y para la cual otros controles no suministran una adecuada protección.

d) La Gerencia de Seguridad de la Información, debe establecer los requisitos mínimos de seguridad para los aplicativos informáticos y debe revisarlos previo a su puesta en producción, como parte de la aceptación del producto.

**Artículo 24.- Tratamiento correcto de las aplicaciones:**

e) La Gerencia de Tecnologías de la Información debe contemplar para el desarrollo de aplicaciones web y de escritorio la custodia de los datos de entrada, así como debe garantizar la seguridad en la información transmitida, para lo cual se debe hacer uso de mecanismos de seguridad tales como, certificados digitales y/o firmas electrónicas, entre otros que se considere.
f) Los usuarios son los responsables de validar la información de entrada y salida de los sistemas de información, empleando las comprobaciones que estime necesarias para garantizar la consistencia de la misma.
g) La Gerencia de Tecnologías de la Información debe contar con un instructivo para el desarrollo interno o para la adquisición de software web, el cual debe estar basado en las mejores prácticas de la industria en cuanto a codificación segura.

**Artículo 25.- Controles Criptográficos:**

h) Por necesidades institucionales y mediante la solicitud del propietario de la información, se puede emplear técnicas criptográficas sobre información sensible a fin de evitar el uso inadecuado o incorrecto de la información.
i) Banca Electrónica: Todos los sistemas que realicen transacciones de los clientes a través de la banca electrónica deben estar protegidos mediante el uso de controles criptográficos de acuerdo a lo establecido por el propietario de la información en coordinación con la Gerencia de Seguridad de la Información. Los sitios o páginas publicadas en internet en las que requieran autenticación del usuario deben usar certificados digitales.
j) Archivos / Discos: La información clasificada como confidencial por el propietario de la información y en coordinación de la Gerencia de Seguridad de la Información, debe estar encriptada a nivel de archivos Los equipos portátiles con información confidencial y que salgan de la institución deben estar encriptados a nivel del disco duro.
k) Correo Seguro; La información confidencial o sensible debe ser transmitida a través de la plataforma de correo seguro con que cuenta la Institución. En aquellos casos que la información supere el tamaño establecido en la plataforma de correo seguro se debe utilizar el servicio de colaboración con que cuenta la Institución implementada por la Gerencia de Tecnologías de la Información.

**Artículo 26.- Seguridad en los procesos de desarrollo y soporte:**

l) La Gerencia de Tecnologías de la Información debe documentar e implantar una metodología para el correcto desarrollo de los sistemas de información que garantice la calidad del código fuente y que la funcionalidad en el procesamiento de información esté acorde a las necesidades del negocio.
m) La Gerencia de Tecnologías de la Información debe documentar e implantar un procedimiento formal para el control de cambios que garantice la correcta y continua operación del negocio.
n) La Gerencia de Tecnologías de la Información debe implantar los mecanismos necesarios para mantener un adecuado control de versionamiento sobre los sistemas de información.
o) Las Gerencia de Tecnologías de la Información debe mantener un inventario resumen de los sistemas de información y aplicaciones comerciales que la soportan con la descripción y versión correspondiente, el mismo que debe residir en un ambiente seguro.

p) La implementación de los sistemas de información se deben llevar a cabo minimizando la discontinuidad de las actividades de la Institución.
q) Todo sistema de información debe contar con la documentación técnica y de usuario debidamente actualizada por la Gerencia de Tecnologías de la Información.

**Artículo 27.- Gestión de la vulnerabilidad técnica**

r) Antes de la salida a producción de un aplicativo, La Gerencia de Tecnologías de la Información debe entregar a la Gerencia de Seguridad de la Información, el informe de vulnerabilidades a nivel de código. El aplicativo se puede poner en producción con la autorización correspondiente de la Gerencia de Seguridad de la Información.
s) La Gerencia de Seguridad de la Información puede hacer revisiones a nivel de vulnerabilidades de código de los aplicativos en producción y de encontrar vulnerabilidades relevantes puede solicitar a la Gerencia de Tecnologías de la Información las correcciones que sean del caso.
t) En caso de encontrar riesgos de seguridad en los aplicativos informáticos, la Gerencia de Seguridad de la Información, debe hacer el seguimiento respectivo a los Planes de Remediación correspondientes, que deben ser acordados previamente con la Gerencia de Tecnologías de la Información.
u) La Gerencia de Seguridad de la Información debe realizar como mínimo una vez al año una prueba de vulnerabilidad y penetración a la infraestructura institucional; y, en caso de que se realicen cambios en la plataforma que pudieran afectar significativamente a la seguridad, debe efectuar una prueba adicional. Complementariamente, se debe realizar un análisis comparativo de los resultados de la prueba actual respecto de la inmediata anterior.
v) Las pruebas de vulnerabilidad y penetración deben ser efectuadas por personal independiente a la CFN B.P., de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional.
w) Con los resultados de las pruebas de vulnerabilidad y penetración, la Gerencia de Seguridad de la Información, debe solicitar a la Gerencia de Tecnologías de la Información establecer los planes de acción sobre las vulnerabilidades detectadas. La Gerencia de Tecnologías de la Información es responsable de la implementación y ejecución de los planes de remediación, mientras que la Gerencia de Seguridad de la Información es la responsable de hacer el seguimiento respectivo.
x) Los resultados de las pruebas de vulnerabilidad y penetración, sus planes de acción e implementaciones realizadas, deben estar a disposición de los organismos de control que los requieran formalmente, cumpliendo los procedimientos y normativas de CFN B.P. para el efecto.

**Artículo 28.- Política de Fuga de Información**

y) El único software autorizado para su uso en las estaciones de trabajo y portátiles de la institución, es el instalado por la Gerencia de Tecnologías de la Información, siendo ésta la responsable de implementar los mecanismos necesarios para controlar la instalación de aplicativos autorizados con sus respectivas licencias. La Gerencia de Tecnologías de la Información, a pedido de los usuarios, no puede instalar software personal en los equipos, ni instalar software no licenciado legalmente, con excepción del software bajo licencia del tipo GNU GPL (Licencia pública general de GNU), siempre y cuando haya sido autorizado por la Gerencia de Seguridad de la Información.
z) No está autorizado el uso de hardware de comunicación integrado o no, que disponen las estaciones de trabajo, tales como: Bluetooth, infrarrojos, Irda, entre otros, a excepción de los utilizados para la conexión a la red corporativa como acceso cableado y Wi-Fi. La Gerencia de Tecnologías de la Información debe implementar los mecanismos necesarios que permitan controlar el uso no autorizado de este tipo de hardware.
aa) La Gerencia de Tecnologías de la Información debe garantizar la confidencialidad de la información considerada como sensible (definida por los propietarios de la información en coordinación con la Gerencia de

Seguridad de la Información) que reside en los discos duros de las estaciones de trabajo; así como de la totalidad de la información contenida en los discos duros de los equipos portátiles asignados a los funcionarios de la CFN B.P aplicando técnicas de cifrado de datos, para lo cual se debe establecer el procedimiento que defina los aspectos técnicos para este fin.

bb) La Gerencia de Tecnologías de la Información debe implementar los mecanismos correspondientes que permita conectar a las estaciones de trabajo únicamente dispositivos de almacenamiento que hayan sido entregados por la Institución, registrados y autorizados por la Gerencia de Seguridad de la Información a los funcionarios, con permisos de lectura y/o escritura, tales como: memoria externa, discos.

cc)Para el caso de unidades ópticas como CD o DVD se debe permitir el acceso de solo lectura y de requerirse permisos de escritura debe ser plenamente justificado y autorizado formalmente por la Gerencia de Seguridad de la Información, en coordinación con los superiores jerárquicos. La Gerencia de Tecnologías de la Información debe implementar los mecanismos y procedimientos necesarios para este fin.

dd) Las estaciones de trabajo que se encuentren dentro de las instalaciones de la CFN B.P. deben hacer uso únicamente de recursos / servicios tecnológicos que sean provistos por la institución.

ee) Las estaciones de trabajo que se encuentren fuera de las instalaciones de la CFN B.P. deben mantener activa las configuraciones que permitan garantizar el cumplimiento de las políticas de seguridad de la Institución.

ff) La Gerencia de Tecnologías de la Información debe controlar la información almacenada en los recursos informáticos y sistemas de transmisión de datos, de tal forma que se prevea la fuga de información, de manera coordinada con la Gerencia de Seguridad de la Información.

gg) La Gerencia de Tecnologías de la Información mediante las herramientas que disponga debe prevenir y restringir el acceso no autorizado en la red, de manera coordinada con la Gerencia de Seguridad de la Información.

hh) Es de competencia del personal de la Gerencia de Tecnologías de la Información examinar los códigos fuentes (de acuerdo al procedimiento de aseguramiento y control de calidad) y entregar los resultados a la Gerencia de Seguridad de la Información. Los aplicativos se ponen en producción únicamente con la autorización de la Gerencia de Seguridad de la Información.

ii) La Gerencia de Tecnologías de la Información debe controlar el acceso y las modificaciones al código instalado, de acuerdo al procedimiento de aseguramiento y control de calidad, en coordinación con la Gerencia de Seguridad de la Información.

jj) La Gerencia de Tecnologías de la Información debe contar con un software o debe utilizar herramientas que permita detectar y bloquear cualquier tipo software con código malicioso. En caso que se presente un evento de este tipo, debe ser notificado inmediatamente a la Gerencia de Seguridad de la Información.

## CAPÍTULO VII: SOBRE EL USO DE FIRMAS ELECTRÓNICAS

**Artículo 29.- Generalidades:**

a) Es responsabilidad de los servidores y servidoras de CFN B.P. verificar mediante procesos automatizados de validación, que el certificado de la firma electrónica recibida sea emitido por una entidad de certificación de información acreditada y que el mismo se encuentre vigente.

b) Si los usuarios no tienen conocimiento sobre los tipos de firmas electrónicas, pueden solicitar asesoramiento a la Gerencia de Seguridad de la Información. El objetivo es que exista uniformidad y compatibilidad en el uso de la firma electrónica a nivel interinstitucional.

c) La conservación de los archivos electrónicos o mensajes de datos firmados electrónicamente, es responsabilidad del usuario o titular del certificado.

d) El certificado de firma electrónica es personal e intransferible.

e) La veracidad de la exactitud de las declaraciones emitidas a la entidad certificadora, es responsabilidad del usuario al acreditarse el certificado para firma electrónica, por lo que el titular del certificado debe notificar cualquier cambio, modificación o variación de los datos que constan en la información proporcionada para la emisión del certificado.

f) El titular de la firma electrónica es el encargado de notificar a la Entidad de Certificación cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente; de manera que se solicite oportunamente la cancelación del mismo.

g) La Gerencia de Seguridad de la Información no almacena ni asigna la CONTRASEÑA o clave, por tanto su olvido implica que el titular de la firma electrónica debe gestionar la solicitud de cambio de contraseña o revocación de la firma electrónica directamente con la Entidad de Certificación.

h) El titular del certificado es el encargado de responder por el uso del Certificado de Firma Electrónica y de las consecuencias que se deriven de su utilización.

i) Es responsabilidad del titular de la firma electrónica gestionar con la Entidad de Certificación la renovación de la misma.

j) La Gerencia de Talento Humano y/o Secretaría General debe adoptar las medidas necesarias para incentivar el uso de firma electrónica en los procesos de negocio de la CFN B.P. con el fin de procurar un manejo de cero papeles.

k) La Gerencia de Seguridad de la Información, debe incluir en el plan de concienciación temas relacionados al uso y responsabilidad de firma electrónica.

l) Las demás contempladas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento.

## CAPÍTULO VIII: DE LA GESTIÓN DE LA CONTINUIDAD DE LOS NEGOCIOS

**Artículo 30.- Generalidades:**

a) La Gerencia de Riesgos debe desarrollar e implementar un plan de continuidad del negocio para garantizar la disponibilidad de la información y continuidad de las operaciones, ante una interrupción o fallos de los procesos críticos de negocio ocasionado por eventos de cualquier índole.
b) El plan de continuidad del negocio debe probarse y actualizarse periódicamente para asegurar vigencia y efectividad.
c) La administración de la continuidad del negocio debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

**Artículo 31.- Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio:**

d) El Plan de Continuidad del Negocio debe contemplar los aspectos relacionados con Seguridad de la Información, de responsabilidad de la Gerencia de Seguridad de la Información.
e) La Alta Gerencia debe garantizar que la Corporación Financiera Nacional B.P. cuente con un proceso para la continuidad del negocio a través de toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad de la organización.
f) La Gerencia de Tecnologías de la Información debe implementar una infraestructura tecnológica para optimizar la comunicación, almacenamiento y procesamiento de datos que garantice la continuidad operacional del negocio, la confidencialidad, integridad y calidad de la información, de acuerdo al Plan de Continuidad del Negocio y de manera coordinada con la Gerencia de Seguridad de la Información, responsable de emitir políticas, procedimientos y directrices en su ámbito de gestión.
g) La Gerencia de Tecnologías de la Información debe considerar y garantizar que las condiciones de seguridad bajo las cuales se solicita la obtención directa y oportuna de cualquier dato o información que se necesite, sea para sus propios fines o para cumplir con los requerimientos de las autoridades competentes, sin crear situaciones que retrasen los procedimientos normales y de manera coordinada con la Gerencia de Seguridad de la Información, responsable de emitir políticas, procedimientos y directrices en su ámbito de gestión.
h) La Gerencia de Riesgos debe trabajar en la elaboración del Plan de Continuidad del Negocio, bajo las consideraciones de la Gerencia de Tecnologías de la Información y de la Gerencia de Seguridad de la Información. La Gerencia de Tecnologías de la Información debe elaborar el Plan de Contingencia de Tecnologías de la Información.
i) Es de responsabilidad de la Gerencia Administrativa garantizar la protección y seguridad del personal, tanto en situación normal como en situación de contingencia.
j) La Gerencia de Tecnologías de la Información, se responsabiliza de la gestión de los planes de contingencia, los cuales son claves para mantener la operatividad de los procesos considerados críticos para la Institución y de manera coordinada con la Gerencia de Seguridad de la Información, responsable de emitir políticas, procedimientos y directrices en su ámbito de gestión, incluyendo las estrategias de seguridad de la información que estén alineadas a las estrategias institucionales para mantener actualizado el sistema de gestión de seguridad de la información, manteniendo la independencias de las diferentes unidades administrativas de la institución .
k) La Gerencia de Riesgos garantiza que los Planes de Continuidad de Negocio se desarrollen e implanten de forma adecuada, teniendo en cuenta todas las Unidades Administrativas, proveedores y servicios críticos.

l) La Gerencia de Riesgos debe garantizar que todo el personal de las distintas Unidades Administrativas de la institución esté informado de las responsabilidades que le competen en el marco de la Continuidad de Negocio, mediante labores periódicas de formación, divulgación y prueba de los Planes de Continuidad de Negocio.
m) La Gerencia de Tecnologías de la Información debe asegurar que los procesos críticos sean recuperados dentro de los márgenes de tiempo requeridos en los Planes de Continuidad y contingencia de la institución.
n) La Gerencia de Riesgos debe garantizar la promoción, divulgación y actualización de la capacidad de Continuidad de Negocio dentro de la cultura de la Institución, al igual que el impacto de los Planes de Continuidad de Negocio en el desarrollo de la Organización.

**Artículo 32.- Evaluación de riesgo del Plan de Continuidad del Negocio:**

o) Dentro del plan de Continuidad del Negocio, la Gerencia de Riesgos en coordinación con la Gerencia de Tecnologías de la Información y la Gerencia de Seguridad de la Información, deben realizar una evaluación formal de riesgo, o análisis de impacto sobre el negocio (BIA- Business Impact Assessment), con el fin de determinar los requerimientos del Plan de Continuidad del Negocio e identificar eventos que puedan causar interrupciones a los procesos de negocio. Los dueños de los procesos del negocio, deben evaluar y analizar todos sus procesos (equipamiento, personas, tareas, departamentos, mecanismos de comunicación, proveedores, entre otros) y no limitarse exclusivamente a los recursos e infraestructura asociado a los sistemas de información
p) La Gerencia de Riesgos debe identificar y valorar el impacto de las interrupciones de los procesos, aplicaciones y servicios Informáticos, para cuantificar y calificar los impactos y saber sus efectos, asimismo debe poder identificar el tiempo máximo de interrupción permitida para a cada servicio o aplicación crítica.
q) La Gerencia de Riesgos debe identificar, analizar y priorizar las vulnerabilidades asociadas a cada activo, de manera conjunta con los propietarios de la información y la Gerencia de Seguridad de la Información, así como el impacto que pueda provocar sobre la disponibilidad de la información y paralización de las actividades de la CFN B.P., se debe crear una estrategia de gestión de control de riesgos y el plan de acción.

**Artículo 33.- Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información:**

r) La Gerencia de Riesgos, la Gerencia de Tecnologías de la Información y la Gerencia Seguridad de la Información deben participar en el desarrollo e implementación de los planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido así como en las escalas de tiempo requeridas después de la interrupción o falla en los procesos críticos del negocio.
s) La Gerencia de Riesgos debe definir los equipos para ejecución del plan, donde se destacan las funciones claves que son realizadas por las diferentes Unidades Administrativas responsables, incluyendo a la Gerencia de Seguridad de la Información, de tal manera de gestionar una adecuada disponibilidad, confidencialidad e integridad de la información, coordinado con los respectivos propietarios de la información:

i. Responsables de respuestas a incidentes; analizan el impacto del incidente.
ii. Logística: Responsable de reunir todos los medios para ayudar a la puesta en operación de las actividades.
iii. Recuperación: puesta en servicio de la infraestructura.

t) Las Unidades Administrativas responsables de la implementación del plan de continuidad del negocio deben desarrollar los procedimientos indicando el objetivo y el alcance, considerando las actividades y los tiempos de recuperación, de manera coordinada con la Gerencia de Riesgos que es responsable del Plan y con la Gerencia de Seguridad de la Información, responsable de gestionar una adecuada disponibilidad, confidencialidad e integridad de la información, coordinado con los respectivos propietarios de la información.

u) La Gerencia de Tecnologías de la Información debe difundir y capacitar al personal responsable en los conceptos que contemplan la continuidad de los servicios informáticos, de manera coordinada con la Gerencia de Riesgos que es responsable del Plan y con la Gerencia de Seguridad de la Información, responsable de gestionar una adecuada disponibilidad, confidencialidad e integridad de la información, coordinado con los respectivos propietarios de la información.

v) Las Unidades Administrativas responsables del Plan de Continuidad del Negocio deben definir las siguientes estrategias con la finalidad de garantizar la disponibilidad, integridad y seguridad de la información:

i. Seleccionar el sitio alterno y de almacenamiento externo
ii. Duplicado de los registros tanto físicos como electrónicos
iii. Estrategia de reinicio de las actividades
iv. Contratos de mantenimiento preventivo y correctivo
v. Estrategia adecuada de respaldos, de aplicarse considerarse la incorporación de RAID en los discos de los servidores - conjunto redundante de discos independientes para procesos de respaldos
vi. De aplicarse, seguros para los activos que se consideren.
vii. Métodos, procedimientos, procesos, entre otras estrategias que conlleven a la recuperación de los servicios.

**Artículo 34.- Estructura para la planificación de la continuidad del negocio:**

w) La Gerencia de Riesgos debe mantener actualizado el "Manual del Sistema de Gestión de Continuidad del Negocio" de tal manera que se garantice que las Unidades Administrativas responsables y partícipes del Plan de Continuidad del Negocio cuenten con los siguientes aspectos:

i. Mantener los documentos de los procesos actualizados, utilizando la Gestión de Cambios.
ii. Crear planes de respuesta a los incidentes.
iii. Definir los calendarios de pruebas e informes.
iv. Definir los acuerdos de niveles de servicios internos y con proveedores
v. Definir los contratos para servicios de recuperación, si fuera el caso
vi. Definir las condiciones para activar los planes que describen el proceso a seguir antes de activar cada plan. Así como sus responsabilidades.
vii. Describir el procedimiento de respaldo para desplazar las actividades esenciales de los servicios informáticos o los servicios de soporte al lugar temporal alterno, y para devolver la operatividad de los procesos en los plazos establecidos.
viii. Describir los procedimientos de reanudación con las acciones a realizar para que las operaciones de los equipos y servicios vuelvan a la normalidad.
ix. Definir los activos y recursos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación de los servicios.
x. Distribuir la política, estrategias, procesos y planes generados

**Artículo 35.- Pruebas, mantenimiento y revisión del Plan de Continuidad del Negocio:**

x) La Gerencia de Riesgos debe garantizar que las Unidades Administrativas responsables y partícipes de las pruebas del Plan de Continuidad del Negocio cumplan con los siguientes aspectos:

i. El Plan de Continuidad del Negocio necesita ser probado periódicamente, verificando los tiempos de respuesta, validez de los procedimientos y capacidad de los responsables, con el fin de garantizar que la Institución entienda claramente como debe ser ejecutado, además que se evalúa su viabilidad y garantiza que los empleados estén familiarizados.

ii. Los diferentes tipos de prueba incluyen:

- Pruebas sobre la mesa de los diferentes escenarios (Por medio del uso de listas de verificación y análisis paso a paso).
- Simulaciones del Plan de Continuidad.
- Pruebas de recuperación técnicas del Plan de continuidad.
- Pruebas de recuperación en sitio alterno.
- Prueba de servicios externos (Energía, comunicaciones etc.).
- Prueba completa, con el fin de evaluar personal, equipos, recursos físicos, para entender su capacidad de soportar interrupciones.
- El periodo de realización de los simulacros para probar el Plan de Continuidad del Negocio no debe mayor a los 6 meses.
- El Departamento de Auditoría Interna debe realizar una auditoría interna con la finalidad de identificar el tipo y alcance de la auditoría a realizar, se debe entregar un plan de medidas correctivas para llevar a cabo las recomendaciones acordadas para ser consideradas en el Plan de Continuidad del Negocio.
- Las Unidades Administrativas responsables deben ejecutar auto-evaluaciones del plan de continuidad del negocio a fin de que esté siempre actualizado y sea éste efectivo.

iii. Deberes y/o compromisos: Las Unidades Administrativas de la Organización encargadas de desarrollar el plan de Continuidad del Negocio tienen la responsabilidad de no faltar a este compromiso, teniendo en cuenta que la Institución pudiera estar expuesta a procesos legales y contractuales, poniendo en riesgo el futuro de las operaciones.

iv. Consideraciones adicionales

- El contar con los recursos humanos y/o financieros suficientes incrementará la probabilidad de éxito del Plan de Continuidad del Negocio.
- Otro factor de éxito del Plan de Continuidad del Negocio es no subestimar el impacto a corto y mediano plazo de incidentes de seguridad de la información, para lo cual se deben establecer las respuestas adecuadas.

## CAPÍTULO IX: DEL CUMPLIMIENTO

**Artículo 36.- Generalidades:**

a) Toda política, norma y procedimiento de la CFN B.P. debe garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales.
b) Todo producto generado por los funcionarios o por terceros para la CFN B.P., es de titularidad de la institución, y por tanto su uso y explotación, están regidos por el Código Orgánico de la Economía Social de los Conocimientos.
c) Se deben respetar los derechos de autor y propiedad intelectual de la información de terceros disponible en cualquier medio y se debe garantizar la protección y privacidad de datos de carácter personal.
d) La Gerencia de Seguridad de la Información periódicamente debe comprobar que los sistemas de información cumplan con las normas de aplicación de seguridad.
e) La información de la Institución debe cumplir con la normatividad de los organismos de control para períodos de conservación y procedimientos de descarte de información, asegurándose que los cambios tecnológicos no dificulten o impidan la recuperación.

**Artículo 37.- Identificación de la Legislación aplicable:**

f) Inventariar todas las normas legales, estatutarias, reglamentarias y contractuales pertinentes para los programas de software, servicio informático y en general todo activo de información que utiliza la CFN B.P.
g) Organizar para cada activo de información las normas legales, estatutarias, reglamentarias y contractuales pertinentes.
h) Considerar las normas y leyes más generales relacionadas a la gestión de los datos e información electrónica en el gobierno; a saber:

i. Constitución de la República del Ecuador.
ii. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
iii. Ley Orgánica de Transparencia y Acceso a la Información Pública.
iv. Ley del Sistema Nacional de Registro de Datos Públicos.
v. Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva.
vi. Ley Orgánica y Normas de Control de la Contraloría General del Estado.
vii. Código Orgánico Monetario y Financiero.
viii. Ley del Sistema Nacional de Archivos.
ix. Otras normas cuya, materia trate sobre la gestión de los activos de información en la entidades de la Administración Pública.

**Artículo 38.- Derechos de Propiedad Intelectual**

i) Se debe adquirir software únicamente a proveedores reconocidos para garantizar que no se violen derechos de propiedad intelectual. Si el software es Libre Opensource se considera los términos de las licencias públicas generales.
j) Se debe implementar mecanismos para concienciar sobre las políticas de software libre o privativo, garantizando la protección de derechos de propiedad intelectual, así mismo se debe reportar el mal uso de los recursos informáticos conforme a lo indicado en las Políticas de Seguridad de la Información y realizar acciones disciplinarias para el personal que las viole.
k) La Gerencia de Tecnologías de la Información puede implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos por parte del personal interno o externo, para poder revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan.
l) La Gerencia de Seguridad de la Información debe monitorear los registros de activos de propiedad intelectual apropiadamente inventariados, así como si ha habido actualizaciones de dicho software, e identificar todos los activos con los requerimientos para proteger los derechos de propiedad intelectual.
m) La Gerencia de Tecnologías de la Información debe custodiar la evidencia de la propiedad de licencias o suscripciones, contratos, discos maestros, manuales y toda la información relevante del software que se utiliza.
n) La Gerencia de Tecnologías de la Información en coordinación con la Gerencia de Seguridad de la Información deben controlar y asegurar que no se exceda el número máximo de usuarios permitidos para un programa de software. Se aplica tanto al software libre como al privativo, donde corresponda.
o) La Gerencia de Seguridad de la Información debe verificar que la Gerencia de Tecnologías de la Información instale únicamente software autorizado y con las respectivas licencias en el caso de utilizar software privativo.
p) La Gerencia de Tecnologías de la Información debe cumplir con los términos y condiciones de uso para el software y la información obtenida del Internet o proveedores (programas freeware, shareware, demostraciones o programas para pruebas.

q) La Gerencia de Tecnologías de la Información debe implementar los mecanismos necesarios con la finalidad de que intencionalmente en las estaciones de trabajo de los usuarios no se pueda escribir, generar, compilar, copiar, coleccionar, propagar, introducir y ejecutar cualquier tipo de código (programa) conocidos como virus, malware, spyware, o similares, diseñado para auto replicarse, dañar, afectar el desempeño, acceso a las computadoras, redes e información de la Institución.
r) Es responsabilidad de los usuarios no duplicar, convertir a otro formato o extraer contenidos de grabaciones (audio, vídeo), si no está expresamente permitido por su autor o la persona que tenga los derechos sobre el material; para tal efecto la Gerencia de Tecnologías de la Información debe garantizar que los equipos de los usuarios cuenten solo con el software autorizado por la institución.
s) Está prohibido por las leyes de derechos de autor, realizar en la CFN B.P. copias no autorizadas de software, ya sea adquirido o desarrollado por la Institución. Se exceptúa los programas de software libre bajo los términos de sus licencias públicas.
t) La Gerencia de Tecnologías de la Información está a cargo de definir y gestionar la aplicación de una licencia pública general al software desarrollado por la institución o contratado a terceros como desarrollo, para proteger la propiedad intelectual.
u) La Gerencia de Seguridad de la Información debe exigir que los funcionarios de la Institución utilicen solo software desarrollado, provisto o aprobado por la CFN B.P.

**Artículo 39.- Protección de Registros Organizacionales**

v) Es responsabilidad de la Gerencia de Tecnologías de la Información contar con una clasificación de los registros electrónicos y físicos por tipos, especificando los periodos de retención y los medios de almacenamiento, como discos, cintas, entre otros.
w) La Gerencia de Tecnologías de la Información debe mantener la documentación y especificaciones técnicas de los algoritmos y programas utilizados para el cifrado y descifrado de archivos y toda la información relevante relacionada con claves, archivos criptográficos o firmas electrónicas, para permitir el descifrado de los registros durante el periodo de tiempo para el cual se retienen.
x) La Gerencia de Tecnologías de la Información debe establecer un procedimiento para revisar el nivel de deterioro de los medios utilizados para almacenar los registros. Los procedimientos de almacenamiento y manipulación se deben implementar según las recomendaciones del fabricante. Para almacenamiento a largo plazo, se recomienda considerar el uso de cintas y discos digitales utilizando formatos de archivos y datos abiertos.
y) Los propietarios de la Información en coordinación con la Gerencia de Tecnologías de la Información y la Gerencia de Seguridad de la Información, deben establecer un procedimiento para garantizar el acceso a los datos e información registrada, tanto el medio como el formato, durante todo el periodo de retención, aplíquese el cumplimiento de este procedimiento para las Unidades Administrativas que requieran de dicho acceso.
z) La Gerencia de Tecnologías de la Información debe establecer un procedimiento para cambiar o actualizar la tecnología del medio en el cuál se almacenan los activos de información y registros de acuerdo a las innovaciones tecnológicas disponibles en el mercado.
aa) Los sistemas de almacenamiento de datos se deben seleccionar de manera que los datos requeridos se puedan recuperar en el periodo de tiempo y en formatos legibles, dependiendo de los requisitos que se deben cumplir, para tal efecto la Gerencia de Tecnologías de la Información debe implementar los mecanismos necesarios.
bb) La Gerencia de Tecnologías de la Información debe garantizar la identificación de los registros y el periodo de retención de los mismos tal como se defina en normas legales ecuatorianas. Este sistema debe permitir la destrucción adecuada de los registros después de este periodo, si la CFN B.P. no los necesita y las normas así lo especifican.

cc) Los propietarios de la Información, de manera conjunta con la Gerencia de Tecnologías de la Información y la Gerencia de Seguridad de la Información deben establecer y difundir en la Corporación Financiera Nacional B.P. las directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información, de manera que se encuentre disponible para el personal de la Institución, así mismo la CFN B.P. debe contar con un inventario de las fuentes de información clave.
dd) Las diferentes Unidades Administrativas de la Institución deben implementar controles apropiados para proteger registros contra pérdida, destrucción y falsificación de la información.

**Artículo 40.- Protección de los datos y privacidad de la información personal**

ee) La Gerencia de Seguridad de la Información debe controlar la aplicación de la política de protección de datos y privacidad de la información personal.
ff) Los propietarios de la Información, de manera conjunta con la Gerencia de Seguridad de la Información deben implementar medidas técnicas y organizacionales apropiadas para gestionar de manera responsable la información personal de acuerdo con la legislación correspondiente.
gg) Los propietarios de la Información, de manera conjunta con la Gerencia de Seguridad de la Información deben implementar mecanismos de carácter organizacional y tecnológico para autorización al acceso, uso e intercambio de datos personales de las personas o ciudadanos en custodia de las entidades públicas. Prima el principio que los datos personales pertenecen a las personas y no a las Instituciones, éstas los custodian al amparar la normativa legal Vigente.
hh) Ningún funcionario de la CFN B.P. debe probar o intentar probar fallas de Seguridad de la información, identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por la Gerencia de Seguridad de la Información.

**Artículo 41.- Prevención del uso inadecuado de servicios de procesamiento de información**

ii) La Gerencia de Tecnologías de la Información debe mantener un Inventario aprobado por parte de la Gerencia General o a su vez por quién ésta delegue, sobre el uso de los servicios de procesamiento de información.
jj) La Gerencia de Tecnologías de la Información debe definir y comunicar a la Gerencia de Seguridad de la Información, los servicios de procesamiento de información aprobados, así como los criterios para establecer el uso de estos servicios para propósitos no relacionados con la Institución sin autorización de la máxima autoridad, su delegado, o para cualquier propósito no autorizado.
kk) La Gerencia de Tecnologías de la Información en coordinación con la Gerencia de Seguridad de la Información debe implementar los mecanismos necesarios para identificar el uso inadecuado de los servicios por medio de monitoreo u otros medios.
ll) Es responsabilidad de la Gerencia Administrativa en coordinación con la Gerencia de Talento Humano definir y especificar en las en las normas internas de la entidad, las acciones legales o disciplinarias cuando se compruebe el uso no adecuado de los servicios de procesamiento de información. Se considera también lo que establece la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos y su reglamento.
mm) Los funcionarios que deseen hacer uso de los servicios de procesamiento de información aprobados, deben llenar el respectivo formulario de usuarios y accesos. Este formulario debe contar con el visto bueno del superior jerárquico, la Gerencia de Talento Humano debe certificar el cargo y el propietario de la información, de manera conjunta con la Gerencia de Seguridad de la Información lo deben autorizar.
nn) Es responsabilidad de la Gerencia de Tecnologías de la Información implementar en todos los servicios de procesamiento de información, el mensaje de advertencia que indique que el servicio al cual se está ingresando es propiedad de la CFN B.P. y que no permite el acceso no autorizado. El usuario debe reconocer y

reaccionar apropiadamente al mensaje de la pantalla para continuar con el proceso de registro de inicio. El uso de los servicios de procesamiento de la información de la entidad tienen como fin principal o exclusivo los asuntos de la institución y no los personales o de otra índole.

oo) La Gerencia de Tecnologías de la Información en coordinación con la Gerencia de Seguridad de la Información debe implementar mecanismos tecnológicos y organizacionales para detectar la intrusión y evitar el uso inadecuado de los servicios de procesamiento de información. Se recomienda advertir o informar a los usuarios sobre el monitoreo y obtener su acuerdo cuando los servicios de información están abiertos a la ciudadanía o son públicos.

**Artículo 42.- Reglamentación de Controles Criptográficos**

pp) La Gerencia de Tecnologías de la Información en coordinación con la Gerencia de Seguridad de la Información deben aplicar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes, para tal efecto debe considerar lo siguiente:

i. Restringir importaciones y/o exportaciones de hardware y software de computadores para la ejecución de funciones criptográficas; o diseñados para adicionarles funciones criptográficas.
ii. Restringir el uso de encriptación, especificar y documentar los ámbitos en dónde se aplican tales procesos (comunicación, firma de documentos, transmisión de datos, entre otros)
iii. Restringir métodos obligatorios o discrecionales de acceso por parte de las autoridades del país a la información encriptada mediante hardware o software para brindar confidencialidad al contenido.
iv. Garantizar el cumplimiento con las leyes y los reglamentos nacionales antes de desplazar información encriptada o controles criptográficos a otros países.

**Artículo 43.- Cumplimiento con las políticas y las normas de seguridad**

qq) La Gerencia de Seguridad de la Información debe revisar en intervalos regulares reportes e informes de seguridad de los sistemas de información.

rr) Es responsabilidad del Departamento de Auditoría Interna auditar las plataformas técnicas y los sistemas de información para determinar el cumplimiento de las normas aplicables sobre implementación de la seguridad y sus controles.

ss) La Gerencia de Seguridad de la Información debe realizar con regularidad monitoreo y revisión tanto físicas como remotas para asegurar el cumplimiento de las Políticas y Normas de la Institución con respecto a la Seguridad de la Información y se apoya en la Gerencia de Tecnologías de la Información para gestionar el cumplimiento de las mismas. Si se determina algún incumplimiento o no conformidad como resultado de la revisión, la dirección debe:

i. Determinar la causa del incumplimiento.
ii. Evaluar la necesidad de acciones para garantizar que no se repitan estos incumplimientos.
iii. Determinar e implementar la acción correctiva apropiada.
iv. Revisar la acción correctiva que se ejecutó.

tt) Es responsabilidad de los directivos de la Institución mantener el registro y conservación de los resultados de las revisiones y las acciones correctivas en el cumplimiento de una recomendación efectuada, sea ésta de índole interna o externa, así como el informar de los resultados a las personas que realizan estas revisiones cuando la revisión tiene lugar a la Unidad Administrativa de su responsabilidad.

**Artículo 44.- Verificación del cumplimiento técnico**

uu) Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad, para tal efecto se deben realizar las siguientes actividades:

i. La Gerencia de Tecnologías de la Información debe verificar el cumplimiento técnico bien sea manualmente (con soporte de las herramientas de software apropiadas, si es necesario) por un Ingeniero de Sistemas con experiencia, y/o con la ayuda de las herramientas automáticas que generen un informe técnico para la interpretación posterior por parte del especialista técnico.
ii. La Gerencia de Seguridad de la Información debe aplicar evaluaciones de vulnerabilidad o pruebas de penetración en coordinación con la Gerencia de Tecnologías de la Información, considerando siempre el riesgo de que dichas actividades pueden poner en peligro la seguridad del sistema. Tales pruebas se deben planificar, documentar y ser repetibles.
iii. La Gerencia de Tecnologías de la Información debe controlar que la verificación del cumplimiento técnico sea realizado por personas autorizadas y competentes o bajo la supervisión de dichas personas.
iv. La Gerencia de Tecnologías de la Información debe analizar los sistemas operativos para asegurar que los controles de hardware y software se han implementado correctamente. Este tipo de verificación del cumplimiento requiere experiencia técnica especializada.
v. La Gerencia de Seguridad de la Información en coordinación con la Gerencia de Tecnologías de la Información debe ejecutar o contratar pruebas de penetración y evaluaciones de la vulnerabilidad, las cuales deben ser efectuadas por personal independiente a la CFN B.P., de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional. Ello puede ser útil para detectar vulnerabilidades en el sistema y verificar que tan efectivos son los controles evitando el acceso no autorizado debido a estas vulnerabilidades. Las pruebas de penetración y las evaluaciones de vulnerabilidad no deben sustituir las evaluaciones de riesgos.

**Artículo 45.- Controles de auditoría de los sistemas de información**

vv) El área de Auditoría Interna debe planear los requerimientos y actividades de las auditorías que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos del negocio, para tal efecto debe considerar lo siguiente:

i. Salvaguardar los servicios de procesamiento de información y las herramientas de auditoría de los sistemas de información.
ii. Acordar los requisitos así como el alcance de las auditorías con la dirección correspondiente.
iii. Únicamente se debe dar a los auditores acceso de lectura a la información.
iv. Solo el personal de la Gerencia de Tecnologías de la Información y la Gerencia de Seguridad de la Información están autorizados a realizar controles en los diferentes elementos de Tecnología de la Información.
v. Identificar y acordar los requisitos para el procesamiento especial o adicional.
vi. Monitorear y registrar todo acceso para crear un rastreo para referencia. El uso de rastreos de referencia de tiempo se debe considerar para datos o sistemas críticos.
vii. Documentar todos los procedimientos, requisitos y responsabilidades de la auditoría.
viii. Asegurar que la persona que realiza la auditoría sea independiente de las actividades auditadas.

**Artículo 46.- Protección de las herramientas de auditoría de los sistemas de información**

ww) La Gerencia de Tecnologías de la Información debe garantizar la protección del acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible, para tal efecto se debe considerar lo siguiente:

i. Instalar y administrar las herramientas de auditoría por parte del personal que las utiliza.
ii. Los programas de software o archivos de datos de auditoría se deben separar de los sistemas de información y desarrollo de la entidad.

iii. Los archivos de seguridad y auditoría que generan los sistemas de procesamiento de información deben ser protegidos contra cualquier manipulación.
iv. Mantener un estricto control de respaldos y tiempo de retención de los archivos de seguridad y auditoría de acuerdo al tipo de información y la política que se defina.
v. Mantener archivos de seguridad y auditoría en librerías de cinta, siempre que se les proporcione un nivel adecuado de protección adicional.
vi. Bloquear el acceso a los archivos de seguridad y auditoría a los funcionarios no autorizados y de acuerdo al procedimiento que se defina.

## CAPÍTULO X: DEL ACUERDO DE PRIVACIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

**Artículo 47.- Generalidades:**

a) La Corporación Financiera Nacional, Banca Pública (CFN B.P.) con domicilio principal en Guayaquil, Ecuador, reconoce la importancia de la seguridad, privacidad y confidencialidad de los datos personales de sus clientes, usuarios, colaboradores, proveedores, accionistas, aliados y en general de todos sus grupos de interés respecto de los cuales ejerce el tratamiento de la información personal, por lo que en cumplimiento de las disposiciones constitucionales y legales, acepta el presente ACUERDO DE PRIVACIDAD DE LA INFORMACIÓN Y PROTECCION DE DATOS PERSONALES.

b) La información contenida en este acuerdo será divulgada a través de los distintos medios y canales, para conocimiento de los clientes, sus relacionados y del público en general. Así mismo, las modificaciones y actualizaciones de este acuerdo serán divulgadas a través de los distintos medios y canales, para conocimiento del cliente, sus relacionados y del público en general. En la medida en que así lo haya aceptado el cliente a través de los formatos y contratos, el contenido de este Acuerdo y sus modificaciones, cuando sean divulgadas, es vinculante y prevalecerá sobre los documentos y contratos suscritos por el cliente, en lo que respecta al tratamiento y la privacidad de sus datos personales, salvo que tales documentos o contratos, establezcan de forma expresa, que su contenido en esta materia prevalece sobre este acuerdo de privacidad.

c) Por favor lea el Acuerdo de privacidad de la CFN B.P., donde podrá conocer cómo serán utilizados y protegidos sus datos personales. Cuando ingrese información personal o sensible en la página web de la CFN B.P., usted estará aceptando automáticamente las reglas de manejo, protección y seguridad que la CFN B.P. establece y que se indican a continuación:

**Artículo 48.- Alcance del Acuerdo de Privacidad de la Información y de Protección de Datos Personales:**

d) De Cliente y Relacionados
i. Para efectos de este Acuerdo, El término “cliente” también incluye a aquellos individuos cuya relación comercial ha terminado, pero cuya información o datos personales se conserven, según lo previsto en el presente Acuerdo.
ii. Por su parte, el término “relacionados”, incluye a las siguientes personas naturales vinculadas a los clientes, sean los clientes personas naturales o jurídicas: cotitulares, accionistas y socios, beneficiarios finales y controladores, directores, dignatarios, ejecutivos, firmantes autorizados y representantes, garantes, protectores, fideicomitentes, fiduciarios, o cualquier otra persona natural relacionada al cliente, cuya información sea requerida por ser relevante para la prestación de los productos y servicios con la institución.

iii. Quedan excluidos del alcance de este Acuerdo, los datos disociados o anonimizados, de forma que no se relacionen con una persona identificable. También quedan excluidos del alcance de este Acuerdo, el tratamiento de datos personales relacionados con proveedores, empleados, directores, dignatarios o accionistas.

e) Responsabilidad del Cliente y de la CFN BP.
   i. El presente Acuerdo de privacidad debe ser leída detenidamente por El Cliente cada vez que accede al sitio web de la CFN B.P., así podrá estar seguro del manejo que la CFN B.P. realiza con sus datos.
   ii. El CFN B.P., está en conocimiento de la responsabilidad de proteger la confidencialidad y privacidad de la información personal y financiera de sus clientes.

f) Quiénes tendrán acceso a su información
   i. CFN B.P. únicamente permitirá el acceso a la información de sus clientes, a personas debidamente autorizadas, o a terceros de confianza, que operen bajo una relación contractual, en la que previamente se hayan comprometido con las condiciones de seguridad y privacidad de la CFN B.P., y en la que hayan acordado operar conforme a las políticas de la institución. Todos los permisos otorgados a un tercero, a los sistemas tecnológicos de CFN B.P., estarán restringidos al propósito de negocio entre la CFN B.P. y la tercera entidad.
   ii. La información de identificación personal que recopilamos, como nombres, correo electrónico, cuenta de redes sociales, números de teléfono, etc., se utilizan con objetivos de difusión de nuestras actividades y productos, así como para mantener y cumplir las obligaciones contractuales, legales y de transparencia que exijan algún tipo de comunicación.
   iii. Podemos divulgar información de identificación personal u otra información recopilada a través del sitio web en respuesta a un proceso legal o cuando creamos que una norma aplicable lo exige, por ejemplo, en respuesta a una orden judicial, citación o solicitud de una agencia de aplicación de una norma aplicable.

**Artículo 49.- Propósitos de la Obtención de Datos Personales:**

g) A continuación, se detallan las finalidades o propósitos para los cuales se obtienen y procesan datos personales de clientes y sus relacionados.
h) El cliente conoce y aprueba, estos propósitos o finalidades mediante la aceptación de este Acuerdo, y de los contratos y formatos en materia de protección de datos personales. Finalidades o Propósitos basados en (i) el cumplimiento contractual, (ii) cumplimiento de normas y requerimientos legales; (iii) la autorización legal o (iv) la satisfacción de intereses legítimos, tales como, el reconocimiento o defensa de derechos dentro de procesos legales, para finalidades que hagan parte de expectativas razonables dada la relación con el cliente, para la prevención del fraude y gestión de ciberseguridad, para la debida diligencia, y la evaluación de riesgo, entre otros:
   i. Para contactarlo, para cualquiera de las finalidades descritas a continuación, por cualquier medio suministrado.
   ii. Para validar su identidad, en las interacciones con el cliente, incluyendo para la ejecución, verificación y autorización de sus solicitudes y operaciones.
   iii. Para ejecutar obligaciones derivadas de un contrato suscrito por el cliente en la prestación de los productos y servicios, incluyendo la entrega del servicio, la gestión del cobro de obligaciones, el procesamiento de pagos.
   iv. Para realizar las gestiones tendientes a establecer una relación contractual que nos haya solicitado.
   v. Para administrar sus productos o servicios, así como entregarle información acerca de los productos o servicios que mantiene.

vi. Para compartirle información acerca de productos y servicios que se ofrecen, y que pudiesen ser de su interés.
vii. Para notificarle cambios relacionados con los productos y/o servicios que mantiene.
viii. Para brindarle soporte en la atención de sus solicitudes, reclamos y requerimientos.
ix. Para confirmar y actualizar su información.
x. Para gestionar los riesgos a los cuales la CFN B.P. está expuesta en el desarrollo de sus negocios.
xi. Para fines relacionados con la prevención del uso indebido de los productos y servicios, incluyendo la prevención del fraude, el blanqueo de capitales, el financiamiento del terrorismo y la proliferación de armas de destrucción masiva.
xii. Para cumplir con las obligaciones legales, en materia prudencial, de intercambio de información para fines fiscales o tributarios, entre otras.
xiii. Para obtener, a través de terceros, incluyendo entidades del grupo, servicios, recursos y capacidades; incluyendo capacidades tecnológicas, uso de redes, de alojamiento, almacenamiento, procesamiento y analítica de datos, así como servicios financieros, de asesoría, auditoría, calificación de riesgos, administrativos, operativos y contables, entre otros; que permiten o facilitan el ofrecimiento de los servicios a su favor.
xiv. Para fines estadísticos, luego de un proceso de disociación o anonimización.
xv. Para la definición, estructuración y ejecución de transacciones estratégicas para la operación, modelo de negocio y oferta de servicios, lo cual podrá implicar la transmisión o transferencia de los datos a entidades aliadas o terceros.
xvi. Para cualquier otra finalidad requerida para el desarrollo del objeto social de la corporación y para fines compatibles con los propósitos anteriores, incluyendo el uso de distintos medios y canales, de acuerdo con los avances tecnológicos finalidades o propósitos basados en el consentimiento. El cliente otorga su consentimiento para el procesamiento de sus datos con estos propósitos o finalidades, mediante la aceptación de este Acuerdo, y los contratos y formatos en materia de protección de datos personales de la corporación.
xvii. Para el desarrollo de actividades de oferta comercial, publicidad, promoción o mercadeo de productos y servicios, a través de distintos medios de comunicación y redes sociales;
xviii. Para el desarrollo y optimización de productos, servicios y canales;
xix. Para obtener, consultar, reportar, rectificar, modificar y eliminar el historial o antecedentes de créditos, ante centrales de riesgo o agencias de información.
xx. Para obtener análisis o evaluación de crédito, investigaciones económicas y comerciales, estadísticas, reputacionales y de mercado.
xxi. Para obtener y conocer el estado de sus operaciones, así como su comportamiento financiero, comercial, reputacional, el cumplimiento de sus obligaciones, la imposición de multas y sanciones, en otras entidades, tanto de las empresas aliadas como no vinculadas, incluyendo operadores de información o proveedores de bases de datos.
xxii. Para obtener, registrar y en general procesar sus datos, para optimizar su experiencia y conocer sus preferencias, monitorear su información, y para presentar contenidos y publicidad relacionados con sus preferencias cuando navegan por los sitios web, plataformas y/o aplicativos tecnológicos y/o digitales de los bancos, incluyendo el uso de cookies propias y de terceros.
xxiii. Para compartirla con aliados estratégicos, para que estos puedan ofrecerle beneficios y servicios asociados a los productos y servicios de la corporación.
xxiv. Para medir, reportar y gestionar el desempeño comercial y administrativo, cumplir con regulaciones que le sean aplicables, gestionar riesgos.
xxv. Para la toma de decisiones relevantes para el cliente, relacionadas con la prestación de los productos y servicios, basadas exclusivamente en el procesamiento automatizado de datos personales.
xxvi. Para realizar encuestas de satisfacción concerniente a los servicios prestados por la CFN B.P.

xxvii. Para compartir información con terceros, tales como, asesores, consultores, contrapartes, aliados, proveedores y corresponsales, cuando lo requieran en el contexto de la ejecución de una transacción o la prestación de servicios financieros, de asesoría o corresponsalía a nuestro favor.

xxviii. Para compartir información con autoridades extranjeras, cuando sea requerida en el contexto de investigaciones y acciones relacionadas con la prevención del blanqueo de capitales, financiamiento del terrorismo, y cualquier otra actividad ilícita, basado en una norma extranjera con aplicación extraterritorial.

xxix. Para la obtención y procesamiento de datos sensibles, para todas las finalidades enunciadas.

xxx. Para compartir información con terceros, a solicitud del propio cliente o su representante autorizado.

xxxi. Para comunicar sobre las políticas de gestión Antisoborno, implementadas por la Corporación Financiera Nacional B.P.

xxxii. Para fines compatibles con los anteriores.

**Artículo 50.- Consideraciones de Seguridad:**

i) Integridad de la Información

i. La información del cliente y sus relacionados, debe ser veraz y actualizada. En consecuencia, se requiere que el cliente entregue información veraz y verificable, así como la actualización de la información del cliente y sus relacionados, cuando se produzcan cambios relevantes, o cuando la CFN B.P., así lo requiera. Por regla general, se mantiene registros de información de los clientes y de sus operaciones por un plazo de al menos cinco (5) años, contados a partir de la terminación de la relación comercial. No obstante, se puede conservar su información y de sus relacionados por plazos superiores a este, en cumplimiento de reglas específicas o políticas internas.

ii. Es responsabilidad del cliente, garantizar la exactitud, veracidad e integridad de la información de tipo personal y financiera que le proporcione a la CFN B.P.

j) Protegemos su Información

i. Para la CFN B.P., la seguridad de su información es una prioridad en la operativa diaria. Ponemos énfasis en la selección de las soluciones tecnologías que se invierten para que estas sean de excelente nivel en la protección de la información de nuestros clientes. Tenemos controles implementados para proteger su información personal en los productos y servicios que entregamos. Sin embargo, es una realidad que el cliente debe considerar, que a pesar de las características técnicas y seguras de transmisión de información a través del Internet, ningún sistema es infalible y totalmente seguro o está exento de sufrir ataques de terceros.

ii. Los clientes pueden estar seguros de que la CFN B.P. no entrega, vende o alquila bajo ningún concepto, la información personal de sus clientes. Para la protección de su información confidencial, CFN B.P., mantiene políticas internas en materia de seguridad de la información, diseñadas para asegurar la confidencialidad, integridad y disponibilidad.

k) Reportes y Denuncias

i. La CFN B.P., mantiene en completa reserva las denuncias que hagan las personas, de buena fe o sobre la base de una creencia razonable, el intento de soborno, supuesto o real, o cualquier violación o debilidad en el sistema de gestión antisoborno, a la función de cumplimiento antisoborno o al personal apropiado (ya sea directamente o a través de una tercera parte apropiada). salvo en la medida requerida para el avance de una investigación, la CFN B.P., trata los informes de estas denuncias de forma confidencial con el fin

de proteger la identidad del informante y otras personas que participen o a las que se haga referencia en el informe.

ii. Si usted conoce sobre alguna irregularidad o posible caso de corrupción, por favor escríbanos a denuncias_sobornos@cfn.fin.ec, o en la página web https://www.cfn.fin.ec/ en el enlace del Sistema de Gestión Antisoborno.

l) Acceso al sitio Web

El acceso a nuestro sitio web que se realice mediante nombre de usuario y una contraseña proporcionada por la Corporación, así como con otros factores de autenticación. Es responsabilidad del Cliente proteger la confidencialidad de su contraseña y de los otros factores de autenticación que la CFN B.P., le haya proporcionado. De igual manera el cliente asume la responsabilidad por todas las actividades que se realicen bajo su usuario y contraseña durante el tiempo que dure la relación con el CFN B.P. Por tal razón el cliente se compromete a: Notificar de inmediato a la CFN B.P. a través del call center 042591-800 sobre el robo o uso no autorizado de su usuario y contraseña. En caso de no cumplir con la notificación, se deslinda a la CFN B.P. de toda responsabilidad por la pérdida o daño sufrido por el uso inapropiado del usuario y contraseña.

m) Concienciación del personal sobre la privacidad de la información

CFN B.P. cuenta con campañas de concienciación y formación sobre seguridad y privacidad, para garantizar que los empleados comprendan la importancia de proteger los datos personales, al igual que acuerdos de privacidad y estándares que regulan la forma en que el CFN B.P. gestiona los datos de nuestros Clientes.

**Artículo 51.- Información Adicional:**

n) CFN B.P. publica en su sitio web, las versiones de los navegadores con los que se puede acceder al sitio. Versiones inferiores a las sugeridas no darán un servicio seguro ni de calidad. Es responsabilidad del cliente mantenerse informado sobre este tema y actualizar las versiones de sus navegadores.

## CAPÍTULO XI: DE LA ADMINISTRACIÓN DE CONTRASEÑAS

**Artículo 52.- GENERALIDADES DE LA ADMINISTRACIÓN DE CONTRASEÑAS:**

La presente política define las directrices necesarias para asegurar la responsabilidad, uso y custodia de las claves de acceso por parte del usuario; establecer los requerimientos mínimos para la construcción de claves; asegurar la utilidad de las mismas como resguardo de los accesos a los distintos sistemas informáticos existentes en CFN B.P.

Debe ser observada y cumplida por todos los funcionarios y colaboradores sean estos empleados directos, externalizados o servicios profesionales, y por entidades externas como proveedores o entidades de control los cuales tengan el acceso a la información y los recursos informáticos que maneja CFN B.P. para el desarrollo de sus actividades.

Es responsabilidad de la Gerencia de Tecnologías de la Información la implementación de las políticas institucionales de Seguridad de la Información, en lo que se refiere a la Administración de Contraseñas, en los sistemas informáticos y servicios tecnológicos institucionales.

Todos los usuarios de la Institución (incluyendo a funcionarios, personal externo o proveedores), deben dar cumplimiento al Política General relacionada con la Administración de Contraseñas

**Artículo 53.-** NORMAS

Las siguientes son las normas de control interno que deben cumplirse.

**1. Uso adecuado de Contraseñas (claves, passwords)**

a) Las contraseñas son de uso personal e intransferible en todo momento; manejadas por el usuario como información confidencial, el compartir o divulgar las contraseñas se considera una falta grave sancionable.

b) Todo usuario que se encuentre en las instalaciones de la Institución, al encender o reiniciar su computador debe ingresar a la red con su cuenta de usuario y contraseña asignadas, no en modo estación de trabajo.

c) Las contraseñas no deben ser escritas o registradas en lugares accesibles como documentos, monitores, escritorios, pared, teclados, agendas, etc., donde puedan ser observadas por otras personas. El no cumplir con esta política se considera falta grave sancionable.

**2. Características de las Contraseñas**

d) Las nuevas contraseñas no puedan ser iguales que por lo menos las 5 últimas contraseñas usadas. Habilitar el control de historial de contraseñas siempre y cuando la herramienta o el sistema lo permita (se recomienda que esta característica sea parametrizable).

e) Las contraseñas no deben ser visibles en la pantalla al momento de digitarlas.

f) En caso que la contraseña no cumpla con los requisitos o controles indicados, o que el usuario este utilizando una contraseña trivial, el aplicativo debe solicitar al usuario el ingreso de otra clave.

g) Todos los usuarios de los recursos informáticos deben utilizar una contraseña fuerte que no pueda ser fácilmente deducida o adivinada por otros, se recomienda:

- Contraseñas no relacionadas al trabajo o a la vida personal del usuario. No deben utilizarse nombres de los cónyuges, hijos, parejas, amigos, mascotas, direcciones, familiares, ciudad, fecha de nacimiento, número de cédula, números de cuentas bancarias, etc.
- La contraseña debe tener mínimo 8 caracteres. Las contraseñas deben estar compuestas por la combinación de palabras, dígitos, letras y caracteres especiales, que contengan mayúsculas, minúsculas, (siempre y cuando la herramienta o el sistema lo permita), diferentes del código de usuario.
- Transformar una palabra con algún método específico, como por ejemplo reemplazando las letras por un número (por ejemplo Inf0rm8tic8).
- No seguir una secuencia de teclado.
- No usar una palabra o combinación de palabras comunes, sean estas del idioma español o de otros idiomas.
- Se considera conveniente no hacer uso de claves con una palabra fija y la otra dependiendo del mes o fecha en curso, porque las mismas son fácilmente deducibles. Por ejemplo JUANENERO, JUAN01262010 o JUAN01*, etc.

**3. Contraseñas y sistemas descuidados**

h) Todos los usuarios deben dejar protegida su computadora con protección de pantalla cada vez que se retiren de su puesto de trabajo o se alejen del computador, a fin de evitar el uso de la contraseña por otra persona (sistema descuidado). A su retorno, el usuario debe proceder con el desbloqueo correspondiente digitando la contraseña respectiva.

i) Los sistemas deben contemplar la opción de cerrado de sesión por inactividad de acuerdo al parámetro definido por la Gerencia de Seguridad de la Información.

**4. Responsabilidad sobre las contraseñas**

j) Todos los usuarios deben asumir que sus contraseñas son individuales y no deben divulgarlo bajo ninguna circunstancia, cada usuario está obligado a mantener la confidencialidad y reserva de su contraseña y a cambiarla periódicamente. Toda actividad realizada con dicha contraseña es de responsabilidad del usuario custodio de la contraseña. Si un usuario comparte su contraseña es considerada falta grave sancionable.

k) La responsabilidad sobre los datos ingresados a un sistema es exclusiva de los usuarios habilitados (que efectúan sus accesos ingresando sus respectivas contraseñas), comprobándose la autoría de estos accesos a través de la información registrada por el sistema.

l) No se debe autorizar el uso de usuarios y contraseñas compartidas o de carácter grupal, ya que favorecen el carácter "anónimo" de los accesos, dificultando el establecimiento de responsabilidades y las auditorías; aunque varias personas realicen las mismas tareas en un sistema, cada persona debe contar con su usuario oficial individual, aunque estos usuarios tengan idénticas características; a excepción de las cuentas de usuarios especiales de carácter grupal, que sean autorizados por la Gerencia de Seguridad de la Información, sin embargo en estos casos, el superior jerárquico debe asignar un responsable del uso de esos usuarios a quien se le reporta cualquier eventualidad.

**5. Cambio de las contraseñas**

m) La contraseña inicial debe ser cambiada inmediatamente por una contraseña personalizada por el usuario. Se debe exigir el cambio de contraseñas por una nueva en el primer acceso después de otorgado el usuario.

n) Las contraseñas deben ser renovadas cada vez que lo exija el sistema y cada vez que se tengan dudas sobre la pérdida de la confidencialidad de la misma.

o) Es responsabilidad del usuario cambiar su contraseña, o solicitar la asignación de una nueva clave, si considera que su contraseña ha perdido confidencialidad.

p) Caducidad o cambio de la contraseña hasta 60 días (se sugiere que exista una parametrización).

q) Los sistemas deben obligar al usuario a cambiar la contraseña si esta es reseteada por el administrador de los diferentes componentes tecnológicos.

r) Al momento de cambiar la contraseña, los sistemas deben permitir al usuario primero ingresar la contraseña actual y luego la nueva, esta última debe reescribirla para confirmarla.

s) Demandar que el tiempo ocioso para desactivar el sistema / sesión sea parametrizable (y el parámetro inicial se establece en 30 minutos).

t) Todas las contraseñas predeterminadas por el proveedor o fabricante de los sistemas operativos, equipos de comunicaciones, cadenas de conexiones, bases de datos, aplicaciones y sistemas, y demás recursos informáticos, deben ser cambiadas antes de ser instaladas en los ambientes de la CFN B.P.

u) Todos los sistemas deben contar con un sistema de expiración automática de contraseñas. Para el caso de las cuentas especiales, el solicitante debe especificar la expiración de la cuenta y/o contraseña para que sea autorizado por la Gerencia de Seguridad de la Información, Unidad Administrativa encargada de generar la clave y hacerle la entrega al responsable de dicha cuenta de manera confidencial, para que se proceda con el cambio respectivo; además es responsabilidad del responsable de la cuenta especial, cambiar la clave por lo menos con una periodicidad anual e informar a la Gerencia de Seguridad de la Información que se cumplió con esta actividad.

**6. Bloqueo de las cuentas y usuarios por uso de las contraseñas**

v) La cuenta de usuario debe ser bloqueada de inmediato, si se conoce o sospecha que la contraseña de dicho usuario ha sido comprometida/puesta en peligro.

w) El reseteo de claves /desbloqueo de cuenta se lo realiza previa solicitud y confirmación de datos con el usuario; esta certificación se la realiza telefónicamente o por email. Las claves temporales que entrega la Gerencia de Seguridad de la Información las debe realizar por correo electrónico, con lo que se asegura que se trata del usuario solicitante. Para la confirmación de información se toma en cuenta aspectos tales como:

- Nombre del usuario.
- Equipo al que accede.
- Motivo de solicitud de restauración de clave, desbloqueo de cuenta.
- Visualización de la extensión que realiza la llamada o la dirección de correo email.

x) Se deben bloquear automáticamente las cuentas / usuarios después de n tentativas de registro inválidas (el parámetro inicia con el valor de 3 pero podría ser modificado por la Gerencia de Seguridad de la Información). El usuario dispone de tres oportunidades para ingresar correctamente la contraseña.
y) Las cuentas de usuarios pueden ser desbloqueadas usando mecanismos de reactivación de contraseñas automatizadas. Se deben usar preguntas de prueba con respuestas que únicamente el usuario individual pueda conocer. Estas preguntas deben ser diseñadas de tal forma que las respuestas no sean información que esté disponible en otras partes de la organización.

**7. Protección técnica de las contraseñas**

z) Las contraseñas deben ser encriptadas, de manera que no puedan ser descifradas o identificadas por ningún medio durante la transmisión y almacenamiento en todos los componentes (por ejemplo en scripts y bases de datos, hilos de conexión, código compilado internamente, etc.).

- La clave de usuario no debe estar "plana" en las tablas de la base de datos, ni tampoco se debe aplicar un algoritmo de reemplazo lineal de caracteres (cambiar un carácter por otro).

aa) Uso de contraseña en las aplicaciones informáticas:

- Con el usuario del aplicativo no se debe poder conectar directamente a la base de datos (utilizando la misma contraseña del aplicativo).
- Debe solicitar cambio de contraseña en forma automática, cada n días parametrizables. El parámetro puede iniciar con 60 días pero puede ser modificado de acuerdo a lo que defina la Gerencia de Seguridad de la Información.
- La primera vez que el usuario ingrese al aplicativo, se debe forzar cambio de clave.
- Cuando el Administrador de Seguridades resetee la contraseña, el aplicativo debe forzar cambio de clave en el siguiente ingreso por parte del usuario (obligatorio).
- La contraseña reseteada desde el aplicativo debe generarse en forma aleatoria, de manera automática, sin intervención humana.
- La complejidad de la contraseña debe ser parametrizable, estableciendo la cantidad de letras mayúsculas, minúsculas, caracteres especiales (indicando los permitidos) y números.
- Posibilidad de excluir contraseñas (diccionario).
- La clave no debe repetirse en n veces parametrizable, es decir, que el sistema recuerde las últimas contraseñas y no permita reutilizarlas. El parámetro puede iniciar con 3 pero puede ser modificado de acuerdo a lo que defina la Gerencia de Seguridad de la Información.
- Debe permitir autogestionar el reseteo de su contraseña, opción "¿Olvidó su contraseña?"

**8. Soporte Tecnológico para asegurar el cumplimiento con las Políticas Institucionales de Seguridad de la Información**

bb) La Gerencia de Tecnologías de la Información debe mantener actualizados los antivirus y parches de seguridad establecidos en servidores y equipos de usuario final.
cc)La Gerencia de Tecnologías de la Información debe velar que los sistemas cumplan con la autenticación de los accesos a los componentes del sistema, de tal manera que permita llevar un control de cambios de claves periódicos de todos los usuarios de servicios, aplicaciones, bases de datos, equipos de comunicaciones, etc. El control debe ser realizado por la Gerencia de Seguridad de la Información.

**9. Monitoreo del cumplimiento con la Política**

dd) La Gerencia de Seguridad de la Información debe considerar el uso de una aplicación de escaneo o monitoreo que resalte los dispositivos con vulnerabilidades conocidas, la existencia de software o firmware obsoleto o la presencia en uso de contraseñas predeterminadas que deberían cambiarse.

ee) La Gerencia de Tecnologías de la Información es responsable de la implementación de las políticas de contraseñas y coordinar las pruebas de aceptación con la Gerencia de Seguridad de la Información previo a su puesta en producción. Además la Gerencia de Seguridad de la Información realiza el monitoreo correspondiente en ambiente productivo.

**10.Sitio Alterno**

ff) La Gerencia de Seguridad de la Información, debe mantener las claves de acceso necesarias para el funcionamiento de los equipos y servicios del sitio alterno, en sobre sellado y alojadas en caja fuerte.

gg) En caso de requerir la habilitación del Sitio Alterno, es responsabilidad de la Gerencia de Seguridad de la Información entregar el sobre con las claves de acceso de los equipos y servicios del sitio alterno, al Gestor del DRP, definido por la Gerencia de Tecnologías de la Información, para que proceda a ejecutar los procedimientos respectivos para habilitar el ambiente de contingencia.

hh) Es responsabilidad de la Gerencia de Seguridad de la Información mantener actualizada la información de accesos.

**11.Gestión de incidentes de seguridad de la información relacionados con contraseñas**

ii) Los funcionarios deben prestar particular atención a la protección de las contraseñas, los documentos e información que cuenten para ejercer sus funciones.

jj) Si el usuario identifica algún incidente de seguridad o evento de riesgo debe reportarlo inmediatamente a su jefe inmediato y/o a la Gerencia de Seguridad de la Información.

## CAPÍTULO XII: MONITOREO PERIÓDICO DE ACCESOS, OPERACIONES PRIVILEGIADAS E INTENTO DE ACCESOS NO AUTORIZADOS

**Artículo 54.- GENERALIDADES DEL MONITOREO PERIÓDICO DE ACCESOS, OPERACIONES PRIVILEGIADAS E INTENTO DE ACCESOS NO AUTORIZADOS:**

La presente política establece los lineamientos necesarios para garantizar el monitoreo periódico de los accesos, operaciones privilegiadas, e intentos de accesos no autorizados a los sistemas y servicios de la entidad, salvaguardando la confidencialidad, integridad y disponibilidad de la información de CFN B.P.

Esta política aplica para el monitoreo de los accesos, operaciones privilegiadas, e intentos de accesos no autorizados a los sistemas y servicios brindados por CFN B.P. y que:

i. Son accesos previamente gestionados por los responsables de las Unidades Administrativas de CFN B.P.
ii. Accesos autorizados para operaciones privilegiadas.
iii. Utilizados por terceros y/o personal facultado por la institución.
iv. Todo acceso no autorizado que se pueda descubrir a través del monitoreo.

Las políticas Institucionales de Seguridad de la Información deben ser concienciadas, observadas, comunicadas y aplica para todos los funcionarios y colaboradores, sean estos empleados directos, externalizados o servicios profesionales, y por entidades externas como proveedores o entidades de control los cuales tengan relación con los prestadores de servicios relacionados con los activos de información que maneja CFN B.P. para el desarrollo de sus actividades.

**Artículo 55.- NORMAS:**

Las siguientes son las normas de control interno que deben cumplirse en CFN B.P.

1. **Monitoreo de los accesos a los sistemas y/o recursos tecnológicos de CFN B.P.**

   a) La Gerencia de Seguridad de la Información debe realizar monitoreo periódico de los accesos a los sistemas y/o recursos tecnológicos, para asegurar que los usuarios solo estén realizando actividades para las cuales han sido autorizados.

   b) El monitoreo debe hacerse de manera permanente a las actividades ligadas con el control de accesos como es: la autenticación (quién soy), la autorización (qué puedo hacer) y el registro de auditoria (qué he hecho) con la finalidad de garantizar el uso adecuado de los permisos asignados a los usuarios.

   c) Se debe analizar y realizar una evaluación de los riesgos de seguridad de la información asociados a la gestión de control de accesos otorgados a los funcionarios, con el objeto de identificar brechas que puedan ser potenciales vulnerabilidades que exponga la continuidad de los procesos operativos o puedan dañar la imagen de la institución.

   d) En base a los resultados del monitoreo, se debe revisar periódicamente las restricciones, accesos privilegiados y otros accesos a los activos de información, tomando en cuenta las políticas de control de acceso aplicables.

   e) Se debe realizar el tratamiento y monitoreo de los usuarios creados en las bases de datos de las aplicaciones existentes en la Institución con la finalidad de mitigar los riesgos que puedan suscitarse por la falta de una desactivación oportuna de los usuarios creados en la base de datos.

2. **Monitoreo de las operaciones privilegiadas de CFN B.P.**

   f) La Gerencia de Seguridad de la Información debe realizar monitoreo periódico de operaciones privilegiadas, para asegurar que únicamente los usuarios autorizados estén realizando accesos privilegiados a los activos de información; de conformidad con las funciones y actividades del cargo que desempeñen.

   g) La Gerencia de Seguridad de la Información debe realizar monitoreo periódico de las operaciones privilegiadas para confirmar que ningún funcionario use perfiles y/o roles que tengan conflicto de intereses.

3. **Monitoreo de intentos de accesos no autorizados en CFN B.P.**

   h) La Gerencia de Seguridad de la Información debe realizar monitoreo periódico para detectar intentos de accesos no autorizados, para asegurar que únicamente los usuarios autorizados estén realizando actividades en los sistemas y/o recursos tecnológicos.

   i) La Gerencia de Seguridad de la Información debe realizar monitoreo periódico para detectar si se realizan las siguientes acciones prohibidas:

   - Compartir y/o divulgar usuarios y contraseñas otorgados.
   - Intentar cambiar cualquier tipo de configuración de la computadora.
   - Colocar información que no tenga que ver con el trabajo y/o respaldarla en cualquier medio de almacenamiento de CFN B.P.
   - Manipular, eliminar y/o destruir cualquier activo de información, sin la previa autorización del propietario de la información o el responsable del activo o sin seguir los protocolos indicados en la normativa vigente de los organismos de control aplicables para períodos de conservación y procedimientos de descarte de información.
   - Acceso a los recursos de información físico o digital sin autorización explícita.

**4. Monitoreo de los sistemas y/o recursos tecnológicos de CFN B.P.**

j) Los accesos a las pistas de auditoria, monitoreo y administración de los sistemas de información y aplicaciones de CFN B.P. son autorizados por los propietarios de la información y por la Gerencia de Seguridad de la Información a los usuarios de las unidades administrativas relacionadas con esta actividad a fin de evitar cualquier peligro o uso indebido. Los propietarios de la información deberán realizar depuraciones continuas de los roles asignados a los usuarios, para asegurar que nadie mantiene privilegios que no corresponden a su cargo o rol actual.

k) El/La Gerente de Seguridad de la Información debe monitorear con una frecuencia al menos semestral, el cumplimiento y la efectividad de los controles establecidos en la entidad y generar informes dirigidos al Comité de Gestión de Seguridad de la Información para su conocimiento y toma de acciones para evitar riesgos de seguridad.

l) El/La Gerente de Seguridad de la Información debe proporcionar al Comité de Gestión de Seguridad de la Información un Plan de Seguridad de la Información que apruebe la implementación de los controles identificados y acciones de mejora para esta política.

## CAPÍTULO XIII: RELACIÓN CON PROVEEDORES ASOCIADOS AL TRATAMIENTO DE INFORMACIÓN EN SITUACIONES DE CONTRATAR SERVICIOS DE TRATAMIENTO O RESGUARDO DE ACTIVOS DE INFORMACIÓN

**Artículo 56.- GENERALIDADES DE LA RELACIÓN CON PROVEEDORES ASOCIADOS AL TRATAMIENT DE INFORMACIÓN EN SITUACIONES DE CONTRATAR SERVICIOS DE TRATAMIENTO O RESGUARDO DE ACTIVOS DE INFORMACIÓN:**

Garantizar la protección de los activos de la información a los cuales los proveedores tienen acceso; así mismo garantizar que se mantenga un nivel acordado de seguridad de la información y de prestación del servicio alineado a los acuerdos pactados entre las partes, manteniendo la confidencialidad, integridad y disponibilidad de la información de CFN B.P.

Esta política aplica para la gestión con los proveedores que presten servicios asociados con el tratamiento o resguardo de los activos de información que tiene CFN B.P. y que cumplan con los siguientes hitos:

i. Activos de información que sean custodiados por entes externos a la institución.
ii. Activos de información utilizados por terceros.

**Artículo 57.- NORMAS:**

Las siguientes son las normas de control interno que deben cumplirse en CFN B.P.

**1. Gestionar la relación con los proveedores asociados al tratamiento o resguardo de los activos de información de CFN B.P.**

a) En caso que la Institución necesite contratar servicios de tratamiento o resguardo de activos de información, tales como: servicios de hosting e infraestructura, plataforma tecnológica, almacenaje de información física o digital, entre otros, la Unidad Administrativa requirente, de manera coordinada con la Gerencia de Seguridad de la Información, debe incluir en los TDR's o especificaciones funcionales, las características relacionadas con los temas de Seguridad de la Información en lo que al tratamiento o resguardo de los activos de información se refiere (al menos, debería contemplar los mismos estándares que los existentes en CFN B.P.), con el fin de garantizar la confiabilidad, disponibilidad e integridad de la información, de tal manera que cuando el proveedor los implemente, sea una responsabilidad de la Gerencia de Seguridad de la Información validarlos.

b) Las unidades requirentes, de manera conjunta con la Gerencia de Seguridad de la Información, deben analizar y realizar una evaluación de los riesgos de seguridad de la información asociados al servicio entregado por el proveedor, con el objeto de identificar brechas que puedan ser potenciales vulnerabilidades que exponga la continuidad de los procesos operativos o puedan dañar la imagen de la institución.
c) La Gerencia de Seguridad de la Información en conjunto con el responsable de la unidad administrativa requirente del servicio de tratamiento o resguardo de activos de información deben realizar un análisis del proveedor y su administración de la seguridad de la información, previo a la contratación del servicio con el fin de minimizar los impactos negativos que pueda representar la relación de dicho proveedor con la institución.
d) Cuando se contraten proveedores que desarrollen sistemas de información para CFN B.P. la Gerencia de Seguridad de la Información debe considerar la revisión de los servicios y/o productos elaborados a partir de revisiones técnicas que cumplan con los requisitos mínimos de seguridad de la información establecidos en la institución.
e) Cuando existan sistemas de información que sean expuestos a la red externa de la institución, como parte de la aceptación del producto (previo a la salida a producción), se debe considerar adicionalmente la ejecución de pruebas de pen testing (penetración) que garanticen razonablemente la confidencialidad, integridad y disponibilidad de los datos manipulados en el sistema.
f) La Gerencia de Seguridad de la Información es la encargada de velar por la contraparte técnica en materia de seguridad en todas aquellas contrataciones de servicios o productos que tengan relación con el tratamiento, manipulación, almacenamiento, transmisión o resguardo de los activos de información de CFN B.P., de ahí la importancia que las Unidades Administrativas requirentes involucren a la Gerencia de Seguridad de la Información cuando se vayan a ejecutar contrataciones relacionadas con la Seguridad de la Información.
g) La Gerencia de Seguridad de la Información debe asesorar a los Propietarios de la Información o personal de la institución encargado de la elaboración del contrato de servicios y/o productos relacionado con el tratamiento o resguardo de la información con el objetivo de que puedan evaluar adecuadamente los riesgos implicados que guarden relación con la seguridad de la información.
h) La Gerencia de Seguridad de la Información debe implementar medidas de seguridad que permitan mitigar los riesgos asociados a la relación con los proveedores o coordinar las implementaciones que sean del caso con las Unidades Administrativas requirentes.
i) La Gerencia de Seguridad de la Información puede analizar, evaluar y controlar la información que CFN B.P. debe entregar en virtud del contrato al proveedor con la finalidad de analizar dicho requerimiento y el/la Gerente de Seguridad de la Información procede a aprobar o rechazar la entrega de la misma.
j) Los Propietarios de la Información deben ejecutar de manera periódica un monitoreo de los servicios brindados por los proveedores de tratamiento o resguardo de los activos de información de CFN B.P. y notificar a la Gerencia de Seguridad de la Información cualquier evento que pueda afectar a la seguridad.
k) El acceso físico por parte de los proveedores a los activos de información debe ser controlado y supervisado por personal técnico, Propietarios de la Información o personal de la Gerencia de Seguridad de la Información correspondiente.
l) Los propietarios de la Información deben revisar periódicamente las restricciones y accesos a los activos de información, tomando en cuenta las políticas de control de acceso aplicables. De encontrar una novedad, deben notificarla a la Gerencia de Seguridad de la Información.
m) El/La Gerente de Seguridad de la Información debe proporcionar al Comité de Administración de Seguridad de la Información un Plan de Seguridad de la Información que apruebe la implementación de los controles identificados y acciones de mejora para esta política.
n) El/La Gerencia de Seguridad de la Información debe monitorear con una frecuencia al menos anual, el cumplimiento y la efectividad de los controles establecidos en la entidad para los representantes de los proveedores, para el buen uso de los activos de información.
o) Es responsabilidad de las Unidades Administrativas requirentes y propietarios de la Información, notificar a la Gerencia de Seguridad de la Información, para que se retiren o se ajusten los derechos de accesos a los

activos de información a todos los empleados de proveedores y/o terceros al término del empleo, contrato o acuerdo y/o cambios en sus funciones, o finalización del contrato.

**2. Seguridad de la información en las relaciones con los proveedores**

p) Analizar, acordar y documentar los requisitos de seguridad de la información que permitan mitigar los riesgos asociados al acceso de los proveedores a los activos de CFN B.P.

q) Establecer y acordar todos los requisitos necesarios relacionados con la seguridad de la información para que cada proveedor autorizado pueda acceder, procesar y/o almacenar información en la infraestructura tecnológica de la institución.

r) Todo acuerdo con los proveedores debe incluir los requisitos para el adecuado manejo de los riesgos asociados con la seguridad de la información.

s) Los funcionarios de la entidad, terceros y/o proveedores deben ser responsables por el tratamiento que se dé a los activos de información que se encuentren a su cargo.

t) Todo usuario externo, está facultado para utilizar única y exclusivamente los activos de información que se le fueron asignados para ejecutar sus actividades y además deberá acatar las responsabilidades que devenga la utilización de dichos activos.

**3. Gestión de la prestación del servicio brindado por parte del proveedor**

u) Los Propietarios de la Información deben monitorear y revisar de manera periódica la prestación de los servicios brindados por el proveedor. Cualquier novedad debe ser notificada a la Gerencia de Seguridad de la Información.

v) Los Propietarios de la Información de CFN B.P. deben analizar y gestionar los cambios relacionados con los servicios prestados por los proveedores, incluyendo el mantenimiento, la mejora de políticas, procedimientos y controles de la seguridad de la información considerando la sensibilidad de la información de la institución, siempre en coordinación con la Gerencia de Seguridad de la Información.

w) Los proveedores no pueden manipular, eliminar y/o destruir cualquier activo de información, sin la previa autorización del propietario de la información o el responsable del activo y/o la Gerencia de Seguridad de la Información o sin seguir los protocolos indicados en la normativa vigente de los organismos de control aplicables para períodos de conservación y procedimientos de descarte de información.

## CAPÍTULO XIV: IDENTIFICACIÓN Y DOCUMENTACIÓN DE LOS REQUERIMIENTOS Y CONTROLES MÍNIMOS DE SEGURIDAD PARA CADA ACTIVO DE INFORMACIÓN EN BASE A UNA EVALUACIÓN DE RIESGOS

### Artículo 58.- GENERALIDADES DE LA IDENTIFICCIÓN Y DOCUMENTACIÓN DE LOS REQUERIMIENTOS Y CONTROLES MÍNIMOS DE SEGURIDAD PARA CADA ACTIVO DE INFORMACIÓN EN BASE A UNA EVALUACIÓN DE RIESGOS:

Define los lineamientos necesarios para la identificación y documentación de los requerimientos y controles mínimos de seguridad para cada activo de información de CFN B.P. con base a una evaluación de riesgos.

Esta política aplica para todos los activos de información que tiene CFN B.P. que cumplan con los siguientes hitos:

i. Activos de información que sean custodiados por los empleados y/o sean utilizados para desempeñar actividades inherentes a su cargo.
ii. Sean utilizados por terceros.
iii. Utilizados dentro y/o fuera de CFN B.P. para el ejercicio de sus funciones.

**Artículo 59.- NORMAS:**
Las siguientes son las normas de control interno que deben cumplirse en CFN B.P.

**1. Gestionar la identificación de los activos de información relevantes de la institución**
a) La Gerencia de Seguridad de la Información debe mantener actualizado el inventario de los activos de información más relevantes que posee CFN B.P. en sus diferentes procesos y funciones, principalmente en los procesos críticos de CFN B.P.

**2. Identificar los activos de información críticos de la institución**
b) La Gerencia de Seguridad de la Información debe identificar los activos de información críticos de CFN B.P, aplicando el procedimiento respectivo del Sistema de Gestión de la Seguridad de la Información, de manera coordinada con los propietarios de la información.

**3. Realizar la evaluación de riesgos de los activos de la información críticos**
c) El Gerente de Seguridad de la Información debe realizar las evaluaciones de riesgos de seguridad de la información sobre los activos de información críticos de CFN B.P., usando el respectivo procedimiento y metodología del Sistema de Gestión de la Seguridad de la Información.
d) La evaluación de riesgos de seguridad de información debe conducir a la identificación de los riesgos más preocupantes para cada activo de información crítico.
e) Se deben identificar los controles existentes para mitigar los riesgos más preocupantes de cada activo de información critico de CFN B.P., usando el respectivo procedimiento y metodología del Sistema de Gestión de la Seguridad de la Información.
f) El/La Gerente de Seguridad de la Información debe proponer un Plan de Seguridad de la Información al Comité de Administración de Seguridad de la Información con un tratamiento a los riesgos más preocupantes para cada activo de información crítico, incluyendo una propuesta que puede contener:

- Nuevos requerimientos de seguridad de la información para mitigar riesgos;
- Controles específicos nuevos, mínimos;
- Eliminación de controles obsoletos o redundantes; y,
- Reforzamiento a controles existentes rescatables para la evaluación y aprobación respectiva.

g) El/La Gerente de Seguridad de la Información debe documentar los requerimientos y las decisiones sobre los controles, organizando las tareas y proyectos siguientes para que el Comité de Administración de Seguridad de la Información realice las respectivas asignaciones.

## CAPÍTULO XV: DEFINICIÓN Y VERIFICACIÓN DE REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA NUEVOS SISTEMAS O SU MANTENIMIENTO

**Artículo 60.- GENERALIDADES PARA LA DEFINICIÓN Y VERIFICACIÓN DE REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA NUEVOS SISTEMAS O SU MANTENIMIENTO:**

Garantiza que la seguridad de la información forme parte integral en los requerimientos de los nuevos sistemas de información y/o su mantenimiento a lo largo de todo el ciclo de vida de las aplicaciones, salvaguardando la confidencialidad, integridad y disponibilidad de la información de CFN B.P.

Esta política aplica a la adquisición de los nuevos sistemas de información, actualización y /o mantenimiento de los sistemas existentes en CFN B.P. y que:

i. Son gestionados por los responsables de las Unidades Administrativas de CFN B.P.
ii. Utilizados por terceros y/o personal facultado por la institución.

**Artículo 61.- NORMAS:**
Las siguientes son las normas de control interno que deben cumplirse en CFN B.P.

**1. Definición de requerimientos de seguridad de la información para nuevos sistemas o su mantenimiento.**
a) La Gerencia de Seguridad de la Información debe definir los requisitos mínimos de seguridad que deben cumplir los nuevos sistemas de información y/o los mantenimientos que se realicen en las aplicaciones de CFN B.P.
b) La Gerencia de Seguridad de la Información debe analizar las especificaciones de los requerimientos de la seguridad de la información que se van aplicar en CFN B.P. cuando se adquieran nuevos sistemas o en el mejoramiento de los sistemas existentes.
c) Los propietarios de los activos de información deben proponer los requerimientos relacionados con las pistas de auditoría de los procesos funcionales de los aplicativos, para que sean aprobados por la Gerencia de Seguridad de la Información. Las pistas de Auditoría relacionadas con la Administración de Usuarios, Roles y Accesos, deben ser presentadas por la Gerencia de Seguridad de la Información.
d) La Gerencia de Seguridad de la Información debe definir los controles necesarios para inspeccionar los cambios dentro del ciclo de vida de las aplicaciones.
e) El Gerente de Seguridad de la Información debe proponer un Plan de Seguridad de la Información al Comité de Administración de Seguridad de la Información con un tratamiento a los riesgos más relevantes relacionados con la adquisición de nuevos sistemas o su mantenimiento, la propuesta puede contener:

- Nuevos requerimientos de seguridad de la información para mitigar los riesgos;
- Controles específicos, nuevos y/o mínimos;
- Eliminación de controles obsoletos o redundantes; y,
- Reforzamiento a controles existentes rescatables para la evaluación y aprobación respectiva.

**2. Verificación de requerimientos de seguridad de la información para nuevos sistemas o su mantenimiento.**
f) La Gerencia de Seguridad de la Información debe revisar y verificar que las nuevas aplicaciones contemplen todos los requisitos mínimos de seguridad, con el fin de garantizar que no haya un impacto negativo sobre las operaciones o la seguridad organizacional.
g) La Gerencia de Tecnologías de la Información debe emitir un informe sobre la validación de vulnerabilidades que afecten a la Seguridad a nivel de código fuente, previo a la liberación de aplicaciones y dicho informe debe ser validado por la Gerencia de Seguridad de la Información.
h) La Gerencia de Tecnologías de la Información debe realizar las actualizaciones periódicas a los procedimientos aplicados para el control de los cambios de los sistemas, los cuales deben ser revisados y validados por la Gerencia de Seguridad de la Información.
i) La Gerencia de Seguridad de la Información establece lineamientos rigurosos que ayuden a verificar la aceptación de los requerimientos solicitados en los nuevos sistemas de información, actualizaciones, renovaciones y/o nuevas versiones, que afecten a su Seguridad.
j) La Gerencia de Seguridad de la Información, de manera coordinada con los propietarios de la información, verifica que los datos de pruebas utilizados para certificar que se cumplan con los requerimientos solicitados en los nuevos sistemas sean seleccionados, protegidos y controlados cuidadosamente.

## CAPÍTULO XVI: DETECTAR Y EVITAR LA INSTALACIÓN DE SOFTWARE NO AUTORIZADO O SIN LICENCIA; Y, PARA INSTALAR Y ACTUALIZAR PERIÓDICAMENTE APLICACIONES DE DETECCIÓN Y DESINFECCIÓN DE VIRUS INFORMÁTICOS Y DEMÁS SOFTWARE

### Artículo 62.- GENERALIDADES PARA DETECTAR Y EVITAR LA INSTALACIÓN DE SOFTWARE NO AUTORIZADO O SIN LICENCIA; Y, PARA INSTALAR Y ACTUALIZAR PERIÓDICAMENTE APLICACIONES DE DETECCIÓN Y DESINFECCIÓN DE VIRUS INFORMÁTICOS Y DEMÁS SOFTWARE:

Detectar y evitar la instalación de software no autorizado o sin la respectiva licencia; así como también definir las consideraciones necesarias para instalar y actualizar de manera periódica las aplicaciones de detección y desinfección de virus informáticos y demás software de seguridad con el fin de garantizar la integridad de los sistemas y evitar la explotación de vulnerabilidades en los equipos informáticos y redes de datos de CFN B.P.

Esta política aplica para los sistemas de información, actualización y/o mantenimiento de los sistemas existentes en CFN B.P. y que:

i. Son gestionados por los responsables de las Unidades Administrativas de CFN B.P.
ii. Utilizados por terceros y/o personal facultado por la institución.
iii. Sirven para detectar software no autorizados y/o sin licencia.
iv. Permiten detectar y desinfectar virus informáticos.

### Artículo 63.- NORMAS:

Las siguientes son normas de control interno que deben cumplirse en CFN B.P.

**1. Gestión para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia.**

a) La Gerencia de Seguridad de la Información debe verificar de manera periódica que los usuarios no tengan habilitada la opción de instalar software en los equipos de CFN B.P. La Gerencia de Tecnologías de la Información debe proporcionar a la Gerencia de Seguridad de la Información, el detalle del inventario de licencias y las instalaciones a los usuarios, de tal manera que se pueda validar que el software que se encuentre instalado, esté actualizado y con sus respectivas licencias.

b) La Gerencia de Tecnologías de la Información debe implementar los controles necesarios para restringir la instalación de software a los usuarios de la Institución. Únicamente el personal designado por la Gerencia de Tecnologías de la Información, debe tener los permisos para la instalación de software y es su responsabilidad evitar la instalación de software no autorizado o sin la respectiva licencia.

c) La Gerencia de Tecnologías de la Información, debe implementar las herramientas tecnológicas necesarias que permitan a la Gerencia de Seguridad de la Información hacer un control para la detección de software no autorizados o sin licencia en los equipos informáticos de CFN B.P., de una manera más automatizada.

d) La Gerencia de Tecnologías de la Información debe garantizar la integridad de los sistemas de información de la entidad y la Gerencia de Seguridad de la Información debe realizar las revisiones del caso, de tal manera de identificar posibles riesgos de seguridad.

e) La Gerencia de Seguridad de la Información debe asesorar a la Gerencia de Tecnologías de la Información para que la institución cuente con tecnología moderna que ayude a controlar, restringir y monitorear la instalación de software no autorizado en CFN B.P.

f) El Gerente de Seguridad de la Información debe proponer un Plan de Seguridad de la Información al Comité de Administración de Seguridad de la Información con un tratamiento a los riesgos más relevantes relacionados con la instalación de software no autorizado o sin la respectiva licencia, la propuesta puede contener:

- Nuevos requerimientos de seguridad de la información para mitigar los riesgos;
- Controles específicos, nuevos y/o mínimos;
- Eliminación de controles obsoletos o redundantes; y,
- Reforzamiento a controles existentes rescatables para la evaluación y aprobación respectiva.

**2. Lineamientos para instalar y actualizar periódicamente software de CFN B.P.**

g) La Gerencia de Seguridad de la Información debe definir los requisitos mínimos de seguridad que deben cumplir los sistemas de información cuando se efectúen las respectivas actualizaciones y/o instalación de software.

h) La Gerencia de Tecnologías de la Información debe tener procedimientos para la instalación y actualización de software en los sistemas de información de la entidad.

i) La Gerencia de Seguridad de la Información debe definir restricciones relacionadas con la instalación o actualización de software que se requieran realizar en los equipos informáticos.

j) La Gerencia de Seguridad de la Información debe establecer reglas que ayuden a controlar los cambios y/o actualizaciones de los paquetes de software, mientras que la Gerencia de Tecnologías de la Información las implementa.

k) Los usuarios de CFN B.P. no pueden instalar y/o actualizar software de CFN B.P.; cuando lo requieran deben hacer la solicitud a la Gerencia de Tecnologías de la Información, quienes previamente deben tener la autorización por parte de la Gerencia de Seguridad de la Información, para proceder.

l) La Gerencia de Seguridad de la Información debe monitorear la instalación y/o actualización de software según los protocolos establecidos en la entidad.

m) La Gerencia de Tecnologías de la Información debe velar por la debida protección de las transacciones efectuadas en los nuevos/actualizados aplicativos y/o aplicaciones de CFN B.P.

**3. Lineamientos para instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos**

n) La Gerencia de Tecnologías de la Información debe revisar, actualizar y generar reportes de monitoreo de las aplicaciones de detección y desinfección de virus informáticos con el fin de salvaguardar la integridad de los sistemas. Además, debe poner en conocimiento los reportes que se generen a la Gerencia de seguridad de la Información, en los cuales se debe contemplar los riesgos y las oportunidades de mejora.

o) La Gerencia de Tecnologías de la Información debe implementar mecanismos de control para la detección, prevención y recuperación para proteger la información contra malware y/o otros virus informáticos. Estos mecanismos deben ser acordados con la Gerencia de Seguridad de la Información.

p) La Gerencia de Tecnologías de la Información debe gestionar de manera oportuna las vulnerabilidades técnicas que estén asociadas a los sistemas de información utilizados en CFN B.P., de manera coordinada con la Gerencia de Seguridad de la Información.

q) La Gerencia de Seguridad de la Información debe plantear reglas que gobiernen la actualización permanente de los antivirus y/o parches de seguridad en los equipos informáticos de la institución, mientras que la Gerencia de Tecnologías de la Información las implementa.

r) La Gerencia de Seguridad de la Información, debe verificar que el software de detección y desinfección de virus informáticos sea el más idóneo para la institución con el fin de garantizar que no haya un impacto negativo sobre las operaciones o la seguridad organizacional.

s) La Gerencia de Seguridad de la Información debe gestionar con las Unidades Administrativas pertinentes para que se realice charlas de concienciación de los usuarios y/o utilizar los canales de comunicación habilitados en la Institución, para evitar la filtración de virus en los equipos informáticos de la institución.

## CAPÍTULO XVII: TRAER SU PROPIO DISPOSITIVO (BYOD, BRING YOUR OWN DEVICE)

**Artículo 64.- GENERALIDADES PARA TRAER SU PROPIO DISPOSITIVO /BYOD, BRING YOUR OWN DEVICE):**

Define las medidas necesarias para controlar y evitar que la información clasificada de CFN B.P. se vea comprometida en su integridad, disponibilidad y confidencialidad al ser almacenada en, o accedida a través de, dispositivos ajenos a la entidad (BYOD-Bring your own device, Traer su propio dispositivo).

La presente política aplica para todos los dispositivos electrónicos personales tales como teléfonos inteligentes y tabletas, computadores portátiles o de escritorio, unidades de memoria USB, cámaras digitales, reproductoras de música y video, etc., que:

i. no son propiedad o no están bajo control permanente de CFN B.P.;
ii. pertenecen y/o usan los empleados y/o terceros; y,
iii. son utilizados para acceder y almacenar información de CFN B.P., dentro o fuera de las instalaciones de la empresa.

En esta política se identifica a estos dispositivos como BYOD-Bring your own device/Traer su propio dispositivo, los cuales tienen la capacidad de almacenar, transferir o hasta procesar diferentes tipos de información.

Los datos e información de CFN B.P. que se almacenan, transfieren o procesan en dispositivos BYOD siguen perteneciendo a la empresa, y CFN B.P. mantiene el derecho a controlar esos datos e información, aunque no sea propietaria del dispositivo.

La política debe ser observada y cumplida por todos los funcionarios y colaboradores sean estos empleados directos, externalizados o servicios profesionales, y por entidades externas como proveedores o entidades de control los cuales tengan el acceso a la información y los recursos informáticos que maneja CFN B.P. para el desarrollo de sus actividades.

**Artículo 65.-NORMAS:**

Las siguientes son las normas de control interno que deben cumplirse.

**1. Quiénes pueden utilizar BYOD y para qué**

a) CFN B.P. acota el uso de BYOD únicamente a esa cantidad LIMITADA de empleados o proveedores que, de otra forma, no podrían realizar su trabajo.

- El Gerente de Seguridad de la Información crea/actualiza una lista de cargos y/o personas a quienes se les permite utilizar BYOD junto con las aplicaciones y bases de datos a las cuales pueden acceder con sus propios dispositivos.
- El Gerente de Seguridad de la Información crea/actualiza una lista de aplicaciones prohibidas para BYOD.

b) Los dispositivos BYOD deben ser registrados con el Gerente de Seguridad de la Información, y aprobados previamente para su uso.

**2. Qué dispositivos BYOD están permitidos**

c) El Gerente de Seguridad de la Información crea una Lista de dispositivos aceptados que pueden ser utilizados como BYOD, junto con configuraciones obligatorias para cada dispositivo (Por ejemplo, cortafuegos, copias de seguridad, bloqueo de pantalla, etc.)

**3. Uso Aceptable de dispositivo BYOD**

Lo siguiente es obligatorio para todos los BYOD:

d) El funcionario, contratista o tercero al que se autorice un BYOD debe garantizar bajo acuerdo de confidencialidad (Anexo 3) que la información de CFN B.P. es almacenada de forma aislada a la información personal que guarde en su dispositivo.

e) El propietario del BYOD debe realizar copias de seguridad periódicas de la información institucional contenida en los BYOD, en la plataforma tecnológica de CFN B.P.

f) En el caso que el propietario del BYOD requiera copiar información desde la plataforma tecnológica de CFN B.P. al BYOD, necesita el consentimiento por escrito del superior jerárquico.

g) A todos los BYOD se les debe aplicar software antivirus, y en la medida de lo posible, software de prevención de intrusiones (malware), software para administración de dispositivos móviles, etc.

h) Cuando sea posible, la información de la empresa esta encriptada (cifrada) en los dispositivos BYOD de acuerdo con la política de controles criptográficos.

i) Los dispositivos BYOD deben estar protegidos mediante métodos de autenticación como, por ejemplo, claves, contraseñas, lectores biométricos, etc.

j) El contenido de CFN B.P. no debe estar compartido para ningún tipo de redes o usuarios (excepto dentro de la intranet de CFN B.P.) o únicamente pueden compartirse mediante algún método seguro de conexión a la red de la empresa, por ejemplo, VPN.

k) Cuando se utilicen dispositivos BYOD fuera de las instalaciones de CFN B.P., no deben ser dejados desatendidos y, si es posible, deben estar físicamente resguardados bajo llave.

l) Cuando se utilizan dispositivos BYOD en lugares públicos, se debe tener la precaución de que los datos e información no puedan ser leídos por personas no autorizadas.

m) Se deben instalar periódicamente parches y actualizaciones aplicables en los BYOD.

n) La información clasificada debe contar con protección adicional de acuerdo con la Política de Clasificación y Tratamiento de la información o equivalente.

o) Se debe notificar a la Gerencia de Seguridad de la Información antes de eliminar, vender o entregar un BYOD a terceros para su reparación.

p) No se permite hacer lo siguiente con los dispositivos BYOD:

- Permitir el acceso a cualquiera que no sea el propietario del dispositivo.
- Instalar aplicaciones que están enumeradas en la Lista de aplicaciones prohibidas para BYOD. Almacenar material ilegal en el dispositivo.
- Instalar software sin licencia.
- Conectarse por Bluetooth con cualquier tipo de dispositivo. Conectarse a redes Wi-Fi desconocidas.
- Almacenar claves localmente.
- Almacenar localmente información de datos personales.
- Transferir datos de CFN B.P. a otros dispositivos no permitidos o no registrados.

## CAPÍTULO XVIII: ELIMINACIÓN DE LA INFORMACIÓN CRÍTICA DE LA ENTIDAD, DE MANERA SEGURA Y CONSIDERANDO LOS REQUERIMIENTOS LEGALES Y REGULATORIOS

**Artículo 66.- GENERALIDADES PARA LA ELIMINACIÓN DE LA INFORMACIÓN CRÍTICA DE LA ENTIDAD, DE MANERA SEGURA Y CONSIDERANDO LOS REQUERIMIENTOS LEGALES Y REGULATORIOS:**

Eliminar la información crítica de CFN B.P., de manera segura en los medios de información, respetando la normativa vigente.

Esta política aplica para la eliminación de la información crítica de CFN B.P. que se encuentre almacenada en:

i. Documentos físicos y/o formato digital.
ii. Medios de almacenamientos.
iii. Listados de programas.
iv. Datos de prueba.
v. Documentación del sistema.

**Artículo 67.-NORMAS:**

Las siguientes son las normas de control interno que deben cumplirse en la CFN B.P.

**1. Eliminación de información crítica de manera segura**

o) La Gerencia de Seguridad de la Información en coordinación con la Gerencia de Tecnologías de la Información, deben asegurar que no se elimina información que debe mantenerse como registro histórico según lo establecen los requerimientos legales y regulatorios.

p) La Gerencia de Seguridad de la Información y los propietarios de la información, validan el tipo de información que se planifica eliminar de los medios de almacenamiento y/o recursos tecnológicos de CFN B.P.

q) El/La Gerente de Seguridad de la Información autoriza la eliminación de la información crítica de la entidad previa consulta y/o permiso de los propietarios de la información.

r) Todos los usuarios de CFN B.P. deben seguir las buenas prácticas de seguridad en lo concerniente a la eliminación segura de la información crítica manejada en la institución.

s) Se debe mantener registro de las autorizaciones proporcionadas por los propietarios de la información para ejecutar eliminación de información crítica de CFN B.P.

t) La Gerencia de Seguridad de la Información verifica que se manejen varios tipos de actividades de saneamiento y eliminación de medios de almacenamiento, y que se considere, por ejemplo, eliminación, limpieza, purga y/o destrucción.

u) La Gerencia de Tecnologías de la Información debe utilizar programas que permitan efectuar un borrado de forma segura de la información de un disco duro o cualquiera de los medios de almacenamiento utilizados en CFN B.P.

v) Al finalizar un proceso de eliminación de información crítica de la CFN B.P., el responsable de esta actividad debe elaborar un informe que compruebe la efectividad del borrado seguro y ponerle en conocimiento de la Gerencia de Seguridad de la Información y de los propietarios de la información.

w) Para eliminar la información crítica en soportes no electrónicos y soportes magnéticos, el responsable de esta actividad debe utilizar el triturado como modo seguro de eliminación y ponerle en conocimiento de la Gerencia de Seguridad de la Información y de los propietarios de la información.

x) A la hora de desechar un soporte de almacenamiento electrónico que no funcione o que se haya quedado obsoleto, la Gerencia de Tecnologías de la Información debe utilizar métodos de des-magnetización o destrucción física, imposibilitando la reutilización de dicho dispositivo y preservando los protocolos de privacidad de la información.
y) Documentar todas las operaciones de borrado que se hayan aplicado para la eliminación segura de la información crítica de la entidad y ponerle en conocimiento de la Gerencia de Seguridad de la Información y de los propietarios de la información.

**2. Gestionar la eliminación de información crítica de manera segura**

z) La Gerencia de Seguridad de la Información debe generar procedimientos formales para la eliminación segura de la información crítica de CFN B.P., de acuerdo con la tecnología involucrada.
aa) La Gerencia de Seguridad de la Información debe velar que se apliquen estándares para la eliminación segura de datos y la eliminación de la remanencia de datos, de acuerdo con la tecnología involucrada.
bb) La Gerencia de Seguridad de la Información en coordinación con el propietario de la información deben monitorear de manera permanente las actividades ligadas con la eliminación segura de la información crítica de la institución.
cc)La Gerencia de Seguridad de la Información debe implementar medidas de seguridad que permitan mitigar los riesgos asociados con la eliminación de la información crítica de la entidad.
dd) El/La Gerente de Seguridad de la Información proporciona al Comité de Gestión de Seguridad de la Información un Plan de Seguridad de la Información que incluya la implementación de los controles identificados y acciones de mejora para esta política.

**3. Responsabilidades de los usuarios relacionadas con la eliminación de información crítica**

ee) Respetar los procesos internos de CFN B.P. para la eliminación segura de la información crítica que tiene la entidad almacenada tanto de manera física y/o digital.
ff) Informar a la Gerencia de Seguridad de la Información y/o propietarios de la información, sobre la información crítica de la institución que se vaya a eliminar.
gg) Solicitar autorización de los propietarios de información y de la Gerencia de Seguridad de la Información antes de realizar cualquier proceso de eliminación de información crítica de CFN B.P.
hh) Seguir las buenas prácticas de la institución para la eliminación segura de la información; con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información de CFN B.P.
ii) Los funcionarios de la entidad, terceros y/o proveedores deben ser responsables por la autorización proporcionada para la eliminación de información crítica que este a su cargo.
jj) Todo usuario externo está facultado para eliminar única y exclusivamente la información crítica que se le sea proporcionada por personal autorizado de CFN B.P.

**4. Prohibiciones de los usuarios relacionados con la eliminación de información crítica**

No se permite a los diferentes usuarios de CFN B.P. que tengan acceso a los sistemas de información, aplicativos y/o recursos tecnológicos de la entidad a que realicen las siguientes acciones:
kk) Eliminar información crítica de la entidad sin seguir los protocolos establecidos.
ll) Intentar eliminar cualquier tipo de configuración establecida en los medios de almacenamiento.
**mm)** Eliminar y/o destruir cualquier información crítica de los activos de información, sin la previa autorización del propietario de la información o la Gerencia de Seguridad de la Información o sin seguir los protocolos indicados en la normativa vigente de los organismos de control aplicables para eliminación y descarte de información.

## CAPÍTULO XIX: PROTEGER LA INFORMACIÓN CONTENIDA EN: DOCUMENTOS, MEDIOS DE ALMACENAMIENTO U OTROS DISPOSITIVOS EXTERNOS E INTERCAMBIO ELECTRÓNICO, CONTRA: ROBO, UTILIZACIÓN O DIVULGACIÓN NO AUTORIZADA DE INFORMACIÓN

**Artículo 68.- GENERALIDADES PARA PROTEGER LA INFORMACIÓN CONTENIDA EN: DOCUMENTOS, MEDIOS DE ALMACENAMIENTO U OTROS DISPOSITIVOS EXTERNOS E INTERCAMBIO ELECTRÓNICO, CONTRA: ROBO, UTILIZACIÓN O DIVULGACIÓN NO AUTORIZADA DE INFORMACIÓN:**

Proteger la información de CFN B.P. contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico; contra: robo, utilización o divulgación no autorizada de la información; garantizando que dicha información de la institución no se vea comprometida en su confidencialidad, integridad y disponibilidad.

Esta política aplica para toda información de la CFN B.P. que se encuentre almacenada en:

i. Documentos físicos y/o o en formato digital.
ii. Medios de almacenamiento.
iii. Otros dispositivos externos.

**Artículo 69.-NORMAS:**

Las siguientes son las normas de control interno que deben cumplirse en CFN B.P.

**1. Proteger la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, contra: robo, utilización o divulgación no autorizada de información.**

a) La Gerencia de Seguridad de la Información debe implementar medidas de seguridad que permitan mitigar los riesgos asociados con el robo, la utilización y/o la divulgación no autorizada de la información de CFN B.P.

b) La Gerencia de Tecnologías de la Información, con la autorización de la Gerencia de seguridad de la Información debe instalar programas licenciados para proteger la información de CFN B.P. contra software malicioso, como antivirus, anti-spyware, anti-phishing entre otras amenazas.

c) La Gerencia de Tecnologías de la Información debe implementar las herramientas tecnológicas pertinentes para proteger la fuga de la información a través de medios removibles u otros dispositivos asignados a los funcionarios y/o utilizados por personal autorizado por la entidad, de manera coordinada con la Gerencia de Seguridad de la Información.

d) La Gerencia de Tecnologías de la Información debe implementar medidas de seguridad adecuadas para el almacenamiento y resguardo de los medios removibles, de tal forma que se evite accesos no autorizados, daños, pérdida de información o robo del medio, de manera coordinada con la Gerencia de Seguridad de la Información.

e) La Gerencia de Tecnologías de la Información debe velar para que no se divulguen direcciones IP privadas ni información de enrutamiento a partes no autorizadas.

f) La Gerencia de Tecnologías de la Información debe implementar la restricción del envío de información a correos externos no autorizados por la Gerencia de Seguridad de la Información.

g) La Gerencia de Tecnologías de la Información debe conocer las políticas de seguridad y los procedimientos operativos para garantizar la continua administración de los firewalls y routers con el objetivo de evitar el acceso no autorizado a la red. Cualquier evento inusual debe ser comunicado a la Gerencia de Seguridad de la Información.

**2. Supervisar que la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, este protegida contra: robo, utilización o divulgación no autorizada de información.**

h) La Gerencia de Seguridad de la Información debe monitorear de manera permanente las actividades ligadas con la protección de la información de la institución.

i) La Gerencia de Seguridad de la Información debe monitorear de manera periódica que no se autorice la divulgación de ninguna dirección IP privada ni de información de enrutamiento a entidades externas.

j) La Gerencia de Seguridad de la Información debe monitorear los medios y comunicaciones de salida de CFN B.P. para determinar la información oculta con el fin de prevenir la fuga de información.

k) La Gerencia de Seguridad de la Información debe monitorear los controles que aseguran que un tercero no pueda deducir, extraer información de las comunicaciones, sistemas de modulación o de enmascaramiento, a partir de un comportamiento específico.

l) La Gerencia de Seguridad de la Información debe monitorear de manera permanente las actividades del personal y de los sistemas con el fin de evitar alguna actividad inusual.

m) La Gerencia de Seguridad de la Información debe monitorear el uso de los recursos utilizados por los funcionarios y la transmisión de datos por la red.

**3. Gestionar la protección de la información contra: robo, utilización o divulgación no autorizada de información.**

n) La Gerencia de Seguridad de la Información debe implementar procedimientos formales que ayuden a proteger la información de CFN B.P. contra el hurto, utilización y/o divulgación no autorizada de su información.

o) La Gerencia de Tecnologías de la Información debe implementar controles apropiados para proteger la documentación digital contra pérdida, destrucción y falsificación de la información, en coordinación con la Gerencia de Seguridad de la Información. De la misma manera, los propietarios de la información deben implementar los controles antes mencionados sobre la documentación física.

p) La Gerencia de Seguridad de la Información debe promover el uso de acuerdos de confidencialidad de no divulgación de información conforme a la constitución, las leyes, las necesidades de protección de información y el Esquema Gubernamental de Seguridad de la Información - EGSI, tanto para los funcionarios y colaboradores, sean estos empleados directos, externalizados o servicios profesionales, y por entidades externas como proveedores o entidades de control, los cuales estén directamente relacionados con el manejo de la información de la entidad.

q) La Gerencia Jurídica debe asesorar a las Unidades Administrativas que gestionen contratos institucionales con empleados, contratistas y terceros para que se incorpore la firma de un acuerdo de confidencialidad o no divulgación (Anexos 1 <personal interno>, 2 <personal externo> y 3 <utilización de herramientas tecnológicas>, según corresponda), antes de que tengan acceso a la información. En el contrato se debe establecer los parámetros de vigencia del acuerdo, información confidencial referida, formas de acceso, responsabilidades y funciones.

r) La Gerencia de Seguridad de la Información debe monitorear la aceptación, entendimiento y firma de los anexos 1 <personal interno>, 2 <personal externo> y 3 <utilización de herramientas tecnológicas>, según corresponda) del acuerdo de confidencialidad y de no divulgación de la información por parte de los empleados y/o terceros (contratistas, proveedores, pasantes, entre otros) que deban realizar labores para CFN B.P., sea por medios lógicos o físicos, y que involucren el manejo de información.

s) La Gerencia de Seguridad de la Información debe garantizar que todo el personal de las distintas Unidades Administrativas de la institución esté informado de las responsabilidades que le competen con respecto a la protección de la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, contra: robo, utilización o divulgación no autorizada de información proporcionada para sus actividades.

**4. Prohibiciones de los usuarios para proteger la información de CFN B.P.**

t) No se autoriza a los diferentes usuarios de CFN B.P. para que realicen las siguientes acciones con la información contenida en documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico:

- Compartir la información a su cargo con usuarios externos y/o no autorizados.
- Divulgar la información en sitios web no seguros y/o no autorizados por la entidad.
- Acceder a sitios web que no cuenten con certificados de seguridad que avalen la autenticidad de la misma.
- Transferir información de CFN B.P. a otros dispositivos no permitidos o no registrados.
- Abrir archivos, hacer clic sobre enlaces, descargar programas enviados por desconocidos.
- Toda conducta de los empleados, que trasgreda la legislación vigente de la institución.

## CAPÍTULO XX: SEGMENTACIÓN DE LA RED DE DATOS, SELECCIÓN/AJUSTES DE SISTEMAS Y CONTROL DE ACCESOS.

**Artículo 70.- GENERALIDADES SOBRE LA SEGMENTACIÓN DE LA RED DE DATOS, SELECCIÓN/AJUSTES DE SISTEMAS Y CONTROL DE ACCESOS:**

Realizar la segmentación de la red de datos y selección/ajustes de sistemas, controles y autenticación, asegurando la protección de la información de las redes de datos utilizadas por los usuarios internos y/o externos de CFN B.P.; y así evitar accesos no autorizados -inclusive de terceros- y ataques externos.

Esta política aplica para todas las redes de comunicaciones y operaciones, los sistemas y empleados que tengan acceso a la información y/o recursos tecnológicos que utilice CFN B.P. para llevar a cabo las operaciones del negocio.

**Artículo 71.-NORMAS:**

Las siguientes son las normas de control interno que deben cumplirse en CFN B.P.

**1. Gestionar la segmentación de la red de datos**

a) El propietario de la Información, de manera conjunta con la Gerencia de Seguridad de la Información, debe definir los servicios (que están relacionados con los activos de información a su responsabilidad) que están habilitados por Unidades Administrativas o Grupos.

b) La Gerencia de Tecnologías de la Información, de manera coordinada con la Gerencia de Seguridad de la Información debe realizar la implementación de una segmentación de las redes de datos utilizadas en CFN B.P. con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información y de los servicios informáticos de la entidad.

c) La Gerencia de Seguridad de la Información debe monitorear y controlar permanentemente las redes de datos segmentadas de CFN B.P. con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información y de los servicios informáticos de la entidad.

d) La Gerencia de Seguridad de la Información debe evaluar la segmentación de la red de datos considerando criterios que vayan acorde a:

- el giro del negocio;
- los recursos tecnológicos y humanos disponibles;
- las mejores prácticas para reducir, mejorar y controlar el tráfico en la red;
- los requerimientos de seguridad de la información.

e) La Gerencia de Seguridad de la Información debe evaluar y confirmar lineamientos de denegación para las interconexiones entre los segmentos de las redes y subredes de CFN B.P.

**2. Gestionar la selección/ajustes de sistemas, controles y autenticación**

f) La Gerencia de Seguridad de la Información, en coordinación con el propietario de la información, realizan la selección de parámetros y ajustes de sistemas, controles y autenticación autorizados.

g) El/La Gerente de Seguridad de la Información debe evaluar y aprobar la selección de parámetros y ajustes de sistemas, controles y autenticación.

h) La Gerencia de Seguridad de la Información, debe revisar periódicamente las restricciones y accesos a los activos de información, tomando en cuenta las políticas de control de acceso aplicables.

i) La Gerencia de Seguridad de la Información retira o ajusta los derechos de accesos a la información confidencial y a la infraestructura tecnológica de CFN B.P. a todos los empleados y/o terceros al término del empleo, contrato o acuerdo y/o cambios en sus funciones.
j) La Gerencia de Tecnologías de la Información, debe notificar a la Gerencia de Seguridad de la Información, cuando se evidencie algún evento inusual o si se detectan inconvenientes en las restricciones y accesos a los activos de información.

**3. Accesos permitidos a la red y/o aplicativos de la institución**

k) Accesos a la red interna son permitidos únicamente a empleados y/o altos funcionarios de la entidad siempre y cuando se cumplan con los requisitos de seguridad requeridos y se apliquen mecanismos de autenticación.
l) El acceso a terceros es concedido siempre y cuando estén autorizados y cumplan con los requisitos de seguridad establecidos en el contrato, el cual debe estar firmado por las partes involucradas en el mismo.
m) Se permite los accesos a la red interna de la institución desde una red externa a CFN B.P. mediante un mecanismo de autenticación segura y considerando que el tráfico entre ambas redes o sistemas sea cifrado.
n) Todos los accesos a los dispositivos de red se registran mediante archivos de registros o log; se identifica la información que considere necesaria la Gerencia de Seguridad de la Información, con el objeto de determinar de dónde provienen estos accesos.
o) La Gerencia de Seguridad de la Información debe tener acceso a los logs de los aplicativos de la entidad, para actividades de monitoreo, o siempre que necesite obtener evidencias que le ayuden a determinar si existe un incidente de Seguridad de la Información.
p) Los logs no pueden ser eliminados, sin la aprobación del propietario de la información y la Gerencia de Seguridad de la Información.

**4. Accesos no permitidos a la red y/o aplicativos de la institución**

q) No se permite accesos a la red y/o aplicativos de la entidad en los siguientes casos:

- Cuando los usuarios no tengan asignados los permisos necesarios para acceder a los recursos tecnológicos de la entidad.
- En caso de que los empleados, terceros y/o proveedores no acaten las disposiciones de seguridad indicadas en los contratos y/o acuerdos.
- Cuando el acceso a la red provenga de un sitio y/o red considerado como no seguro.
- Cuando los empleados, terceros y/o proveedores no tengan una relación laboral o trabajo pactado con la institución.
- La Gerencia de Seguridad de la Información debe identificar y establecer mecanismos de seguridad de la información, los niveles del servicio y los requisitos de todos los servicios de redes e incluirlos en los acuerdos de servicios de redes; ya sea que dichos servicios sean proporcionados por la misma entidad o por un externo. La implementación está a cargo de la Gerencia de Tecnologías de la Información.

**5. Gestionar la seguridad de las redes de datos y los controles de accesos**

r) El/La Gerente de Seguridad de la Información proporciona al Comité de Gestión de Seguridad de la Información un Plan de Seguridad de la Información que incluya la implementación de los controles identificados y acciones de mejora.
s) La Gerencia de Seguridad de la Información coordina auditorías de seguridad de la red de datos e infraestructura tecnológica cuando considere pertinente con base en el perfil de riesgo de la entidad, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de la información y de los servicios que se brindan en CFN B.P.

## CAPÍTULO XXI: CIFRAR INFORMACIÓN REQUERIDA COMO RESULTADO DEL ANÁLISIS DE RIESGOS.

**Artículo 72.- GENERALIDADES PARA CIFRAR INFORMACIÓN REQUERIDA COMO RESULTADO DEL ANÁLISIS DE RIESGOS:**

Cifrar la información -almacenada o en tránsito, según sea requerido como resultado de un análisis de riesgos; y así evitar que esa información clasificada, manejada por CFN B.P., se vea comprometida en su integridad, confidencialidad, autenticidad y el no repudio.

Los riesgos de seguridad de la información evaluados (medición de riesgos de la seguridad de la información) permiten identificar a los activos de información que deben ser cifrados según lo establezcan los planes de acción determinados.

La lista de activos de información a cifrar puede contener activos de información que no necesariamente se identificaron dentro de un análisis de riesgos.

La presente política debe ser observada y cumplida por todos los funcionarios y colaboradores sean estos empleados directos, externalizados o servicios profesionales, y por entidades externas como proveedores o entidades de control los cuales tengan participación en el cifrado de la información que maneja CFN B.P.

**Artículo 73.-NORMAS:**

Las siguientes son las normas de control interno que deben cumplirse.

**1. Evaluación (medición) de riesgos de seguridad de la información**

a) Los riesgos de seguridad de la información evaluados permiten identificar a los activos de información que deben ser cifrados según establezcan el tratamiento y los planes de acción determinados.

b) Es responsabilidad de los propietarios de la información identificar y presentar a la Gerencia de Seguridad de la Información, los activos de información que deben ser cifrados.

c) La lista de activos de información completa (identificados por Seguridad de la Información en la evaluación de riesgos e identificados por los propietarios de la información) debe ser presentada con solicitud, por parte de la Gerencia de Seguridad de la Información a la Gerencia de Tecnologías de la Información, para que se proceda a instrumentar el cifrado requerido.

**2. De la Selección del Tratamiento a los Riesgos de la Seguridad de la Información**

d) La Gerencia de Tecnologías de la Información debe evaluar si tiene disponible en CFN B.P. la tecnología o servicio para cumplir con el requerimiento de cifrado requerido.

e) En el caso de herramientas o servicios disponibles, la Gerencia de Tecnología debe resolver el requerimiento, estableciendo los protocolos adecuados para la administración continua y permanente del cifrado sobre los activos de información indicados; para lo cual coordina el procedimiento conveniente con la Gerencia de Seguridad de la Información.

f) La Gerencia de Tecnologías de la Información debe proceder a tramitar la adquisición o contratación, lo que aplique, para las herramientas o servicios no disponibles en CFN B.P., para cumplir con los requerimientos de cifrado.

**3. Consideraciones**

**3.1. Información Sensible**

g) A través del análisis de riesgos de seguridad de la información, y del proceso de clasificación de la información se debe identificar qué información debe ser cifrada para garantizar su confidencialidad e integridad. Dicha información puede ser:

- Información sensible, de carácter personal o confidencial;
- Registros con credenciales de autenticación;
- Información almacenada en dispositivos personales o de terceros, incluidos los servicios en nube (cloud);
- Información transferida a través de redes de telecomunicación no confiables o en soportes de almacenamiento físicos no protegidos adecuadamente.

**3.2. Uso de firma electrónica.**

h) Se debe hacer uso de la firma electrónica en aquellos escenarios en los que sea imprescindible garantizar la autenticidad y el no repudio de la información.

i) Se debe establecer el tipo de certificado de representación legal a implantar:

- Certificado de persona jurídica;
- Certificado de pertenencia a empresa;
- Certificado de representante legal;
- Certificado de factura electrónica.

j) Se debe seleccionar la entidad que debe generar los certificados y se debe controlar lo siguiente:

- Periodo de validez;
- Periodos de la revocación;
- Cumplimiento con la legislación (entidad cualificados);
- Gestión de su almacenamiento.

**3.3. Certificados web**

k) Para garantizar la seguridad de la información en el sitio web, se debe hacer uso de certificados digitales web (SSL/TLS), equivalente o superior:

- Para un dominio, múltiples dominios y subdominios, lo que aplique.

**3.4. Cifrado de datos sensibles cuando se contratan servicios externos.**

l) Para contratar servicios externos que requieran la transmisión de datos confidenciales o sensibles se debe verificar que las trasferencias de datos sean seguras, cifrando los datos antes de transferirlos y utilizando canales seguros.

**3.5. Cifrado de datos sensibles cuando se solicitan desarrollos de aplicaciones.**

m) Todos los aplicativos (web, cliente / servidor o de otro tipo) o app para dispositivos móviles que ofrezca acceso a nuestros usuarios (login), deben considerar que las claves de acceso se almacenen de manera cifrada.

**3.6. Acceso desde el exterior con VPN.**

n) Todo acceso externo autorizado a los servidores de CFN B.P., ya sea por motivo de teletrabajo, soporte técnico, transferencia de información con entidades clientes o entidades del sector público, debe ser habilitado por canales VPN cifrados (equivalente o superior) que garanticen la confidencialidad e integridad de las comunicaciones.

**3.7. Algoritmos de cifrado autorizados.**

o) Para evitar el uso de sistemas de cifrado obsoletos se debe comprobar continuamente que estén vigentes los algoritmos de cifrado que se aplican. Se debe tener en cuenta de forma prioritaria los algoritmos y sistemas de cifrado de carácter abierto y de especificación pública (conocidos y evaluados ampliamente). Se aconseja el uso de sistemas de cifrado asimétrico en detrimento de los sistemas de cifrado simétrico.

**3.8. Cifrado de la wifi de la empresa.**

p) La configuración de la red wifi de CFN B.P. debe contar con un estándar de cifrado, actualmente WPA2, superior o equivalente, cambiando su clave de acceso inicial (default).

## CAPÍTULO XXII: TELETRABAJO

**Artículo 74.- GENERALIDADES DE TELETRABAJO:**

Controlar y evitar que la información clasificada de CFN B.P. se vea comprometida en su integridad, disponibilidad y confidencialidad mientras los empleados y terceros usan o acceden a esta información por medio de la modalidad de teletrabajo.

La presente política debe ser observada y cumplida por todos los funcionarios y colaboradores sean estos empleados directos, externalizados o servicios profesionales, y por entidades externas como proveedores o entidades de control los cuales tengan el acceso a la información y los recursos informáticos que maneja CFN B.P. para el desarrollo de sus actividades, bajo la modalidad de teletrabajo.

En la presente política no se duplican las directrices que CFN B.P. ya ha establecido previamente en otros documentos y resoluciones como el Plan de Teletrabajo institucional.

**Artículo 75.- NORMAS:**

Las siguientes son las normas de control interno que deben cumplirse.

**1. Protección de Equipos Computacionales utilizados para Teletrabajo**

a) La Gerencia de Tecnologías de la Información debe mantener actualizados los antivirus y parches de seguridad establecidos en las computadoras institucionales.

b) Únicamente las computadoras personales de propiedad de los usuarios que sean autorizadas por la Gerencia de Seguridad de la Información pueden ser utilizadas para teletrabajo, previo a una validación por parte de la Gerencia de Tecnologías de la Información en la cual se identifique que cumple con las características mínimas que se definan entre la Gerencia de Seguridad de la Información y la Gerencia de Tecnologías de la Información.

c) La Gerencia de Seguridad de la Información debe considerar el uso de una aplicación de escaneo o monitoreo que resalte los dispositivos con vulnerabilidades conocidas, la existencia de software o firmware obsoleto o la presencia en uso de contraseñas predeterminadas que deberían cambiarse.

d) El propietario o usuario de un dispositivo usado en modalidad de teletrabajo debe asegurar para el equipo un área protegida, libre de riesgos de accesos no autorizados, ambiente climático adecuado, y no expuesto a contingencias como robos, incendios, vandalismo y accidentes.

**2. Directrices de seguridad para los usuarios que trabajan bajo la modalidad de Teletrabajo**

e) Los funcionarios deben garantizar el cumplimiento de las políticas y procedimientos establecidos de seguridad de la información.

f) Proteger y custodiar en sitio seguro cualquier informe, documento, información, base de datos a las que tenga acceso.

g) Con el fin de mantener la confidencialidad de la información, no deben hacer comentario alguno con cualquier persona que no esté relacionada a las actividades laborales, sobre las funciones o actividades que estén ejecutando.
h) No permitir que amigos ni familiares se acerquen a los equipos de trabajo, los cuales deben ser de uso exclusivo del usuario bajo la modalidad de teletrabajo.
i) No se debe compartir el equipo (prestarlo a familiares y/o amigos).
j) Mantener absoluta confidencialidad de toda la información a la que tenga acceso, por lo que no debe extraer física, digitalmente, tomar fotos o mediante cualquier otro medio, tampoco puede compartirla a terceras personas no autorizadas por ningún medio sea físico, digital, auditivo, entre otros. Esto debe cumplirse durante y después de ejecutar sus actividades.
k) Dejar bloqueada la pantalla del computador de trabajo cada vez que no lo estén utilizando.
l) Los funcionarios deben prestar particular atención a la protección de las contraseñas, los documentos e información que cuenten para ejercer sus funciones.
m) Si el usuario identifica algún incidente de seguridad o evento de riesgo debe reportarlo inmediatamente a su jefe inmediato y/o a la Gerencia de Seguridad de la Información.

**3. Gestión de seguridad de la información bajo la modalidad de Teletrabajo**

n) La Gerencia de Seguridad de la Información debe realizar periódicas evaluaciones de los riesgos y los controles, a fin de implementar los controles adicionales para mitigar los riesgos probables bajo la modalidad de teletrabajo.

## CAPÍTULO XXIII: SEGURIDAD DEL ALMACENAMIENTO EN LA NUBE

### Artículo 76.- GENERALIDADES DE LA SEGURIDAD DEL ALMACENAMIENTO EN LA NUBE:

Garantizar la seguridad de la información del almacenamiento en la nube.

Esta política aplica al resguardo de la información de CFN B.P. en la nube.

### Artículo 77.- NORMAS:

Las siguientes son las normas de control interno que deben cumplirse en CFN B.P.

**1. Definición de servicios en la nube**

a) Es la provisión de servicios informáticos accesibles a través del internet, estos pueden ser de infraestructura, plataforma y/o software.
b) Los propietarios de la información, de manera conjunta con la Gerencia de Seguridad de la Información, deben clasificar los servicios que pueden habilitarse en la nube y la información que se requiera cifrar.
c) La Gerencia de Tecnologías de la Información debe analizar la factibilidad de la implementación de los servicios en la nube, bajo la coordinación de la Gerencia de Seguridad de la Información.
d) La Gerencia de Seguridad de la Información es la encargada de informar a los organismos de control, el detalle de los servicios en la nube asociados a los procesos críticos a ser contratados.
e) La Gerencia de Tecnologías de la Información es la encargada de la contratación para la implementación de los servicios en la nube.
f) La Gerencia de Tecnologías de la Información es la encargada del monitoreo de la tecnología para garantizar su correcto funcionamiento, la Gerencia de Seguridad de la Información será la encargada del monitoreo desde la óptica de la disponibilidad, confidencialidad e integridad y Auditoría Interna la responsable de las revisiones desde su ámbito de gestión.
g) La Gerencia de Seguridad de la Información debe gestionar informes de auditorías de seguridad relacionadas con el servicio contratado, con base en el perfil de riesgo del proveedor de servicios en la nube, por lo menos una vez al año, con el fin de identificar amenazas y vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que brindan. Los procedimientos de auditoría deben ser ejecutados por personas o empresas especializadas en seguridad de la información en la nube o empresas especializadas en seguridad de la información en la nube e independiente al proveedor, aplicando estándares vigentes y reconocidos a nivel internacional. El proveedor de servicios en la nube debe definir y ejecutar planes de acción para gestionar las vulnerabilidades detectadas.
h) Los acuerdos o contratos relacionados con servicios en la nube, deben considerar por lo menos: La información no puede ser utilizada para ningún propósito diferente al establecido (inclusive bajo el modelo de subcontrataciones), entrega de informes y certificaciones que demuestren la calidad, desempeño y efectividad en la gestión de los servicios contratados, y borrado seguro de los datos en los medios de almacenamiento cuando finalice el contrato, cuando lo solicite la institución o cuando el proveedor de servicios en la nube elimine y/o reemplace dichos medios.

**2. Consideraciones de seguridad de servicios en la nube**

i) La infraestructura utilizada en la nube, debería ser actualizada incluyendo los parches de seguridad.
j) La autenticación a la nube debe cumplir con la política de contraseñas y el uso de claves fuertes; así como también la opción de un múltiple factor de autenticación.
k) Debe permitir opciones de cifrado en la información o servicios que se requieran.

l) Debe permitir el registro de eventos que permitan un análisis forense en caso que se produzca un incidente de seguridad.
m) Debe tener la posibilidad de emitir Alertas y Reportes de eventos.
n) Debe permitir la Segmentación de Recursos y Accesos.
o) Debe considerar una Política de respaldos.
p) Debe permitir la eliminación de información controlada, es decir con las autorizaciones del caso.
q) Debe considerar temas de disponibilidad que garantice la continuidad de los servicios, en los términos acordados por la Institución.
r) Los centros de procesamiento de datos principal y/o alterno, contratados en la nube deben haber sido implementados siguiendo el estándar TIA-942 o superior y contar como mínimo con la certificación TIER III o su equivalente para diseño, implementación y operación y así garantizar la disponibilidad de los servicios brindados.
s) El proveedor de servicios en la nube debe contar, para los servicios ofertados como mínimo, con certificación ISO 27001 en seguridad de la información, así como la implementación de los controles establecidos en los estándares ISO 27017 (controles de seguridad para servicios en la nube), ISO 27018 (protección de información personal en la nube) y/o aquella que aplique conforme el servicio ofertado.

## CAPÍTULO XXIV: DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

**Artículo 78.- GENERALIDADES DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:**

Gestionar los incidentes de seguridad de la información reportados en la institución con el fin de garantizar una aproximación consistente y efectiva a la gestión de los incidentes de seguridad de la información, incluyendo la comunicación sobre los eventos y debilidades de la seguridad y los protocolos aplicados para minimizar el impacto en las operaciones de CFN B.P.

Esta política aplica para los incidentes de seguridad de la información que:

i. Son reportados por el personal interno y/o externo que colaboran con CFN B.P.
ii. Son gestionados por los responsables de las Unidades Administrativas de CFN B.P.

**Artículo 79.-NORMAS:**

Las siguientes son las normas de control interno que deben cumplirse en CFN B.P.

**1. Reporte de eventos de Seguridad de la Información.**

a) Los usuarios internos y/o externos que presten sus servicios para CFN B.P. deben reportar cualquier evento inusual de seguridad de la información a través de canales oficiales utilizados por la entidad lo más rápido posible.

b) Todos los empleados de CFN B.P., contratistas y usuarios contratados por los proveedores deben tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible.

c) Los funcionarios de la entidad deben notificar incidentes de seguridad directamente a Seguridad de la Información.

d) El Responsable de Seguridad de la Información debe proponer los canales oficiales para reportar los eventos y/o incidentes de seguridad detectados en la CFN B.P.

e) El Responsable de Seguridad de la Información debe instar a los empleados, proveedores y/o terceros que tomen nota e informen acerca de cualquier debilidad que se observe o sospeche con respecto a los sistemas o servicios de seguridad de la información.

**2. Análisis e identificación de incidentes de Seguridad de la Información.**

f) El/La Analista de Seguridad de la Información revisa y analiza los eventos de Seguridad de la Información reportados e identifica los incidentes de Seguridad de la Información.

g) El Responsable de Seguridad de la Información debe aplicar estrategias y/o controles que permitan identificar incidentes de Seguridad de la Información.

h) El/La Analista de Seguridad de la Información debe monitorear los log's de seguridad, alertas tempranas de aplicaciones de negocio y/o herramientas, y realizar análisis de vulnerabilidades en componente de infraestructura según los procedimientos de seguridad establecidos en la institución con el fin de detectar incidentes de seguridad de la información proactivamente.

**3. Registro de incidentes de Seguridad de la información.**

i) El/La Analista de Seguridad de la Información registra los incidentes de seguridad de la información en la herramienta implementada por la Gerencia de Tecnologías de la Información para el efecto; en el registro se debe incluir fecha, hora, nombres y apellidos del funcionario que registró el incidente, persona que reporta el

incidente en caso que aplique, departamento o Unidad Administrada afectada, equipo o sistema o servicio afectado y breve descripción del incidente.

j) El/La Analista de Seguridad de la Información debe registrar de manera oportuna los incidentes de seguridad de la información reportados por los usuarios de CFN B.P.

**4. Evaluación de incidentes de Seguridad de la Información.**

k) El/La Analista de Seguridad de la Información evalúa los incidentes de seguridad y los clasifica de acuerdo al tipo de servicio afectado y al nivel de severidad.

l) El/La Analista de Seguridad de la Información asigna una prioridad de atención al incidente en el caso de que se produjeran varios de manera simultánea.

m) El/La Analista de Seguridad de la Información realiza un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar la causa raíz y/o posibles causas.

**5. Tratamiento y respuesta a incidentes de Seguridad de la Información.**

n) El/La Analista de Seguridad de la Información debe escalar el incidente en caso de que no pueda solucionarlo, el escalamiento debe ser registrado en la herramienta implementada por la Gerencia de Tecnologías de la Información para el efecto.

o) En caso de que no se pueda solucionar un incidente, en conjunto con el/la Gerente de Seguridad de la Información, deben solicitar soporte a la Unidad Administrativa administradora del contrato o responsable del servicio afectado.

p) El/La Analista de Seguridad de la Información debe investigar y diagnosticar las causas por las cuales se produjo el incidente de seguridad de la información en CFN B.P.

q) El/La Analista de Seguridad de la Información debe usar el conocimiento obtenido del análisis y resolución de incidentes de seguridad de la información anteriores con la finalidad de reducir la probabilidad o impacto de futuros incidentes.

r) En el caso que el incidente esté relacionado con un servicio de la Gerencia de Tecnologías de la Información, el/la Gerente de Seguridad de la Información debe asegurar con el Responsable en la Gerencia de Tecnologías de la Información la restauración del servicio afectado por el incidente de seguridad de la información. El responsable de atender el incidente en la Gerencia de Tecnologías de la información debe registrar en la mesa de servicios de TI el incidente con toda la información necesaria (entre ella, número, prioridad, diagnóstico, detalle de la solución). La Gerencia de Tecnologías de la Información debe presentar trimestralmente un informe de Gestión de Incidentes, por lo menos aquellos que en la mesa de servicios de TI se los haya categorizado como “Críticos” o “Altos”, en el cual se detallen las solicitudes atendidas en el período, la gestión realizada para los incidentes repetitivos, los incidentes que se convirtieron en problemas, recomendaciones para que se eviten incidentes futuros por las mismas causas, etc. Además se debe anexar el listado de incidentes mínimo con la siguiente información: Número de incidente, Fecha y Hora de registro, solicitante, Unidad Administrativa, Detalle del Incidente, Estado, Nombre de la persona que resolvió, Diagnóstico Inicial, Solución aplicada, Fecha de solución.

s) El/La Analista de Seguridad de la Información debe cerrar el incidente de seguridad de la información, actualizando el estado de registro del incidente en la herramienta implementada por la Gerencia de Tecnologías de la Información para el efecto como estado “resuelto”.

t) El/La Analista de Seguridad de la Información debe notificar y confirmar con el responsable del equipo o del sistema de que el incidente de seguridad de la información reportado ha sido resuelto.

u) El/La Gerente de Seguridad de la Información debe proponer un Plan de Seguridad de la Información al Comité de Administración de Seguridad de la Información con un tratamiento a los riesgos más relevantes relacionados con la gestión de incidentes de Seguridad de la Información, la propuesta puede contener:

- Nuevos requerimientos de seguridad de la información para mitigar los riesgos;
- Controles específicos, nuevos y/o mínimos;
- Eliminación de controles obsoletos o redundantes; y,
- Reforzamiento a controles existentes rescatables para la evaluación y aprobación respectiva.
- Mejora en los procedimientos para el manejo de incidentes de seguridad de la información.

**6. Comunicación de incidentes de Seguridad de la Información.**

v) El/La Gerente de Seguridad de la Información debe presentar informes, notificación e investigaciones realizadas sobre los incidentes y/o violaciones de seguridad de la información presentados en CFN B.P.

w) EL/La Gerente de Seguridad de la Información debe comunicar de manera periódica al Comité de Administración de Seguridad de la Información los incidentes de seguridad de la información con el fin de tomar las acciones pertinentes para que se resuelvan dichos incidentes.

x) El/La Gerente de Seguridad de la Información debe comunicar los incidentes de seguridad de la información de acuerdo a los procedimientos establecidos en CFN B.P.

**7. Monitoreo de incidentes de Seguridad de la Información.**

y) El/La Analista de Seguridad de la Información revisa y monitorea los incidentes de seguridad de la información de la CFN B.P.

z) El/La Analista de Seguridad de la Información debe proponer controles que ayuden a efectuar un monitoreo eficaz de los incidentes de seguridad de la información.

aa) El/La Gerente de Seguridad de la Información debe establecer mecanismos que permitan dar seguimiento a los diferentes tipos de incidentes de seguridad de información de CFN B.P.

## CAPÍTULO XXV: DEL INTERCAMBIO DE INFORMACIÓN INTERNA Y CON TERCEROS

**Artículo 80.- GENERALIDADES DEL INTERCAMBIO DE INFORMACIÓN INTERNA Y CON TERCEROS:**

a) Las partes interesadas con las que se intercambia información son principalmente: funcionarios, contratistas, proveedores, entidades de control gubernamental, clientes, medios de prensa, otras instituciones públicas relacionadas, entidades del sistema judicial.

b) Continuamente se deben definir, actualizar, y establecer procedimientos específicos de intercambio de información segura con las diferentes partes interesadas, que hacen parte de la operación de CFN B.P., teniendo en cuenta la utilización de medios de transmisión confiables y la adopción de controles y herramientas seguras.

c) No está permitido el intercambio de información no pública de CFN B.P., por medio telefónico, mensajería inmediata o por correo electrónico, sin la debida protección y controles necesarios que la ameritan por su nivel de clasificación.

d) Las partes interesadas deben evitar tener conversaciones confidenciales sobre información de la entidad en lugares públicos, oficinas abiertas, ascensores, escaleras, video-llamadas, redes sociales, teleconferencias, y lugares de reunión social para evitar la escucha, grabación, o interceptación de información no autorizada.

e) En cuanto a la información tipo verbal que no es de uso público, se debe tener reserva y solo comentarla en áreas o zonas seguras dentro de la entidad.

f) Quien está intercambiando información no pública debe confirmar que cuenta con la autorización expresa del titular del dato o su representante para ese tratamiento.

g) No se permite el intercambio de información por medios no autorizados por CFN B.P.
h) CFN B.P. firma un compromiso de confidencialidad con los servidores públicos y con terceros (contratistas y proveedores) que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información no pública de la entidad. En este compromiso quedan especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se firman antes de permitir el acceso o uso de dicha información. Los acuerdos de confidencialidad deben garantizar la protección de la información durante y posterior al tiempo de ejecución de las labores encomendadas.
i) La información con datos personales, recibida de cualquier parte interesada, debe protegerse en CFN B.P., conforme a lo indicado en la Ley de Protección de Datos Personales (LPDP).

**Artículo 81.- NORMAS:**

**INTERCAMBIO DE INFORMACIÓN ENTRE PERSONAL DE CFN B.P.:**

j) Se puede realizar intercambio de información de CFN B.P. entre su personal cuando dicho intercambio corresponda a actividades relacionadas con el desarrollo de sus labores.
k) Siempre que se realice intercambio de información que no está clasificada como pública o de uso interno, dicho intercambio debe ser aprobado por el jefe directo.
l) CFN B.P. favorece el uso de carpetas compartidas en lugar de medios removibles (USB, discos externos, teléfonos inteligentes, tabletas, entre otros) para el intercambio de información al interior de la entidad.

**INTERCAMBIO DE INFORMACIÓN CON TERCEROS:**

m) Se deben regular formalmente los intercambios de información con terceros, comunicando los requisitos al personal de la organización y a todos los terceros involucrados en dichos intercambios.
n) Todo intercambio de información electrónica con terceros debe ser respaldado con un acuerdo (convenio o contrato o acuerdo formalizado), determinando en ellos los medios y controles en el tratamiento de la información, e incluyendo una cláusula de confidencialidad y no divulgación de la información proporcionada. Entre los aspectos más importantes se consideran los siguientes:

- Responsabilidades y procedimientos para controlar la transmisión y recepción de información.
- Procedimientos para garantizar la trazabilidad y no repudio.
- Responsabilidades en caso de incidentes de seguridad de la información.
- Políticas, procedimientos y normas para proteger la información y los medios contenedores.
- Prohibición de divulgar la información entregada.
- Destrucción segura de la información una vez cumpla el objeto del contrato.

o) La información recibida de otra entidad o persona se debe salvaguardar a un nivel igual o mayor que el aplicado por la entidad que originó el documento.
p) La solicitud de intercambio de información puede iniciarse por requerimientos de CFN B.P., del organismo externo o incluso de un tercero que, ante disposiciones legales o directrices del gobierno hacen necesaria dicha interoperabilidad.
q) El intercambio de información digital que no esté clasificado como de uso público o de uso interno debe realizarse por canales cifrados que garanticen la protección de la confidencialidad de la información y que cumpla con la política respectiva de controles criptográficos, esto debe quedar registrado en los convenios o acuerdos de intercambio de información que firmen las partes.
r) Cualquier excepción en la entrega de información debe estar regida por lo establecido según legislación y normativa interna vigente.

s) Cuando por necesidades institucionales se requiera intercambiar información con otras organizaciones, sean gubernamentales, privadas o proveedores, el responsable del intercambio debe asegurar la confidencialidad e integridad de la información.
t) El intercambio de información con organismos de control y autoridades de supervisión se rige por las directrices de dichos entes externos para el intercambio de información, tales como, uso de aplicaciones específicas, tokens, certificados o firmas digitales.

**INTERCAMBIO DE INFORMACIÓN FÍSICA:**

u) El intercambio de información que se encuentre en formatos físicos debe estar debidamente etiquetada con respecto a su clasificación, en caso de que no sea clasificada como de uso público, el intercambio debe realizarse en un sobre sellado para ser enviada a terceros.
v) Para el transporte de información (no de uso público) en medios físicos, se debe generar una bitácora de entrega de estos medios y recepción de estos. Se debe transportar en un dispositivo con un sello de seguridad que garantice que en su desplazamiento no ha sido intervenido por un tercero.
w) Para la apertura de ese sello se debe generar un registro y garantizar que no se reutilice el sello.
x) Se deben transportar estos medios en un recipiente que proteja al activo de información de amenazas ambientales.

**INTERCAMBIO DE INFORMACIÓN VÍA CORREO ELECTRÓNICO INSTITUCIONAL:**

y) Los mensajes de correo electrónico que salieren de CFN B.P. deben contener una nota adjunta de descargo que oriente el manejo de la información enviada por este medio.
z) Toda información enviada desde CFN B.P. a través de correos electrónicos debe incluir en su pie de página la siguiente advertencia (o equivalente):
Este mensaje (y cualquier archivo que se adjunte) es confidencial y podría contener información clasificada y reservada de CFN B.P., para el uso exclusivo de su destinatario. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje es prohibida y sancionada por la ley. Si por error recibe este mensaje, por favor reenviarlo al remitente y borre el mensaje recibido inmediatamente.

aa) La Gerencia de Tecnologías de la Información debe asegurar la confidencialidad e integridad en el envío y recepción de mensajes de correo electrónico, para lo cual debe aplicar los mecanismos de seguridad que correspondan.

**DEL TRATAMIENTO PARA PROTEGER EL INTERCAMBIO DE INFORMACIÓN:**

bb) La Gerencia de Tecnologías de la Información, debe hacer las implementaciones tecnológicas necesarias, bajo la coordinación de la Gerencia de Seguridad de la Información, de tal manera de garantizar el cumplimiento de las políticas “DEL INTERCAMBIO DE INFORMACIÓN INTERNA Y CON TERCEROS”.
cc) En el caso de herramientas o servicios disponibles, la Gerencia de Tecnologías de la Información debe mantener activa la protección, estableciendo los protocolos adecuados para la administración continua y permanente, para lo cual debe coordinar el procedimiento conveniente con la Gerencia de Seguridad de la Información.
dd) La Gerencia de Tecnologías de la Información debe proceder a tramitar la adquisición o contratación, lo que aplique, para las herramientas o servicios no disponibles en CFN B.P., que son necesarias para cumplir con los requerimientos de la protección del intercambio de Información.

**MONITOREO SOBRE CUMPLIMIENTO:**

ee) La Gerencia de Seguridad de la Información debe monitorear periódicamente si las partes interesadas y los proveedores críticos de la entidad están cumplimiento con: los acuerdos de niveles de servicio sobre intercambio de información y seguridad, los acuerdos de confidencialidad, los acuerdos de intercambio de información, procedimientos de entrega o eliminación de la información, gestión de riesgos y los compromisos de Seguridad de la Información, exigiendo que se cumplan sin excepción.

## CAPÍTULO XXVI: DE LA GESTIÓN DE ACTIVOS DE INFORMACIÓN Y SU USO ACEPTABLE

**Artículo 82.- GENERALIDADES DE LA GESTIÓN DE ACTIVOS DE INFORMACIÓN:**

a) La Gerencia General debe mantener una adecuada protección de los activos de información de la Institución, para lo cual debe designar propietarios de la información, de los cuales se exige la debida rendición de cuentas por el mantenimiento de los controles apropiados.

b) La designación de los propietarios de la información se la debe realizar con una periodicidad de 12 meses o cuando lo amerite (especialmente cuando exista alta rotación del personal asignado como propietario de la información).

c) Todo activo de información debe tener un propietario, quien es responsable de identificar claramente el valor relativo e importancia del activo, y definir el grado de confidencialidad y el nivel de criticidad considerando las características de integridad y disponibilidad; así como, identificar los riesgos a los que pueden estar expuestos los activos de información.

d) Todo activo que se encuentre en formato electrónico y que resida en los equipos del centro de cómputo está bajo la responsabilidad de la Gerencia de Tecnologías de la Información quien aplica las medidas de seguridad necesarias para mantener, controlar y resguardar dichos activos.

e) Todo activo que se encuentre en formato electrónico y que resida en los equipos asignados a cada funcionario, es responsabilidad del mismo aplicar las medidas de seguridad necesarias en base al mecanismo definido por la Gerencia de Tecnologías de la Información.

f) La Gerencia de Seguridad de la Información es responsable del control y actualización (mantenimiento) del inventario de los activos de información.

g) La información debe ser clasificada basándose principalmente en términos de su valor, analizando los perjuicios que pudiera ocasionarle a la Corporación Financiera Nacional B.P. y/o su personal la manipulación o mal uso de la información. Dichos perjuicios pueden ser económicos, financieros, políticos, sociales, de imagen, legales, operativos, entre otros no especificados. Para la clasificación se debe tener en cuenta las definiciones de las autoridades de la Institución y las leyes y reglamentaciones vigentes.

**Artículo 83.- NORMAS (Gestión de Activos de Información)**

**Responsabilidad sobre los Activos (Inventario y Propiedad):**

h) La Gerencia General o su delegado designa los propietarios de la información, considerando a los titulares de las unidades administrativas como candidatos ideales para dicha designación.

i) Los propietarios de la información, deben clasificar los riesgos y grado de exposición (amenaza y vulnerabilidad) al que pueden estar expuestos dichos activos, a fin de protegerlos y custodiarlos adecuadamente.

j) Para la clasificación de los activos se debe evaluar las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

k) La clasificación de la información y el grado de confidencialidad y reserva debe ser socializada a nivel nacional para que los funcionarios conozcan los cuidados y formas del manejo de información.

l) Los procesos de definición, actualización y socialización de las políticas y procedimientos para la administración, custodia y conservación de los activos de información (archivos físicos o digitales) a nivel nacional; así como, implementación del proceso de etiquetado de los activos, son de responsabilidad de Secretaría General; procesos que deben efectuarse al menos cada 12 meses.

**Clasificación de la Información (Criterios y Etiquetado):**

m) Para clasificar un Activo de Información, se evalúan las características de confidencialidad, integridad y disponibilidad como se detalla a continuación:

***Confidencialidad:***

- Baja: Información de tipo pública, disponible para todos en general.
- Media: Información que puede ser conocida y utilizada por los funcionarios de la Institución al interior de la misma.
- Alta: Información que no puede ser divulgada, es de conocimiento limitado a las personas del manejo de la misma, considerada como reservada o confidencial.

***Integridad:***

- Baja: Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatividad de la CFN B.P.
- Media: Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para la CFN B.P., el Sector Público Nacional o terceros.
- Alta: Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas o graves para la Institución o terceros.

***Disponibilidad:***

- Baja: Información cuya inaccesibilidad no afecta la operatividad.
- Media: Información cuya inaccesibilidad durante 1 día podría ocasionar pérdidas materiales, de imagen, de valor estratégico de la información, de obligaciones contractuales o públicas, de disposiciones legales, etc. significativas para la Institución o terceros.
- Alta: Información cuya inaccesibilidad durante 4 horas podría ocasionar pérdidas significativas o graves a la Institución o a terceros.

n) Para el etiquetado, se asigna a la información un valor por cada uno de estos criterios. Luego, se clasifica la información en una de las siguientes categorías:

- Información Pública – Criticidad Baja: ninguno de los valores asignados superan el 1.
- Información de Uso Interno – Criticidad Media: alguno de los valores asignados es 2.
- Información Reservada o Confidencial – Criticidad Alta: alguno de los valores asignados es 3.

Únicamente la información pública puede ser transmitida al exterior de la CFN B.P., no requiere previa autorización, todas las demás, requieren autorización previa para su divulgación al exterior.

o) Solo el propietario de la información puede asignar o cambiar un nivel de clasificación.

**Artículo 84.- GENERALIDADES DEL USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN:**

Define las directrices y el marco general para el uso aceptable de los activos de información y recursos informáticos, que garantizan la confidencialidad, integridad y disponibilidad la información contenida en dichos activos y recursos distribuidos en las oficinas de CFN B.P.

La presente política debe ser observada y cumplida por todos los funcionarios y colaboradores sean estos empleados directos, externalizados o servicios profesionales, y por entidades externas como proveedores o entidades de control los cuales tengan acceso a la información que maneja CFN B.P.

Para la aplicación de la política se toman en cuenta a los siguientes recursos informáticos:

- Activos de Información: información contenida en bases de datos y archivos físicos o electrónicos, presentaciones grabadas, manuales técnicos y de usuario de aplicativos y sistemas, formularios o informes con datos de clientes, material de capacitación, políticas y procedimientos de soporte, planes de continuidad.
- Activos de Software: software propio de CFN B.P. o desarrollado por terceros, herramientas de desarrollo, herramientas de ofimática, utilitarios y licencias de los mismos.
- Activos tecnológicos: equipamiento informático (servidores, sistemas de respaldo y almacenamiento, computadoras de escritorio y portátiles, impresoras, ups), equipos de comunicaciones (firewalls, ips, ruteadores, switches, módems, centrales telefónicas, máquinas de fax, teléfonos), medios magnéticos (cintas y discos internos y externos). componente configurable, software, firmware o hardware que forme parte del sistema o subsistema
- Servicios Informáticos: Internet, Correo Electrónico, contratos de prestación de servicios tecnológicos y comunicaciones (outsourcing), contratos de soporte y mantenimiento de hardware, ups, plantas eléctricas, cableado estructurado, aire acondicionado, cada subsistema interconectado o no conectado usado para la adquisición, almacenamiento, manipulación, gestión, movimiento, control, despliegue, conmutación, intercambio, transmisión o recepción de voz, datos, vídeo en formas análogas o digitales.

**Artículo 85.- NORMAS (Uso Aceptable de los Activos de Información):**

**Uso aceptable de los activos (recursos) informáticos**

- Los recursos que provee CFN B.P. deben exclusivamente ser utilizados para propósitos laborales y para actividades autorizadas por el Superior Jerárquico. El uso aceptable de los recursos informáticos está regido por todas las políticas aplicables de la Institución, incluyendo, pero no limitándose, a derechos de propiedad intelectual (copyright) y políticas disciplinarias de los colaboradores, así como leyes locales aplicables.

- Los funcionarios y colaboradores pueden aprovechar en forma limitada los servicios y activos tecnológicos para un uso personal que derive en su mejor capacitación, jerarquización y/o especialización en sus conocimientos y destrezas en temas afines al campo donde desempeñan sus actividades dentro de CFN B.P., considerándose estas actividades como uso aceptable de los recursos informáticos.

- El uso aceptable no puede interferir con las actividades laborales propias o las de otros funcionarios o colaboradores, ni con la consecución de los objetivos institucionales ni los propios de la Unidad Administrativa para la que trabaja, por lo tanto se puede aplicar el uso aceptable siempre y cuando el recurso se encuentre disponible y no exista otro usuario que precise emplear el recurso para el desarrollo de sus tareas laborales.

- El uso aceptable implica evitar violaciones de los derechos de propiedad (copyright) de cualquier persona o empresa protegida por derechos de autor, secretos industriales, patentes u otra propiedad intelectual, o leyes o reglamentos similares.

- El uso aceptable no se considera un derecho del funcionario o colaborador y se encuentra sujeto al estricto control de la línea de supervisión donde desempeña sus funciones, por lo tanto es controlado, y puede ser revocado o limitado en cualquier momento por razón de la función, por cuestiones operativas y/o de seguridad de la Red.

- CFN B.P. se reserva el derecho a monitorear el acceso a los servicios de Correo Electrónico e Internet para garantizar el uso aceptable de estos recursos y para disponer de registros de conexión que permitan posterior análisis, con lo cual se puede determinar parámetros de uso adecuados.

**Uso NO aceptable de los activos (recursos) informáticos**

- CFN B.P. califica el uso indebido sobre los recursos informáticos como no ético e inaceptable, y las siguientes actividades se consideran no aceptables:

    - Hacer uso para beneficio exclusivo propio, o para implementación de negocios personales.

    - Dañar o esconder cualquier activo de información.

    - Eliminar cualquier activo de información sin la previa autorización o delegación, o sin seguir la normatividad de los organismos de control para períodos de conservación y procedimientos de descarte de información.

    - Intentar descifrar las claves / contraseñas, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos.

    - Revelar la contraseña de su cuenta a otros o permitir el uso de su cuenta por parte de otros, lo que incluye a la familia y otros miembros del hogar cuando se trabaja en casa.

    - Violar cualquier ley local vigente y aplicable, orientada a la tecnología de información o delitos informáticos.

- Se prohíbe el uso indebido de los Activos Tecnológicos que incluye entre otras, las siguientes acciones:

    - Modificar la configuración básica, estándar, de los equipos de procesamiento.

    - Sobrepasar (evitar) o pretender traspasar los límites autorizados para el uso del recurso, como por ejemplo procedimientos de conexión y regulaciones de seguridad.

    - Eliminar, destruir, retirar o desinstalar software, impresiones o medios magnéticos sin el explícito permiso del autorizador correspondiente.

    - Apoderarse del uso del recurso tecnológico de otro colaborador, interrumpiendo sus actividades por el uso de video juegos, envío de cadenas de correos electrónicos o cantidad excesiva de mensajes, tanto local como externa; impresión excesiva de documentos, archivos, información o programas; modificación de facilidades de los sistemas, sistemas operativos, o partición de discos; pretender sobrecargar computadoras o redes, o dañar computadoras o redes, equipos, software o archivos de las computadoras.

- Instalar dispositivos de almacenamiento o periféricos, en los computadores, que no sean autorizados y de propiedad de CFN B.P.

- Ingresar sin autorización a las áreas restringidas (áreas seguras) donde se encuentran los recursos o activos informáticos/tecnológicos que procesan información.

- Conectar computadores personales propiedad de funcionarios, colaboradores, entes externos, a la red de datos de CFN B.P. sin la debida autorización del superior jerárquico de la Unidad Administrativa.

- Se prohíbe el uso indebido de los Activos de Software que incluye entre otras, las siguientes acciones:

  - Violar cualquier licencia o copyright de un software, incluyendo las copias o la distribución no autorizada de software con licencia, información o reportes, sin la autorización apropiada documentada.

  - La copia no autorizada de material con derechos de autor que incluye, entre otros, la digitalización y distribución de fotografías de revistas, libros u otras fuentes con derechos de autor, música con derechos de autor y la instalación de cualquier software con derechos de autor para lo cual CFN B.P. o el usuario final no tienen una licencia activa.

  - Instalar software no autorizado o no licenciado en los computadores de CFN B.P. Toda instalación de software autorizado debe ser realizado exclusivamente por el personal técnico destinado para estos propósitos. La autorización debe provenir de la Gerencia de Tecnologías de la Información y de la Gerencia de Seguridad de la Información.

  - El acceso a los sistemas debe advertir a los usuarios que se está ingresando a un sistema privado que es propiedad o esta licenciado para CFN B.P., el cual es monitoreado y no permite el acceso no autorizado, dicho mensaje debe aparecer antes del inicio de sesión, la aceptación de este mensaje por parte del usuario da por entendido que acepta las condiciones del uso aceptable del recurso informático definidas en esta política y de la política de control de accesos y uso de contraseñas de CFNB.P.

- Se prohíbe el uso indebido de los Servicios Informáticos que incluye entre otras, las siguientes acciones:

  - Colocar información que no tenga que ver con el trabajo en los directorios compartidos, de respaldo o en cualquier medio de almacenamiento de CFN B.P.

  - Ejecutar programas de escaneo de puertos, uso de técnicas de enumeración, obtención de información interna de la configuración de la red, ataques de negación de servicio (DoS), obtención de contraseñas vía ataques de fuerza bruta, entre otros.

  - Conectar equipos eléctricos externos a la red de UPS ya que dicha red es de uso exclusivo de los recursos informáticos de CFN B.P.

  - Desperdiciar energía eléctrica generada por el mal uso de luces, equipos eléctricos, equipos electrónicos y electromecánicos.

  - Contradecir e incumplir las observaciones de seguridad y mantenimiento al conectar equipos con cables, extensiones y otros dispositivos no apropiados o defectuosos que puedan generar cortocircuitos en la red eléctrica.

  - Instalar equipos en las áreas de procesamiento que disponen de aire acondicionado, sin el debido análisis de capacidad de los sistemas de aire acondicionado y eléctrico.

  - Desactivar premeditadamente cualquier sensor que permita detectar anomalías en los sistemas de enfriamiento, incendio, seguridad, eléctrico o electrónico.

**Uso aceptable del correo electrónico institucional**

- Los colaboradores deben usar el correo electrónico para mensajes relacionados con el trabajo y asegurarse que no interfieren con su productividad.
- Ejecutar el programa antivirus sobre cualquier archivo recibido de fuentes externas.
- Evitar transmitir información confidencial de clientes, empleados, proveedores, accionistas. Si es necesario transmitir información confidencial, se debe tomar las acciones necesarias para asegurar que sea correctamente recibida y usada de acuerdo con la ley.
- La Gerencia de Seguridad de la Información puede limitar el envío de mensajes a grupos de distribución grandes, considerando personal autorizado o tamaño de mensaje.
- Es responsabilidad del usuario depurar su buzón de correo electrónico, eliminando los mensajes innecesarios y archivando los correos electrónicos de forma local a su computador personal para liberar el espacio del buzón de correo electrónico en el servidor.
- Cada usuario es responsable de eliminar todo mensaje cuyo origen sea desconocido, o que contengan textos extraños; por tanto las consecuencias que pueda ocasionar la ejecución de cualquier archivo adjunto de origen desconocido son de absoluta responsabilidad del usuario. Si se reciben mensajes de origen desconocido se debe enviar una copia a la Gerencia de Seguridad de la Información para, a través del Oficial de Seguridad de la Información efectuar y/o coordinar las tareas de seguimiento e investigación necesarias; o eliminar el mensaje en forma inmediata sin abrirlo.
- El tamaño máximo para el buzón de correo electrónico así como para los mensajes de entrada y salida son definidos formalmente por la Gerencia de Tecnologías de la Información, en coordinación con la Gerencia de Seguridad de la Información, como parte del plan de capacidad, el mismo que debe prever los recursos tecnológicos y las necesidades de los usuarios.
- La Gerencia de Seguridad de la Información puede, en cualquier momento, cancelar o inhabilitar la cuenta de cualquier usuario sin previo aviso e incluso eliminar ésta si se considera que el usuario ha cometido una falta grave en el uso del correo electrónico que expone a CFN B.P.
- La Gerencia de Tecnologías de la Información debe mantener el respaldo de la información contenida en las cuentas de correo electrónico, de acuerdo al procedimiento establecido para el efecto
- Toda cuenta de correo electrónico está restringida a una única cuenta de usuario.
- El correo electrónico institucional debe contar con las facilidades automáticas que notifiquen al usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo el motivo del error.
- Debe utilizarse programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución.
- Para el envío y la conservación de la información catalogada como sensible o crítica para la institución, la Gerencia de Tecnologías de la Información debe aplicar los mecanismos correspondientes con la finalidad de que garantice la seguridad y el envío de los datos.
- Para asuntos legales el contenido de los mensajes es responsabilidad del propietario de la cuenta de correo.
- El funcionario que distribuya información de manera ilegal está sujeto a las penas que contempla el Código Orgánico Integral Penal COIP en lo relacionado a la revelación ilegal de base de datos.

**Uso NO aceptable del correo electrónico institucional**

- Se prohíbe el uso indebido del correo electrónico institucional que incluye entre otras, las siguientes acciones:

  - Utilizar el correo electrónico o Internet para asuntos que no tengan que ver con la administración y operaciones de CFN B.P. y que vayan en contra de las políticas de uso aceptable.

  - Utilizar otros sistemas de correo electrónico no autorizados dentro de las redes de comunicación de CFN B.P. para enviar información de CFN B.P.

  - Enviar información confidencial de CFN B.P. por correo sin las respectivas seguridades de cifrado.

  - Transmitir materiales sujetos a leyes de derechos de autor y propiedad intelectual, sin el permiso expreso del autor.

  - Usar recursos informáticos de CFN B.P. para el desarrollo, envío o transmisión de: avisos comerciales o personales, promociones, programas destructivos, material político o religioso, mensajes fraudulentos, ofensivos, acosadores, obscenos, indecentes, intimidatorios, profanos, discriminadores, sexuales, etc. u otro uso no autorizado o personal y que vayan en contra de las leyes locales.

  - Enviar correos electrónicos fraudulentos, cadenas, ofertas, mensajes de multidifusión, entrar a buzones de correo ajenos, o leer correos de otros usuarios sin la autorización correspondiente.

  - Crear y enviar mensajes a nombre de otro funcionario.

  - Abrir correos electrónicos de remitentes desconocidos o extraños que puedan causar la infección con cualquier tipo de malware a la red corporativa de CFN B.P. Tener especial cuidado cuando dichos correos vienen con archivos ejecutables con extensiones como exe, .com, .pif, .dll, .vbs, .bat, etc.

  - Acceder a Sitios Web ilegales o que atenten contra la moral y el ambiente controlado de trabajo como pornográficos, música, juegos, violencia, drogas, terrorismo, sitios donde se hace apología de delitos, etc.

  - Descargar archivos, fotos, videos que no tengan que ver con el desarrollo de las actividades autorizadas en CFN B.P.; la descarga e instalación de programas desde Internet está completamente prohibido.

**Uso aceptable del Internet**

- Utilizar navegadores de Web para obtener información laboral disponible en sitios Web orientados hacia empresas.

- Acceder a bases de datos para buscar información laboral, de clientes, de proveedores, de entidades gubernamentales, etc.

- Acceder a sitios y grupos de profesionales en internet para obtener contenido y noticias que beneficien a CFN B.P. Las opiniones personales de los empleados (usando la dirección de correo de la empresa) en los grupos de noticias y debates deben contener un descargo de responsabilidad que indique que las opiniones expresadas son estrictamente propias y no necesariamente las de CFN B.P.

- Responsabilizarse del contenido de todo el texto, audio, o imágenes que coloque o envíe a través de la Internet, así como de la información y contenidos a los que accede y de aquella que copia para conservación.

- La Gerencia de Seguridad de la Información realiza monitoreos de los accesos al internet por parte de los funcionarios, así mismo conserva de forma permanente los reportes que evidencien dichos accesos. El Oficial de Seguridad de la Información, puede acceder a los contenidos monitoreados, con el fin de asegurar el cumplimiento de las medidas de seguridad. En el caso que la Gerencia de Tecnologías de la Información

identifique anomalías con el acceso al internet por parte de los usuarios, deben comunicarlo a la Gerencia de Seguridad de la Información.

- La Gerencia de Tecnologías de la Información debe implementar mecanismos para limitar el accesos a descargas de archivos, para que la Gerencia de Seguridad de la Información, revise y lo controle, e informa los incumplimientos al jefe inmediato del funcionario, quien en aplicación de la Política de Seguridad de la Información debe motivar el hecho y remitir toda la documentación a la Gerencia de Talento Humano para la aplicación de las acciones que correspondan.

- La Gerencia de Seguridad de la Información puede en cualquier momento bloquear o limitar el acceso y uso de la Internet a los funcionarios o a terceros que accedan tanto por medio alámbrico como inalámbrico.

- La Gerencia de Seguridad de la Información mediante el Oficial de Seguridad de la Información debe establecer categorías para navegación a internet considerando las funciones de competencia y desempeño de los funcionarios de las diferentes Unidades Administrativas de la institución. La Gerencia de Tecnologías de la Información debe implementar los mecanismos que permitan el establecimiento de categorías de navegación.

- El acceso a servicios de correo electrónico de libre uso, mensajería instantánea, almacenamiento de datos y redes sociales, entre otros, debe ser restringido, exceptuándose los usuarios que se encuentren en las categorías que por sus funciones es permitido y que son autorizados previamente por la Gerencia de Seguridad de la Información.

**Uso NO aceptable del Internet**

- Se prohíbe el uso indebido del Internet que incluye entre otras, las siguientes acciones:
  - Uso para propósitos ilegales, inmorales, perjudiciales a la institución o improductivos.
  - Para implementar negocios personales por medio de recursos de la institución.
  - Acceder a cualquier tipo de mensajes que contengan información ofensiva, fraudulenta o sexual.
  - Para participar en redes sociales con fines de entretenimiento, diversión o actividades personales.
  - Para asuntos que no sean relativos a las funciones desempeñadas en el cargo.
  - Para acceder y utilizar servicios de correo electrónico en la Internet (Nube), con empresas privadas o públicas cuyos centro de datos, redes (salvo Internet), equipos software base y de gestión de correo electrónico y cualquier elemento tecnológico necesario, se encuentren fuera del territorio nacional; y adicionalmente, si las condiciones de los servicios que tales empresas prestaren no se someten a la Constitución y leyes ecuatorianas. Si algún usuario necesita la utilización de estos servicios de manera excepcional, deben ser autorizados por la Gerencia de Seguridad de la Información.
  - Para utilizar cualquier sistema de mensajería instantánea, charlas en línea o video chat y otros sistemas para compartir archivos de CFN B.P. Si algún usuario necesita la utilización de estos servicios de manera excepcional, deben ser autorizados por la Gerencia de Seguridad de la Información.

**Uso aceptable de los sistemas de video-conferencia (o teleconferencia)**

- El uso de los sistemas de videoconferencia es aplicable para permitir la conexión simultánea en tiempo real por medio de audio/video para intercambiar información de forma interactiva entre funcionarios, proveedores, entidades de la administración pública, entre otros que se encuentren distantes o en teletrabajo, y requieran establecer una comunicación para propósitos laborales, teniéndose en consideración los siguientes aspectos para su aplicación:

- Cada Unidad Administrativa que tenga asignado el servicio de una sala de video conferencia es la responsable de autorizar el uso de la misma y se encarga de verificar que al término de su uso se encuentre en las mismas condiciones previo a su préstamo, de tal forma que pueda garantizar la integridad de los equipos institucionales.

- La Gerencia de Tecnologías de la Información es responsable de instalar, configurar, administrar y dar el debido mantenimiento para que los servicios de video conferencia de las diferentes Unidades Administrativas de la Institución funcionen de forma adecuada durante la comunicación a establecerse, así mismo deben implementar los mecanismos necesarios para establecer videoconferencias seguras mediante sesiones virtuales y de punto a punto.

- La Gerencia de Tecnologías de la Información debe garantizar que la respuesta automática de los equipos del sistema de video-conferencia estén deshabilitadas.

- Para el servicio de video conferencia con entidades externas la Gerencia de Tecnologías de la Información debe acoger las medidas de seguridad establecidas por las mismas; mientras que para el servicio de video conferencia inter institucional, debe garantizar que no existan riesgos en la comunicación a mantenerse.

**Uso NO aceptable de los sistemas de video-conferencia (o teleconferencia)**

- Se considera falta grave:

  - Divulgar hacia a fuera de la institución la información clasificada como “de uso interno” o “reservada o confidencial.

  - Hacer uso de los activos de información, para beneficio propio o implementación de negocios personales.

  - Dañar o esconder cualquier activo de información.

  - Eliminar cualquier activo de información sin la previa autorización del propietario de la información o sin seguir la normatividad de los organismos de control para períodos de conservación y procedimientos de descarte de información.

  - Otros no declarados expresamente de uso aceptable

## CAPÍTULO XXVII: DE LA GESTIÓN DE CAMBIOS DE TI

**Artículo 86.- GENERALIDADES DE LA GESTIÓN DE CAMBIOS DE TI:**

Define las directrices y el marco general para que los cambios normales, estándar y de emergencia se registren, evalúen, autoricen, prioricen, planifiquen, prueben, implementen, documenten y revisen de una manera controlada, habilitando de esta forma la implementación de cambios exitosos con una mínima afectación a la operación cotidiana de CFN B.P.

La presente política debe ser observada y cumplida por todos los funcionarios y colaboradores que soliciten cambios (cambio normal, estándar o de emergencia) en CFN B.P.

La política contempla el registro del cambio (normal, estándar y de emergencia), así como la gestión del cambio sobre los componentes, elementos o servicios tecnológicos, hasta el trámite del cierre del cambio.

**Artículo 87.- NORMAS:**

**Comisión de Administración de Cambios (CAB) y Comisión de Administración de Cambios de Emergencia (ECAB)**

- La Comisión de Administración de Cambios (CAB) aprueba y supervisa los cambios normales -de riesgos e impacto mayor- para CFN B.P., estableciendo las prioridades y las condiciones para la implementación.
- En la Comisión de Cambios (CAB) deben participar al menos los siguientes funcionarios o sus delegados:
  - Gerente de Tecnologías de la Información.
  - Gerente de la Unidad Administrativa en la que trabaja el propietario de la aplicación y de la información mayormente impactada por el cambio.
  - Gerente de Seguridad de la Información.
  - Subgerente de Riesgo Operativo.
  - Otras gerencias impactadas por el cambio.
- La Comisión de Administración de Cambios de Emergencia (ECAB) únicamente acepta cambios de emergencia por las siguientes condiciones:
  - Un evento está produciendo que se acumulen pérdidas económicas contra CFN B.P. conforme el tiempo transcurre, si no se realiza el cambio.
  - Un evento está perjudicando a más clientes de CFN B.P. conforme el tiempo transcurre, si no se realiza el cambio.
  - Una exigencia gubernamental establece un plazo muy cercano lo que produce la emergencia, pues si no se cumple el plazo se expone a CFN B.P. al incumplimiento, sanciones económicas y administrativas, pérdida de reputación.
- En la Comisión de Administración de Cambios de Emergencia (ECAB) deben participar al menos tres gerentes de la lista a continuación o sus delegados:
  - Gerente de Tecnologías de la Información.

- Gerente de la Unidad Administrativa en la que trabaja el propietario de la aplicación y de la información mayormente impactada por el cambio. Si no está presente, el Gerente de la Unidad Administrativa involucrada, siendo una condición de emergencia, se acepta que otro gerente asuma como reemplazo, pudiendo ser otra gerencia impactada por el cambio, el Gerente de Seguridad de la Información, Subgerente de Riesgo Operativo.

**Presentación de la Solicitud / Requerimiento del Cambio**

- En todos los casos se debe elaborar una solicitud formal de cambio (Request For Change). El solicitante del cambio debe proporcionar:
  - Una clara descripción de las necesidades del negocio, las metas y objetivos del cambio.
  - Información adicional relacionada con el cambio cuando se lo requiera.
- Se debe aplicar un procedimiento y tramite diferentes si se trata de un cambio normal, estándar o de emergencia.
- Para los cambios estándares y normales se debe considerar el cumplimiento de los Acuerdos de Nivel de Servicios (ANS) acordados con las unidades y divisiones de los solicitantes de cambios.
- Se deben identificar los conflictos que existan con otros cambios pendientes o en curso.
- Se deben estimar los tiempos, costos, recursos requeridos para la implementación del cambio en función de la información de la solicitud de cambio (RFC) y de las especificaciones técnicas y funcionales.
- Se deben considerar en forma anticipada las implicaciones mayores de la puesta en producción del cambio, junto con sus riesgos, fechas y posibles consecuencias.

**Aprobación y priorización del Cambio**

- Aprobación de Cambios estándares.
  - Los cambios estándares deben ser autorizados por una única vez por CAB, por lo que aquellos que sean del mismo tipo de cambio estándar se amparan en la autorización otorgada originalmente por la Comisión de Administración de Cambios.
- Aprobación de Cambios de emergencia.
  - Se deben aprobar los cambios de emergencia en Comisión de Administración de Cambios de Emergencia (ECAB), y se debe proceder a su ejecución inmediata.
  - Se deben evaluar mediante estimaciones anticipadas las implicaciones visibles de la puesta en producción del cambio de emergencia, junto con sus componentes, riesgos, fechas y posibles consecuencias, y reportar al ECAB.
  - La documentación formal de los cambios de emergencia debe completarse hasta dos días después de implementado el cambio de emergencia, antes de realizar el cierre del cambio. Al final, el cambio de emergencia debe quedar con los mismos registros que un cambio normal.
- Aprobación de Cambios Normales.
  - La Comisión de Administración de Cambios aprueba y prioriza, o rechaza, los cambios normales según los criterios de urgencia, plazos, impacto, riesgos, costos, planeación, utilización de recursos.
  - Todos los cambios normales deben ser evaluados y priorizados adecuadamente, considerando la posición del solicitante del cambio y sus argumentos.

**Realizar el Cambio**

- Dentro de la Gerencia de Tecnologías de la Información se debe Asignar un Coordinador o Responsable del Cambio aprobado, así como los recursos para gestionar el cambio.
- Se debe garantizar el cumplimiento de la agenda de cambios aprobada.
- Asegurar que la Unidad Administrativa requirente esté informada de la programación, impacto, costo, riesgos, y progreso de los cambios.
- Se debe trabajar de manera estructurada y oportuna con todos los involucrados (internos, externos) de la organización para lograr una implementación eficiente del cambio.
- Elaborar los documentos necesarios de acuerdo a los procedimientos de la Gerencia de Tecnologías de la información, como por ejemplo: Manuales técnicos (de ser el caso) manuales de usuarios (de ser el caso), manuales de operación, manuales de instalación, modelos de datos, en el caso de creación usuarios gestionar formularios de permisos para roles. Documentar o actualizar la documentación de las versiones implementadas. Dar mantenimiento a la información requerida sobre Elementos de Configuración (CI's).
- Se deben realizar las pruebas unitarias como evidencia previa a la ejecución de las pruebas de certificación.

**Pruebas del Cambio**

- Antes del paso a producción, se debe certificar el cumplimiento de los cambios y el éxito de su ejecución, tanto a nivel técnico como funcional. Analizar las causas de falla de los cambios no exitosos y proponer acciones de mejora.
- El solicitante del cambio debe participar en la ejecución de las pruebas del cambio.
- Se debe validar la documentación generada por el cambio.

**Gestionar Puesta en Producción**

- Después de realizar las Pruebas del Cambio, se debe solicitar la implementación del cambio en el ambiente de producción.
- Revisar las recomendaciones o acuerdos realizados por la comisión con respecto a la autorización de la liberación de puesta en producción.
- Todo cambio, previo a su puesta en producción, debe contemplar una capacitación a los funcionarios de la Gerencia de Tecnologías de la Información que brindan el soporte de primer nivel, y a los Solicitantes del cambio.
- Verificar el resultado de la implantación y devolver el producto de ser requerido.
- Evaluar, notificar, mitigar las implicaciones de la puesta en producción del cambio, junto con sus componentes, riesgos, fechas y posibles consecuencias.
- Validar la documentación requerida para el paso a producción y gestionar las versiones de los componentes o elementos modificados por el cambio
- Emitir las tareas para la actualización de los elementos de configuración afectados por el cambio en la CMDB (Base de Datos de Gestión de Configuraciones).

**Periodos de estabilización y producción**

- Proporcionar soporte entrenado al Solicitante del Cambio, para los periodos de estabilización y de producción, mientras se da la transición completa.

- Se debe evaluar el resultado del cambio puesto en producción.
- Si el ambiente de producción no se estabiliza, considerar la devolución del cambio. Todo cambio debe tener un procedimiento de Rollback o marcha atrás, asegurar que se incluya en los planes de prueba y que están aptos para ser utilizados en el caso de materializarse una contingencia que desestabilizo el ambiente de producción.

**Cierre del Cambio**

- Se debe confirmar que el equipo de soporte esta adecuadamente entrenado sobre el cambio.
- Se debe confirmar con el solicitante del cambio que el cambio puede cerrarse.

**Retroalimentación y Mejoramiento continuo**

- Se deben presentar reportes de gestión de cambios al Gerente de Tecnologías de la Información, Comisión de Cambios y al Gerente de Seguridad de la Información, para que los cambios sean evaluados y priorizados.
- Se deben proponer mejoras sobre el procedimiento de Gestión de Cambios, en base a métricas y tendencias, para que el análisis y evaluación de los cambios sean siempre más eficientes, así como la realización de los cambios.
- Se deben ejecutar directrices para el mejoramiento continuo de los procedimientos de gestión de cambios.

## CAPÍTULO XXVIII: DISEÑAR, MONITOREAR, PISTAS DE AUDITORÍA EN APLICATIVOS Y BASES DE DATOS

### Artículo 88.- GENERALIDADES PARA DISEÑAR, MONITOREAR, PISTAS DE AUDITORÍA EN APLICATIVOS Y BASES DE DATOS:

Esta política define las directrices para diseñar, monitorear, pistas de auditoría en aplicativos y bases de datos de CFN B.P.

Los accesos y transacciones a bases de datos realizados en los aplicativos, que previamente han sido definidos por los propietarios de los activos de información, deben contar con pistas de auditoria (rastro de las acciones realizadas -en bitácoras o logs) que permitan en cualquier momento revisar / analizar / establecer trazabilidad de actividades realizadas en el pasado para determinar optimizaciones, correctivos, mejoras, investigaciones, reparaciones en el futuro, y para prevenir condiciones que atenten contra la seguridad de la información de CFN B.P. en los aplicativos y las bases de datos.

En algunas circunstancias los requerimientos de pistas de auditoria pueden provenir de entidades gubernamentales, unidades internas de control, resultados de auditoria recientes, nuevas aplicaciones o rediseño de las aplicaciones actuales, gestión estratégica, etc.; las cuales deberán ser solicitadas por los propietarios de los activos de información.

Las pistas de auditoria registradas deben mantenerse disponibles en línea por el período dispuesto por los propietarios de los activos de información (pueden basarse en decisiones gerenciales internas o por los organismos de control).

Los accesos a las pistas de auditoria para monitoreo y administración deben ser autorizados por el propietario / responsable de información, únicamente a las unidades administrativas relacionadas y/o de interés.

Los propietarios de los activos de información deben proponer los requerimientos relacionados con las pistas de auditoría de los procesos funcionales de los aplicativos, para que sean aprobados por la Gerencia de Seguridad de la Información.

**Artículo 89.- NORMAS:**

**Diseñar pistas de auditoría en aplicativos y bases de datos**

- Los propietarios de los activos de la información son los responsables de plantear la solicitud de implementación de pistas de auditoría en los sistemas informáticos, a la Gerencia de Tecnologías de la Información o al Área encargada de planificar los proyectos a nivel Institucional. Para ello deben presentar toda la documentación habilitante, misma que previamente debe contar con la revisión por parte de la Gerencia de Seguridad de la Información.
- La Gerencia de Tecnologías de la Información debe implementar las pistas de auditoría solicitadas por los propietarios de los activos de información mismas que previamente fueron revisadas por la Gerencia de Seguridad de la Información.
- La Gerencia de Tecnologías de la Información debe exigir a los desarrolladores (internos o externos) que crean o modifican programas de las aplicaciones (web, móvil, tradicionales) criticas -que soportan a los procesos críticos o administran información de clientes de CFN B.P.- que incluyan las pistas de auditoria requeridas en cuanto a accesos a aplicativos y bases de datos.
- Las pistas de auditoria deben contener por lo menos los siguientes datos:
  - Acción realizada
  - Usuario que realiza la acción (Código de usuario, perfil, rol)
  - Fecha/hora
  - Recursos (activos de información) consultados/modificados/eliminados/creados
  - En modificaciones, se debe registrar el valor anterior y el valor nuevo
  - Nombre del dispositivo / IP (computador, Tablet, Smartphone) desde donde se realiza la acción
- La Gerencia de Tecnologías de la Información es responsable por la obtención de copias de seguridad (backups / respaldos) de la configuración e información residente en las pistas de auditoria de bases de datos y aplicaciones.
- En caso de ser necesario vaciar (eliminar) las pistas de auditoria y log's de seguridad, la Gerencia de Tecnologías de la Información debe notificar al propietario de la información y solicitar su autorización expresa.
- La Gerencia de Tecnologías de la Información debe implementar mecanismos seguros con controles de integridad para que las pistas de auditoria estén protegidas contra manipulaciones indebidas y accesos no autorizados. Los propietarios de los activos de la información son los que definirán los accesos a las pistas de auditoría a los diferentes usuarios, mientras que la Gerencia de Seguridad de la Información son los encargados de parametrizar dichos accesos en los sistemas informáticos y herramientas tecnológicas.

**Monitorear pistas de auditoría en aplicativos y bases de datos**

- La Gerencia de Tecnologías de la Información debe revisar trimestralmente la existencia de información en los repositorios de las pistas de auditoria.
- La Gerencia de Seguridad de la Información debe revisar semestralmente la existencia de información en los repositorios de las pistas de auditoria.
- Cada Gerencia de áreas usuarias y/o propietarios de la información serán los responsables de la revisión regular de las pistas de auditoria de las aplicaciones / servicios informáticos a su cargo, sobre lo cual deben informar de sus resultados a Auditoria Interna y a la Gerencia de Seguridad de la Información.
- La Gerencia de Tecnologías de la Información, la Gerencia de Seguridad de la Información, la Gerencia de Riesgos, y Auditoria Interna pueden realizar revisiones y análisis a las pistas de auditoria en todo momento.

## CAPÍTULO XXIX: CONTROL DEL ESCANEO AUTOMATIZADO DE VULNERABILIDADES EN CÓDIGO FUENTE

### Artículo 90.- GENERALIDADES PARA EL CONTROL DEL ESCANEO AUTOMATIZADO DE VULNERABILIDADES EN CÓDIGO FUENTE:

Esta política define las directrices para el control del escaneo automatizado de vulnerabilidades en código fuente, orientado a reforzar la seguridad de la información de CFN B.P.

La presente política aplica sobre todos los archivos fuentes de los aplicativos informáticos usados en CFN B.P.

### Artículo 91.- NORMAS:

**Responsabilidades elementales**

- La Gerencia de Tecnologías de la Información debe contar con un instructivo para el desarrollo interno o para la adquisición de software web, el cual deberá estar basado en las mejores prácticas de la industria en cuanto a codificación segura.

- La Gerencia de Tecnologías de la Información debe exigir a los desarrolladores (internos o externos) que crean o modifican programas de las aplicaciones (web, móvil, tradicionales) que soportan a los procesos críticos o administran información de clientes de CFN B.P.- a aplicar estándares de desarrollo seguro para evitar vulnerabilidades en el código fuente, ataques cibernéticos, así como errores en la presentación o alteraciones en el contenido de la información que se reporta a clientes, entidades de control, comités internos, y público.

- La Gerencia de Tecnologías de la Información debe mejorar continuamente, documentar e implantar la metodología para el correcto desarrollo de los sistemas de información que garantice la calidad y seguridad en el código fuente, y que la funcionalidad en el procesamiento de información esté acorde a las necesidades de CFN B.P.

- La Gerencia de Tecnologías de la Información debe consultar continuamente las Bases de Datos con Registro de Vulnerabilidades o equivalente, y distribuir a los desarrolladores las noticias y alertas sobre las vulnerabilidades que aplican a CFN B.P. Los hackers siempre consultan estos mismos repositorios, es necesario adelantarse a sus intenciones.

- La Gerencia de Tecnologías de la Información debe priorizar la corrección de vulnerabilidades, pues los resultados del escaneo y las noticias en las bases de datos pueden involucrar cientos de vulnerabilidades.

- La Gerencia de Tecnologías de la Información en colaboración con las unidades administrativas que correspondan, debe capacitar continuamente a los desarrolladores de CFN B.P., internos o externos, sobre las buenas prácticas de codificación segura.

- La Gerencia de Tecnologías de la Información deberá implementar las herramientas necesarias que permitan el análisis de vulnerabilidades de seguridad en los sistemas informáticos, considerando la infraestructura tecnológica que requieran

**Escaneo automatizado de vulnerabilidades en código fuente**

- La Gerencia de Tecnologías de la Información debe efectuar una validación (escaneo) de vulnerabilidades a nivel de código fuente, previo al paso de las aplicaciones a ambiente de producción. Este escaneo debe

hacerse de manera obligatoria sobre cada programa creado o modificado de las aplicaciones críticas de CFN B.P. (aplicaciones que soportan a los procesos críticos)

- La Gerencia de Seguridad de la Información debe validar el escaneo realizado por la Gerencia de Tecnologías de la Información. Además será responsable de actualizar la documentación formal relacionada con esta temática.

- La Gerencia de Tecnologías de la Información debe instalar y aplicar la tecnología, metodología o servicios necesarios para escanear vulnerabilidades en código fuente de CFN B.P.

- Los desarrolladores deben reportar a la Gerencia de Seguridad de la Información las vulnerabilidades encontradas en código fuente de CFN B.P., o certificar que no existen vulnerabilidades después de su revisión.

- La Gerencia de Tecnologías de la Información debe priorizar y aplicar, cuanto antes sea posible, los parches de seguridad liberados para resolver las vulnerabilidades descubiertas, pues la mayoría de los ataques se producen sobre las vulnerabilidades que no se han parchado.

**Control del escaneo automatizado de vulnerabilidades en código fuente**

- La Gerencia de Seguridad de la Información debe realizar revisiones cuatrimestrales para identificar evidencias de que los escaneos de vulnerabilidades a nivel de código fuente se han realizado previo al paso de las aplicaciones a ambiente de producción, especialmente sobre los cambios realizados por emergencia, y sobre las aplicaciones críticas.

- La Gerencia de Seguridad de la Información debe revisar los reportes de los desarrolladores sobre las vulnerabilidades encontradas, así como las certificaciones que confirman que no encontraron vulnerabilidad.

- La Gerencia de Seguridad de la Información debe ser informada sobre los parches de seguridad que se instalan para prevenir o corregir vulnerabilidades, así como las novedades presentadas en el proceso de instalación.

## CAPÍTULO XXX: MONITOREAR LA EFECTIVIDAD DE LOS NIVELES DE SEGURIDAD IMPLEMENTADOS EN HARDWARE, SOFTWARE, REDES Y COMUNICACIONES

**Artículo 92.- GENERALIDADES PARA MONITOREAR LA EFECTIVIDAD DE LOS NIVELES DE SEGURIDAD IMPLEMENTADOS EN HARDWARE, SOFTWARE, REDES Y COMUNICACIONES:**

Esta política define las directrices para monitorear la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones de CFN B.P.

En algunas circunstancias los requerimientos de monitoreo pueden provenir de entidades gubernamentales, unidades internas de control, resultados de auditoria recientes, nuevas aplicaciones o rediseño de las aplicaciones actuales, gestión estratégica, etc.

**Artículo 93.- NORMAS:**

**Responsabilidades de monitoreo de la efectividad de los niveles de seguridad**

- Diversas políticas y procedimientos internos establecen niveles de seguridad sobre hardware, software, redes y comunicaciones de CFN B.P.

- La Gerencia de Seguridad de la Información debe monitorear en forma integral la efectividad de los niveles de seguridad determinados por las políticas y procedimientos internos sobre hardware, software, redes y comunicaciones de CFN B.P.

- Todas las Unidades Administrativas son responsables de monitorear internamente la efectividad de los niveles de seguridad sobre los activos de información a su cargo, en el ambiente de trabajo de la Unidad Administrativa correspondiente.

**Insumos para el monitoreo de la efectividad de los niveles de seguridad**

- Los responsables designados deben obtener información de las siguientes fuentes para realizar el monitoreo periódico de la efectividad de los niveles de seguridad:
    - Bases de datos de riesgos;
    - informes de auditoría interna y externa;
    - informes de consultores contratados;
    - bitácoras de Tecnologías de la Información;
    - informes de solución a incidentes mayores;
    - diagnósticos y evaluaciones de riesgos de seguridad de la información;
    - base de datos de incidentes y problemas de Tecnologías de la Información;
    - registros (logs);
    - observación;
    - entrevistas;
    - otra información que La Gerencia de Seguridad de la Información considere relevante.
- La información puede ser histórica o vigente.

**Herramientas para el monitoreo de la efectividad de los niveles de seguridad**

- La Gerencia de Seguridad de la Información debe proponer y coordinar con la Gerencia de Tecnologías de la Información la adquisición de productos o la contratación de servicios, si no están disponibles en CFN B.P., para monitorear la efectividad de los niveles de seguridad.

- La Gerencia de Tecnologías de la Información debe implementar y habilitar los productos aprobados, adquiridos o contratados, según requerimiento de la Gerencia de Seguridad de la Información, para monitorear la efectividad de los niveles de seguridad.

**Monitoreo de la efectividad de los niveles de seguridad**

- La Gerencia de Seguridad de la Información debe monitorear con la frecuencia que determinen los procedimientos (según los componentes de hardware, software, redes y comunicaciones), la eficacia y la efectividad de los controles de seguridad de la información establecidos en la entidad y generar informes dirigidos al Comité de Administración de Seguridad de la Información para su conocimiento y toma de acciones que eviten o disminuyan los riesgos de seguridad.

- Cada Unidad Administrativa y/o propietarios de la información deben informar de sus resultados sobre el monitoreo de los niveles de seguridad a la Gerencia de Seguridad de la Información.

- La Gerencia de Tecnologías de la Información, la Gerencia de Seguridad de la Información, la Gerencia de Riesgos, y Auditoria Interna, dentro del ámbito de sus competencias, deben realizar revisiones, análisis, monitoreo de la efectividad de los niveles de seguridad en todo momento.

- La Gerencia de Seguridad de la Información debe informar al Comité de Gestión de Seguridad de la Información sobre las acciones que incluyen la implementación de los controles identificados y planes de mejora para esta política.

## CAPÍTULO XXXI: PRINCIPIO DE INGENIERÍA EN SISTEMAS SEGUROS

### Artículo 94.- GENERALIDADES PARA EL PRINCIPIO DE INGENIERÍA EN SISTEMAS SEGUROS:

Esta política define las directrices para cumplir con el principio de ingeniería en sistemas seguros.

El principio de ingeniería en sistemas seguros se especifica en la guía ISO 27002, norma que establece que la seguridad debe ser incluida en el diseño de todas las capas de arquitectura (por ejemplo negocios, datos, aplicaciones, tecnología), contemplando la necesidad de accesibilidad a funciones e información.

### Artículo 95.- NORMAS:

**Responsabilidades elementales basadas en el principio de ingeniería en sistemas seguros**

- La Gerencia de Tecnologías de la Información, con apoyo de la Gerencia de Seguridad de la Información, debe definir estrategias, políticas, procedimientos y directrices sobre cómo se identifican, evalúan y tratan los riesgos de la información en el curso (a lo largo de todo el ciclo de vida) de las actividades de desarrollo de software / sistemas.

- La Gerencia de Tecnologías de la Información debe considerar:

  - métodos de desarrollo con documentados análisis de riesgo, diseño / selección de seguridad, plataformas seguras, servicios / funciones / procesos de seguridad,

  - desarrollo / codificación seguros, pruebas de seguridad y rendimiento, implementación / configuración segura,

  - verificación posterior a la instalación, actividades de gestión y mantenimiento del sistema y su seguridad, etc., así como asegurar un tratamiento correcto de las aplicaciones informáticas y sus datos en todo su ciclo de vida.

- En relación con la amplia gama de requerimientos y necesidades de seguridad del sistema / aplicación, la Gerencia de Tecnologías de la Información debe considerar la seguridad en:

  - ingeniería de seguridad (ISO 27002),

  - arquitectura y diseño,

  - cumplimiento de obligaciones / expectativas legales, reglamentarias, contractuales, éticas y comerciales,

- procesos del negocio / controles administrativos,
- identificación y autenticación, controles de acceso y privacidad -incluidos las especificaciones, el código, los datos de prueba y los resultados de prueba,
- criptografía,
- controles de fraude,
- seguridad de la red / mensajería,
- controles de malware,
- alarmas y alertas,
- registro,
- administración de seguridad,
- integridad de los datos,
- copias de seguridad, resistencia y recuperación.

- La Gerencia de Tecnologías de la Información debe exigir a los desarrolladores (internos o externos) que crean o modifican programas de las aplicaciones (web, móvil, tradicionales) -que soportan a los procesos o administran información de clientes de CFN B.P.- que apliquen permanentemente el principio de ingeniería en sistemas seguros (ISO 27002) y basados en técnicas para la seguridad del software en general como OWASP.

- La Gerencia de Tecnologías de la Información debe priorizar la corrección de cualquier desvío en la aplicación del principio de ingeniería en sistemas seguros.

- La Gerencia de Tecnologías de la Información en colaboración con las unidades administrativas que correspondan, debe capacitar continuamente a los desarrolladores de CFN B.P., internos o externos, sobre la aplicación del principio de ingeniería en sistemas seguros.

**Requisitos de seguridad para los sistemas de información / aplicaciones informáticas**

Los sistemas de información de CFN B.P. que entren a producción deben contemplar al menos las siguientes características para el control de accesos:

- Permitir la administración de cuentas de usuario del sistema considerando:
  - Creación, mantenimiento, eliminación lógica de usuarios.
  - Validación de usuario único.
  - Manejo de estados de la cuenta: vigente, bloqueado, eliminado, expirado.
  - El estado expirado debe ser manejado con fecha de expiración.
  - Permitir la creación de usuarios con característica de Administrador de Seguridades.
  - Bloqueo de cuenta por n intentos fallidos parametrizable. El parámetro debe iniciar con el valor de 3, pero podría cambiar por definición de la Gerencia de Seguridad de la Información.
  - Un usuario con rol de Administrador de Seguridades, que no debe poder administrarse a sí mismo.
  - El desbloqueo automático de una cuenta de usuario, luego de n tiempo.

- Permitir la administración de contraseñas considerando:
  - Encriptación de contraseñas: la clave de usuario no debe estar en texto “plano” en las tablas de la base de datos.
  - Con el mismo usuario del aplicativo no se debe poder conectar directamente a la base de datos.
  - Debe solicitar cambio de contraseña en forma automática, cada n días, parametrizables. El parámetro puede iniciar con 60 días pero puede ser modificado de acuerdo a lo que defina la Gerencia de Seguridad de la Información.
  - La primera vez que el usuario ingrese al aplicativo, se debe forzar cambio de clave.
  - Cuando el Administrador de Seguridades resetee la contraseña, el aplicativo debe forzar cambio de clave en el siguiente ingreso por parte del usuario.
  - La contraseña reseteada desde el aplicativo por el Administrador de Seguridades debe generarse en forma aleatoria, es decir, que el administrador de seguridades no establezca la misma.
  - La complejidad de la contraseña debe ser parametrizable, estableciendo la cantidad de letras mayúsculas, minúsculas, caracteres especiales (indicando los permitidos) y números.
  - Posibilidad de excluir contraseñas (diccionario).
  - La clave no debe repetirse en n veces parametrizable, es decir, que el sistema recuerde las últimas contraseñas y no permita reutilizarlas. El parámetro puede iniciar con 3 pero puede ser modificado de acuerdo a lo que defina la Gerencia de Seguridad de la Información.
  - Posibilidad de auto-gestionar el reseteo de su contraseña, con la facilidad “¿Olvidó su contraseña?”.
- Administración de instancias, considerando:
  - Debe permitir controlar el número de instancias abiertas del aplicativo (n, parametrizable).
  - Debe controlar que un usuario no se pueda conectar en más de 1 PC al mismo tiempo.
  - Debe permitir la desconexión automática del sistema o bloqueo del mismo, luego de n tiempo de inactividad, parametrizable.
- Permitir la administración de roles (perfil) considerando:
  - Creación, mantenimiento, eliminación lógica.
  - Personalización del rol de acuerdo a las necesidades del negocio, en forma gráfica (árbol): Aplicación – Módulo – Sub módulo – Menú – Sub menú – Opción (insertar, eliminar, modificar, procesos especiales).
  - Cuando se creen nuevas pantallas, las opciones de menú deben reflejarse en forma automática en la pantalla de administración de roles.
  - Las opciones de menú en un rol por defecto deben estar deshabilitadas, para la asignación de una pantalla a un rol, se deberá hacerlo en forma explícita.
  - Asignación de usuarios a roles.
  - Creación de roles en base de otro rol (copia).
- Administración de calendario y horarios (deseable):
  - Debe permitir controlar los días hábiles para conexión de los usuarios.
  - Debe permitir controlar el horario de conexión de los usuarios.

- Reportes de Seguridades, obtener al menos listados de usuarios (por estado), usuario/roles, rol(es)/usuarios, rol/opciones, opción/roles, información de pistas y logs de auditoria, entre otros.

- La administración de seguridades debe poder integrarse a otras soluciones del eDirectory, para manejo centralizado de identidades.

- En caso de que la solución este basada en Web debe:

  o Para garantizar la seguridad de la información en el sitio web, se deberá hacer uso de certificados digitales web (SSL/TLS), equivalente o superior.

  o Incluir seguridad: a nivel de cliente (browser), a nivel de servidor a fin de garantizar la confidencialidad e integridad de la información (obligatorio si es Web).

  o La renovación de por lo menos una vez (1) al año de las claves de acceso a los canales electrónicos.

  o Se procede con el bloqueo de la cuenta en el canal electrónico después de un número máximo de (n) intentos de acceso fallido. El parámetro puede iniciar con el valor de 3, pero puede ser modificado por la Gerencia de Seguridad de la Información.

  o En todas las transacciones de clientes que se realicen a través de la Banca Virtual deben implementarse métodos de autenticación que contemplen por lo menos dos de tres factores: “algo que se sabe, algo que se tiene, o algo que es”, considerando que uno de ellos debe ser dinámico por cada vez que se efectúa una transacción.

  o Establecer el tiempo de inactividad en la cual se debe expirar la sesión, para reanudar la misma el usuario deberá autenticarse nuevamente.

- Para aplicaciones orientadas al cliente de CFN B.P., se debe considerar adicionalmente:

  o Implementar mecanismos de control, autenticación mutua y monitoreo, que reduzcan la posibilidad de que los clientes accedan a páginas web falsas similares a las propias de la CFN B.P.

  o Implementar teclados virtuales para el ingreso de claves, las mismas que deben estar enmascaradas.

  o Informar al cliente al inicio de cada sesión, la fecha y hora del último ingreso al aplicativo.

  o Notificar al cliente de su actividad en el aplicativo (ingresos exitosos, fallidos, bloqueos, desbloqueos, cambios de clave, transacciones realizadas - si aplicara, entre otros) a través de cual medio por ejemplo: mensajería móvil, correo electrónico.

- A fin de asegurar el portal institucional, se implementarán mecanismos para impedir la copia de sus diferentes componentes, verificar constantemente que no sean modificados sus enlaces (links), suplantados sus certificados digitales, ni modificada indebidamente la resolución del sistema de nombres de dominio.

**Seguridad en los procesos de desarrollo y soporte**

- La Gerencia de Tecnologías de la Información debe documentar, implantar y mejorar un procedimiento formal para el control de cambios que garantice la segura operación del negocio.

- La Gerencia de Tecnologías de la Información debe implantar los mecanismos necesarios para mantener un adecuado control de versiones de los sistemas de información y cada componente de los servicios informáticos.

- La Gerencia de Tecnologías de la Información debe mantener un inventario resumen de los sistemas de información y aplicaciones comerciales que la soportan con la descripción y versión correspondiente, el mismo que deberá residir en un ambiente seguro (CMS/CMDB).

- La implementación de los sistemas de información se debe llevar a cabo minimizando la discontinuidad de las actividades de la empresa.

- Todo sistema de información debe contar con la documentación técnica y de usuario debidamente actualizada.

**Seguridad en ambientes de prueba**

- La Gerencia de Tecnologías de la Información debe implementar políticas y procedimientos para proteger adecuadamente los datos (originalmente de producción) que fueren destinados para pruebas.

## CAPÍTULO XXXII: GESTIÓN DE LOS REPORTES DE MONITOREO EMITIDO POR SOC Y ALARMAS ANTIMALWARE – ANTIVIRUS - ANTIPHISHING

**Artículo 96.- GENERALIDADES DE LA GESTIÓN DE LOS REPORTES DE MONITOREO EMITIDO POR SOC Y ALARMAS ANTIMALWARE – ANTIVIRUS - ANTIPHISHING:**

Esta política define las directrices para la gestión de los reportes del monitoreo emitido por el Security Operation Center (SOC) y de las alarmas del Software antimalware, antivirus, antiphishing, incluyendo las actividades que debe de realizar el personal técnico autorizado ante eventos inusuales o falla de los servicios de CFN B.P.

Con el uso de servicios SOC y software antimalware, antivirus, antiphishing, CFN B.P. busca detectar a tiempo un ciberataque o violaciones de seguridad para responder lo más rápidamente posible y minimizar el impacto de una amenaza materializada.

**Artículo 97.- NORMAS:**

**Resultados de la gestión de los servicios SOC y el software antimalware, antivirus, antiphishing**

- El Security Operation Center (SOC), un servicio de ciber seguridad interno o contratado con un proveedor, debe generar reportes con los resultados del monitoreo (escaneo de vulnerabilidad) realizado sobre las redes y plataformas que son objeto de dicho monitoreo permanente.

- El servicio SOC puede tener la delegación para actuar preventiva o reactivamente sobre las amenazas y debilidades encontradas, o puede informarlas para acción posterior.

- El servicio SOC debe detectar oportunamente actividades maliciosas que encajan en un patrón de un ataque típico, y puede neutralizarlas.

- El software antimalware, antivirus, antiphishing adquirido por CFN B.P., administrado internamente, o administrado por un servicio SOC contratado, debe generar alarmas para que se tomen acciones de remediación o prevención.

**Responsabilidades de la gestión de los reportes de monitoreo**

- La Gerencia de Seguridad de la Información y la Gerencia de Tecnologías de la Información deben acordar con el servicio SOC (interno o externo) el tipo de reportes y alertas requeridos, la periodicidad de la generación de reportes, el nivel de severidad de los tipos de incidentes para CFN B.P., y las prioridades de acción sobre los mismos.

- La Gerencia de Seguridad de la Información debe recibir oportunamente la información con las alertas generadas por el software antimalware, antivirus, antiphishing.

- La Gerencia de Seguridad de la Información y la Gerencia de Tecnologías de la Información deben decidir las acciones de remediación o prevención a seguir en función de la gravedad de las alertas generadas por el software antimalware, antivirus, antiphishing.

- La Gerencia de Tecnologías de la Información y la Gerencia de Seguridad de la Información deben evaluar y decidir sobre las recomendaciones del servicio SOC para adaptar y modificar las protecciones de las redes de CFN B.P., en función de lo reportado.

- La Gerencia de Seguridad de la Información debe evaluar las recomendaciones del servicio SOC, y proponer continuamente los cambios necesarios en la infraestructura y redes para cumplir legalmente con las medidas de protección obligatorias con respecto a la ciber seguridad.

- La Gerencia de Tecnologías de la Información debe instruir al personal técnico autorizado las actividades que debe realizar ante eventos inusuales o falla de los servicios de CFN B.P. reportados por el servicio SOC. Las actividades obedecen a los casos particulares y circunstanciales, pero se deben aplicar los procedimientos Gestión de Incidentes de TI y Gestión de Problemas de TI.

## CAPÍTULO XXXIII: MONITOREAR, CONTROLAR Y EMITIR ALARMAS EN LÍNEA QUE INFORMEN OPORTUNAMENTE SOBRE EL ESTADO DE LOS CANALES ELECTRÓNICOS

### Artículo 98.- GENERALIDADES PARA MONITOREAR, CONTROLAR Y EMITIR ALARMAS EN LÍNEA QUE INFORMEN OPORTUNAMENTE SOBRE EL ESTADO DE LOS CANALES ELECTRÓNICOS:

Definir las directrices para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas, para mantener la seguridad de la información de CFN B.P.

La presente política aplica para todos los canales electrónicos o digitales (sitio web interno -correo, sitio web externo – y otros aplicativos informáticos habilitados para clientes externos (por ejemplo: remates, factoring electrónico, fondo de garantías, etc.). Se refiere a todas las vías o formas mediante el uso de internet u otras redes, a través de las cuales los clientes o usuarios pueden efectuar transacciones, consultas, intercambio de información, etc., con CFN B.P.

La presente política debe ser observada y cumplida por todos los funcionarios y colaboradores sean estos empleados directos, externalizados o servicios profesionales, y por entidades externas como proveedores o entidades de control los cuales tengan acceso a la información que maneja CFN B.P.

**Artículo 99.- NORMAS:**

**Concienciación en el uso de los Canales electrónicos**

- La Gerencia de Seguridad de la Información en colaboración con las unidades administrativas que correspondan, debe informar y capacitar a los clientes sobre los riesgos derivados del uso de canales electrónicos y de tarjetas; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de éstos, de acuerdo a su planificación operativa anual.

- La Gerencia de Seguridad de la Información, debe informar y capacitar a los clientes de acuerdo a su programación operativa, sobre los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los canales electrónicos ofrecidos por la entidad.

**Monitoreo sobre el estado de las medidas de seguridad de los Canales Digitales**

- La Gerencia de Tecnologías de la Información debe implementar y habilitar los productos aprobados, adquiridos o contratados, según requerimiento de la Gerencia de Seguridad de la Información, para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas. Son los encargados de la Administración Tecnológica de los productos, su configuración y mantenimiento, de tal manera de garantizar su disponibilidad. En el caso que se detecten eventos inusuales, deben ser notificados a la Gerencia de Seguridad de la Información.

- La Gerencia de Seguridad de la Información debe tener acceso de consulta a los productos implementados que le permitan monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas.

**Monitoreo sobre el acceso y uso**

- La Gerencia de Seguridad de la Información debe monitorear, controlar y emitir alarmas cuando algún funcionario de CFN B.P. conoce de manera no autorizada las claves de acceso o cualquier información confidencial que se use para autenticación remota de los clientes a los canales electrónicos de CFN B.P.

- La Gerencia de Seguridad de la Información debe monitorear, controlar y emitir alarmas cuando detecta que se producen repetidos intentos de acceso fallidos a los canales electrónicos.

**Monitoreo sobre consultas, transacciones y envío o recepción de información.**

- La Gerencia de Seguridad de la Información debe monitorear, controlar y emitir alarmas cuando detecta que las transacciones, consultas o solicitudes en canales electrónicos no son realizadas bajo una sesión segura (SSL-Secure Sockets Layer, con cifrado de 256 bits, equivalente o superior).

- La Gerencia de Seguridad de la Información debe monitorear, controlar y emitir alarmas cuando la información que se reciba o envíe no se realice estando dentro de un ambiente transaccional seguro, utilizando encriptación cuando fuera requerido.

**Información Estadística para identificar amenazas**

- La Gerencia de Seguridad de la Información debe recopilar información estadística e histórica que le permita controlar y emitir alarmas para informar oportunamente sobre el deterioro o ineficacia de las condiciones de seguridad de los canales electrónicos.

**Monitoreo sobre Cumplimiento de Términos**

- La Gerencia de Seguridad de la Información debe monitorear, controlar y emitir alarmas cuando detecte que las partes interesadas o los proveedores críticos de la entidad, relacionados con canales electrónicos, no están cumplimiento con: los acuerdos de niveles de servicio sobre intercambio de información y seguridad, los acuerdos de confidencialidad, los acuerdos de intercambio de información, procedimientos de entrega o eliminación de la información, gestión de riesgos y los compromisos de Seguridad de la Información, exigiendo que se cumplan sin excepción.

**Mejoramiento del ambiente seguro**

- La Gerencia de Seguridad de la Información debe monitorear, controlar y emitir alarmas cuando los canales electrónicos de CFN B.P. no funcionen bajo los protocolos de seguridad SSL y HTTPS equivalente o superior, los que proporcionan elementos necesarios para establecer una conexión segura y evitar que la información transmitida por la red pueda ser vista por personas no autorizadas.

- La Gerencia de Seguridad de la Información debe realizar análisis periódicos para detectar vulnerabilidades de seguridad de los canales electrónicos sobre internet que expongan a CFN B.P. a ataques cibernéticos.

- La Gerencia de Seguridad de la Información debe monitorear, controlar y emitir alarmas cuando se detecte que no toda información enviada desde CFN B.P. a través de canales electrónicos incluye en su pie de página la siguiente advertencia (o equivalente):

    - *Este mensaje (y cualquier archivo que se adjunte) es confidencial y podría contener información clasificada y reservada de CFN B.P., para el uso exclusivo de su destinatario. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje es prohibida y sancionada por la ley. Si por error recibe este mensaje, por favor reenviarlo al remitente y borre el mensaje recibido inmediatamente.*

## CAPÍTULO XXXIV: ANEXOS

- **Anexo 1 – ACUERDO DE CONFIDENCIALIDAD (Interno)**
- **Anexo 2 – ACUERDO DE CONFIDENCIALIDAD (Externo)**
- **Anexo 3 – ACUERDO DE CONFIDENCIALIDAD PARA LA UTILIZACIÓN DE HERRAMIENTAS TECNOLÓGICAS**

## DISPOSICIONES FINALES:

**PRIMERA.-** La presente Regulación entrará en vigencia a partir de su fecha de expedición, sin perjuicio de su publicación en el Registro Oficial.

**SEGUNDA.-** Encargar a la Gerencia de Calidad la actualización en la normativa institucional; y a la Secretaría General, su envío al Registro Oficial.

**TERCERA.-** Encargar a la Gerencia de Calidad la actualización del Subtítulo I: Política Institucional para la Administración de la Normativa CFN B.P. del Título I: Disposiciones normativas CFN B.P., Libro Preliminar: Generalidades de la Normativa CFN B.P., lo siguiente:

- Incorporar en el CAPÍTULO VI: POLÍTICAS PARA LA ADMINISTRACIÓN DEL LIBRO II NORMATIVA SOBRE ADMINISTRACIÓN, Título XVII Seguridad de la Información, Subtítulo I Políticas Institucionales para el Sistema de Gestión de Seguridad de la Información, el capítulo "Políticas Institucionales para el Sistema de Gestión de Seguridad de la Información" y el Capítulo "Anexos Política" y como área promotora a la Gerencia de Seguridad de la Información.

- Incorporar los Anexos en la siguiente ubicación dentro del repositorio de documentos: Normativa CFN: Libro II: Administración; Título XVII: Seguridad de la Información, Subtítulo I: Políticas Institucionales para el Sistema de Gestión de Seguridad de la Información; Anexos:

    - Anexo 1 – Acuerdo de confidencialidad (Interno)
    - Anexo 2 - Acuerdo de confidencialidad (Externo)
    - Anexo 3 - Acuerdo de confidencialidad para la utilización de herramientas tecnológicas

**CUARTA.-** Encargar a la Gerencia de Talento Humano la actualización del “Manual de procedimiento para la vinculación del personal” (MP-TSO-01-VP), respecto a la eliminación de la sección 5.5. Acuerdo de confidencialidad de la información del Registro operativo “Listado de documentos para la vinculación del personal” (R-TSO-VP-01).

**DADA**, en la ciudad de Guayaquil, el 23 de septiembre de 2022, **LO CERTIFICO.-**

NELSON IVAN PATRICIO ANDRADE APUNTE
Firmado digitalmente por NELSON IVAN PATRICIO ANDRADE APUNTE
Fecha: 2022.09.28 10:35:07 -05'00'

Mgs. Nelson Iván Patricio Andrade Apunte
**PRESIDENTE**

Firmado electrónicamente por:
**KATHERINE LISETH TOBAR ANASTACIO**

Lcda. Katherine Tobar Anastacio
**SECRETARIA GENERAL**


Ing. Hugo Del Pozo Barrezueta
DIRECTOR

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Telf.: 3941-800
Exts.: 3131 - 3134

www.registroficial.gob.ec

MG/XX

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

*"Al servicio del país desde el 1º de julio de 1895"*