BANCO CENTRAL DE COSTA RICA

# Políticas Específicas de Ciberseguridad

**HISTÓRICO DE VERSIONES Y CONTROL DE CAMBIOS A LA POLÍTICA.**

| Versión: | Fecha de creación: | Aprobado por: | Cambios realizados: |
|---|---|---|---|
| 6.0 | 02 de julio de 2024 | Aprobación del Gerente del Banco Central de Costa Rica | Se cambia la consideración C, se actualizan términos, se agregan los controles 12.2 y 14.2, y se actualizan las políticas específicas 29 y 30, las cuales cambian su redacción incluyendo sus controles y lineamientos. Se reenumeran las políticas de acuerdo con los cambios aplicados. |
| 5.0 | 19 de mayo de 2023 | Aprobación del Gerente del Banco Central de Costa Rica | Se ajusta el control C-8.1, se agrega el lineamiento L-8.1.4 sobre modificaciones directas a las bases de datos.<br>Se ajusta el control C-10.1, se elimina el lineamiento L-10.2.1 y se agrega el lineamiento L-28.1.1 sobre cifrado y equipo de usuario final, incluyendo su respectivo transitorio en la Consideración C.<br>Se ajusta el lineamiento L-16.1.1 relacionado al programa de concientización.<br>Se agrega el control C-27-2 sobre modificaciones de configuración en equipos institucionales.<br>Se realizan actualizaciones de términos, nombres de áreas y departamentos, se ajustan numeraciones y se realizan correcciones de forma.<br>Se ajusta el nombre de las Políticas Específicas a fin de que reflejen el cambio organizacional. |
| 4.0 | 19 de octubre de 2020 | Aprobación del Gerente del Banco Central de Costa Rica | Se incorporan 3 términos en la política P-2.<br>Se modifica la redacción de los lineamientos L-3.1.3., L-3.2.6, control C-10.2. y políticas P-15. y P-16.<br>Se agregan los lineamientos L-3.1.6, L-3.2.4.<br>Se agregan y ajustan numeraciones. |
| 3.0 | 10 de enero de 2020 | Aprobación del Gerente del Banco Central de Costa Rica | Reformulación completa de las políticas |
| 2.0 | 30 de agosto de 2018 | Aprobación del Gerente del Banco Central de Costa Rica | Se incorpora el lineamiento L-3.2.1 |
| 1.0 | 21 de junio de 2016 | Aprobación del Gerente del Banco Central de Costa Rica. | Emisión de las políticas. |

**Contenido**

# POLÍTICAS DE CIBERSEGURIDAD

## Consideraciones que sustentan la emisión de estas políticas específicas

A. La Junta Directiva, mediante el acuerdo JD-5681/05 del 10 de marzo del 2015, dispuso Ratificar lo resuelto por el Consejo Nacional de Supervisión del Sistema Financiero en el inciso I, artículo 14, del acta de la sesión 1150-2015, celebrada el 23 de febrero del 2015, modificado en lo que interesa, en el artículo 8, del acta de la sesión 1152-2015, del 2 de marzo del 2015, la integración de las dependencias - Departamentos de Informática o de Tecnologías de Información, según se les denomine en cada Superintendencia - junto con sus plazas, equipos y funcionarios, a la División Servicios Tecnológicos del Banco Central, con la finalidad de proveer la totalidad de los servicios de tecnologías de información de forma centralizada por parte del Banco Central.

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

C. El Control C-12.2. cuenta con un transitorio en su implementación y será de acatamiento obligatorio a partir del 30 de setiembre de 2024.

# I. ASPECTOS GENERALES

P-1. El Banco Central de Costa Rica establece como alcance de estas políticas los servicios brindados por la División Servicios Tecnológicos del Banco Central de Costa Rica (BCCR)[1] a la institución para velar por la adecuada gestión de la Seguridad Tecnológica y brindar una protección adecuada a los recursos de información de la institución custodiados mediante la plataforma tecnológica.

P-2. Con el fin de procurar la adecuada interpretación de los aspectos relacionados con la Seguridad Tecnológica, se definen los siguientes términos:

Este documento aplica para la institución Banco Central de Costa Rica (BCCR). Tanto el nombre como las siglas son utilizados indistintamente. Cuando en el documento se indique Banco Central, Banco Central de Costa Rica o BCCR, debe interpretarse como Banco Central, todos sus organismos de desconcentración máxima (SUGEF, SUGEVAL, SUPEN, SUGESE) y el Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF).

| | |
|---|---|
| **a) Activo** | Cualquier cosa que tenga valor para la institución, entre ellos:<br>i. ***Activos de información (***sinónimo de ***Información)***: todo aquello que tenga valor informativo para la organización, con respecto a la Seguridad de la Información.<br>ii. ***Activos de software***: software de aplicación, software de sistemas, herramientas de desarrollo, utilitarios y otros elementos lógicos pertenecientes a la infraestructura tecnológica.<br>iii. ***Activos tecnológicos físicos***: computadoras, equipos de comunicaciones, medios removibles y otros elementos físicos pertenecientes a la infraestructura tecnológica.<br>iv. ***Servicios tecnológicos***: servicios de procesamiento y comunicaciones.<br>v. ***Recursos humanos:*** *persona o grupo de personas.* |
| **b) Ambiente** | Combinación de hardware y software para realizar una tarea o una serie de tareas específicas. Generalmente existen ambientes de pruebas, ambientes de desarrollo, ambientes de pre-producción y ambientes de producción. |
| **c) Autenticación** | Es el acto o proceso de confirmar que algo o alguien es quien dice ser. |
| **d) Cuenta de usuario** | Una cuenta de usuario es una colección de información que identifica a un usuario particular. |

[1] Debe interpretarse como Banco Central, todos sus organismos de desconcentración máxima (SUGEF, SUGEVAL, SUPEN, SUGESE) y el Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF).

| | |
|---|---|
| **e) Cuenta de administración** | Una cuenta de administración es una cuenta de usuario con permisos especiales para tareas de gestión de operaciones de seguridad, software, hardware, telecomunicaciones y sistemas. Son para uso exclusivo de los empleados que por sus funciones así lo requieran. |
| **f) Cuenta de administración local** | Cuenta de administrador creada para su uso exclusivo dentro de un servidor, computadora o equipo de red específico. |
| **g) Cuenta privilegiada** | Una cuenta privilegiada es una cuenta que, en virtud de su función se le ha garantizado acceso especial a sistemas de información y/o recursos de red, tal acceso es de mayor función que aquellas que comúnmente se asignan a otros usuarios en los sistemas. Se administra mediante un sistema de gestión de cuentas privilegiadas. |
| **h) Cuenta de recuperación** | Una cuenta de recuperación es una cuenta privilegiada, que se le asignan funciones administrativas para cambiar contraseñas en el sistema o recurso de red destino. Su objetivo principal es permitir que el sistema de gestión de cuentas privilegiadas se adueñe de forma automática de cuentas privilegiadas en el proceso de verificación y/o de cambio de contraseña regular. |
| **i) Cuenta de servicios** | Una cuenta de servicios es una cuenta que no utilizan los usuarios, sino que son utilizadas como identidad por los sistemas para ejecutar aplicaciones. |
| **j) Datos personales de acceso restringido** | Los datos personales que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.[2] |
| **k) Devolución de una base de datos** | Cuando el Administrador de Bases de Datos restaura de forma total o parcial una base de datos del entorno de producción organizacional, siguiendo los procedimientos establecidos para atender soporte interno o continuidad de negocio, o como alternativa de "reversión" en la gestión de cambios para las soluciones tecnológicas, y solamente por los medios y con las herramientas autorizadas en la institución. |
| **l) Dispositivo o equipo móvil** | Cualquier elemento electrónico no fijo con capacidad de registrar, almacenar y/o transmitir datos, voz, video o imágenes, incluyendo entre ellos a computadoras portátiles, teléfonos celulares, tabletas (tablets), entre otros. |
| **m) Dispositivo móvil institucional** | Dispositivo móvil que es propiedad de la institución y que fue entregado a un funcionario para el desarrollo de sus labores. |
| **n) Dispositivo móvil personal** | Dispositivo móvil que es propiedad de un funcionario, y que el funcionario de forma voluntaria decide disponer del mismo para el desarrollo de sus labores dentro y fuera de la institución. |

[2] Ley N. ª 8968 Protección de la Persona frente al tratamiento de sus datos personales, artículo 3, inciso d.

| | |
|---|---|
| **para fines laborales** | |
| **o) Información Crítica** | Información que es indispensable para la operación de los negocios de la institución. |
| **p) Información de acceso restringido** | Información que solo puede ser conocida por las personas autorizadas dentro de la institución y que está clasificada de acuerdo con los niveles de confidencialidad especificados en las Políticas Específicas de Seguridad de la Información como: Uso Interno, Propietario, Confidencial y Máxima Seguridad. |
| **q) Mecanismos fuertes de autenticación** | Son mecanismos de control de acceso informático en el que a un usuario se le concede acceso al sistema solo después de que presente dos o más pruebas diferentes de que es quien dice ser. Estas pruebas pueden ser diversas, como una contraseña, que posea una clave secundaria rotativa, características biométricas, un certificado digital instalado en el equipo, entre otros. |
| **r) Modificación directa a una base de datos** | Cuando el Administrador de Bases de Datos aplica un cambio de manera manual sobre la información de una base de datos del entorno de producción organizacional, siguiendo los procedimientos establecidos para atender soporte interno o continuidad de negocio para las soluciones tecnológicas, y solamente por los medios y con las herramientas autorizadas en la institución. |
| **s) Necesidad de saber** | Principio utilizado para la definición de perfiles de usuario según el cual a éste se le deben asignar los permisos estrictamente necesarios para tener acceso a aquella información que resulte imprescindible para la realización de su trabajo. |
| **t) Parchado** | Proceso para aplicar cambios a un programa para corregir errores, agregarle funcionalidad, eliminarle funcionalidad o actualizarlo. |
| **u) Privilegio Mínimo** | Reducción de los privilegios de la cuenta de usuario al mínimo necesario para el desempeño de sus funciones, con el fin de mitigar el impacto de cualquier fallo, accidente o vulnerabilidad en los sistemas. |
| **v) Proceso de endurecimiento (Hardening)** | Proceso para asegurar un sistema mediante la mitigación de vulnerabilidades y reducción de su superficie de ataque. |
| **w) Repositorio seguro** | Ubicación lógica dentro de un almacenamiento o sistema informático el cual ha sido protegido mediante técnicas de cifrado de última generación vigentes y actualizadas, al cual se le aplican procesos de autenticación y autorización robusta. |
| **x) Rol** | Conjunto de privilegios de acceso a la información en los diferentes sistemas o dispositivo en la que esta se almacene. |

| | |
|---|---|
| **y) Sesión de sistema operativo** | Intercambio de información interactiva entre el sistema operativo y el usuario, este último debe autenticarse para poder iniciar la sesión y que el sistema operativo configure el entorno de trabajo. |
| **z) Sistema** | Un sistema informático es un entorno que permite almacenar y procesar información; es el conjunto de partes interrelacionadas: hardware y software. El hardware incluye computadoras o cualquier tipo de dispositivo electrónico, que consisten en procesadores, memoria, sistemas de almacenamiento externo, etc. El software incluye al sistema operativo y aplicaciones. |
| **aa) Sistema Crítico** | Sistema que fue definido como crítico por su importancia para el negocio, por lo que debe operar en caso de un evento de impacto medio o bajo. El sistema crítico ha sido establecido como tal en el Plan de Continuidad o en el Catálogo de Servicios. |
| **bb) Sitio no clasificado** | Sitio web que no ha sido categorizado por una herramienta de filtrado web. |

## II. ASPECTOS OPERATIVOS

# CONTROL DE ACCESOS.

P-3. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, establece controles de acceso a todos sus activos, para prevenir el acceso y divulgación no autorizada de información. Estos controles se establecen de acuerdo con los requerimientos del negocio y de seguridad, estableciendo mecanismos para mantener los principios de privilegio mínimo, necesidad de saber y separación de funciones.

C-3.1. Cuando se accede a los diferentes activos del Banco Central de Costa Rica, la División Servicios Tecnológicos implementa mecanismos de seguridad que procuran que dichos activos son accedidos solo por personal autorizado por medio del respeto de los siguientes lineamientos:

L-3.1.1. El BCCR podrá utilizar los datos personales considerados de acceso restringido para implementar controles de seguridad y operativos de las soluciones tecnológicas. No obstante, dichos datos no serán publicados ni utilizados fuera de la infraestructura del BCCR sin previo consentimiento del empleado.

L-3.1.2. Las cuentas de usuario son únicas, personales e intransferibles.

L-3.1.3. Debe utilizarse un nombre de usuario diferente para las cuentas de usuario, de administración, privilegiadas, de recuperación y de servicio, para ello las cuentas de administración tienen el prefijo ca_, las cuentas privilegiadas el prefijo cp_, las cuentas de recuperación tienen el prefijo cr_, las cuentas de servicio el prefijo cs_, y las cuentas de usuario no tienen prefijo.

L-3.1.4. La cuenta de cada usuario posee únicamente los privilegios necesarios para poder cumplir con las funciones y responsabilidades del puesto y/o tareas especiales que éste desempeña.

L-3.1.5. Las cuentas de administración poseen los privilegios necesarios para poder cumplir con las funciones y responsabilidades del puesto y/o tareas especiales que desempeña y serán utilizadas únicamente cuando se necesiten. Estas cuentas se asignan a los empleados que según sus funciones así lo requieran, respetando los principios de privilegio mínimo y necesidad de saber.

L-3.1.6. Las cuentas privilegiadas poseen permisos especiales necesarios para poder cumplir con funciones y/o tareas especiales que desempeña en sistemas muy específicos y serán utilizadas únicamente cuando se necesiten. Estas cuentas se asignan a los empleados que según sus funciones así lo requieran, respetando los principios de privilegio mínimo y necesidad de saber.

L-3.1.7. Cada vez que una sesión de sistema operativo de un usuario final asociada a un funcionario del BCCR cumpla con el tiempo de inactividad establecido por la División Servicios Tecnológicos, el sistema habilitará el protector de pantalla institucional, el cuál además bloqueará la sesión automáticamente.

L-3.1.8. Los sistemas internos del BCCR estarán disponibles para su uso las 24 horas del día, todos los días del año, respetando las condiciones de acceso que posee cada usuario.

L-3.1.9. Cuando se identifica que una cuenta de usuario se ha visto comprometida, el evento se tratará como un incidente de seguridad tecnológica y se gestionará de acuerdo con lo establecido en el Proceso de atención de incidentes de seguridad tecnológica.

L-3.1.10. Las cuentas de usuarios que no presenten actividad por más de un (1) mes, serán desactivadas.

L-3.1.11. El personal que por sus funciones requiere trabajar en más de un ambiente, dispondrá de cuentas de usuario distintas para cada ambiente.

C-3.2. Para la administración de contraseñas, la División Servicios Tecnológicos implementa mecanismos para velar que los lineamientos establecidos para el uso y administración de las contraseñas se cumplan.

L-3.2.1. La persona funcionaria deberá dar preferencia al uso de mecanismos fuertes de autenticación antes que el basado en contraseñas, en los dispositivos que así lo soporten técnicamente.

L-3.2.2. Las contraseñas no se deben almacenar en formatos legibles, en ningún medio electrónico o impreso, salvo que se encuentren protegidas por otros mecanismos (por ejemplo, cajas fuertes o repositorios seguros).

L-3.2.3. Las contraseñas que correspondan a cuentas de servicio serán administradas por el área responsable y solamente deben ser utilizadas por los servicios para los que fueron creadas.

L-3.2.4. Las contraseñas que correspondan a cuentas de recuperación serán de uso exclusivo del sistema de gestión de cuentas privilegiadas y solamente deben ser utilizadas para su propósito de recuperación de credenciales.

L-3.2.5. Las contraseñas de cuentas de servicio y cuentas de administración locales de equipos de red no vencerán, pero serán renovadas en caso de verse comprometidas cuando se determine mediante un incidente de seguridad que esto ha sucedido o en caso de la salida de miembros del área que administra la contraseña.

L-3.2.6. Las contraseñas deberán estar conformadas por al menos 12 caracteres, que deben incluir al menos tres de las siguientes características: letras minúsculas, mayúsculas, números y caracteres especiales.

L-3.2.7. Las contraseñas de las cuentas en los ambientes de producción deberán cambiarse al menos una (1) vez en los periodos que se establecen a continuación:

a) Cuentas de usuario: 60 días.
b) Cuentas de administración: 60 días.
c) Cuentas privilegiadas: 20 días o cuando se realice una acción de visualización de contraseña mediante el sistema de gestión de cuentas privilegiadas.
d) Cuentas de recuperación: 20 días o cuando se realice una acción de visualización de contraseña mediante el sistema de gestión de cuentas privilegiadas.
e) Cuentas de administración local en los servidores: 180 días.
f) Clave (PIN) telefónico: 90 días.
g) Otros equipos administrados por personal de la DST: 180 días.

L-3.2.8. Todas las contraseñas por defecto que traigan los dispositivos tecnológicos adquiridos por el BCCR, deberán ser cambiadas durante su configuración inicial por el responsable de la administración del dispositivo o por el personal responsable de su administración.

L-3.2.9. Las cuentas de usuario deberán bloquearse luego de un máximo de cinco (5) intentos no exitosos de ingreso de la contraseña. Luego de 10 minutos, una cuenta bloqueada por este motivo podrá desbloquearse automáticamente. Las cuentas de servicio y cuentas con previa justificación estarán exentas de este bloqueo.

L-3.2.10. Ante el ingreso de una nueva persona usuaria a la institución, o cuando una actual olvide su contraseña, se deberá generar una contraseña temporal, la cual deberá ser cambiada en el momento que la persona ingresa a los sistemas de la institución por primera vez o luego del cambio producto del olvido.

L-3.2.11. Para los usuarios que cuenten con teléfono físico, cuando ingresan por primera vez a la institución, o cuando se les olvide el PIN (clave de acceso), se deberá generar un PIN temporal, el cual deberá ser cambiado en el momento que el funcionario ingrese al teléfono de la institución por primera vez o luego del cambio.

L-3.2.12. Para realizar un cambio o reinicio de contraseña para un usuario, éste debe contactar a la Mesa de Ayuda de la DST

quien debe validar la identidad del solicitante por medio de datos comprobables previo a realizar el cambio.

L-3.2.13. No está permitida la inclusión de contraseñas en texto plano, es decir fácilmente identificables, como parte del código fuente del software que esté siendo desarrollado, modificado, administrado o adquirido por el BCCR.

L-3.2.14. Al cambiar su contraseña, el usuario responsable no podrá reutilizar al menos las últimas 6 contraseñas anteriores o según lo defina el Departamento de Ciberseguridad.

P-4. El Banco Central de Costa Rica por medio de la División Servicios Tecnológicos, establece los siguientes mecanismos para controlar la creación, modificación y eliminación de usuarios de los sistemas de información, así como la asignación, modificación y revocación de privilegios a los usuarios, siguiendo los principios de privilegio mínimo y necesidad de saber de cada usuario para prevenir cualquier acceso no autorizado.

C-4.1. Para apoyar la debida segregación de funciones y el principio de privilegio mínimo, la División Servicios Tecnológicos implementa herramientas que administran la creación, modificación y eliminación de usuarios, así como la asignación y revocación de privilegios.

L-4.1.1. La asignación de roles en herramientas tecnológicas (que corresponden con los roles otorgados a los funcionarios por cada negocio) debe contar con la autorización expresa de la jefatura inmediata, ya sea que la asignación sea automática y aprobada directamente por ésta, o bien, que la jefatura inmediata solicite las asignaciones a un administrador técnico de la herramienta tecnológica.

L-4.1.2. Para la creación de cuentas de usuario que pertenezcan a personal temporal externo a la institución, incluyendo, pero no limitado a consultores, pasantes, auditores o desarrolladores; la persona que supervise las actividades de estos usuarios deberá solicitarlos a través de la Mesa de Ayuda.

La información obligatoria para la creación de dichos usuarios es la siguiente:

a) Nombre completo.
b) Número de identificación (Nacional, Extranjera, Pasaporte).
c) Nombre de la empresa para la que trabaja.

d) Dirección de correo electrónico de la empresa para la que labora.
e) Número de teléfono de la empresa.
f) Ubicación geográfica (País, provincia o estado).
g) Periodo de vigencia de la cuenta de dominio (Fecha inicial y final).

P-5. El Banco Central de Costa Rica establece que ninguna persona funcionaria debe compartir las contraseñas de usuario final por ningún motivo, a fin de impedir el acceso no autorizado a las soluciones disponibles.

P-6. El Banco Central de Costa Rica establece que cada funcionario es responsable por toda la actividad que se genere con sus credenciales de usuario, con el fin de establecer la autoría de los accesos y transacciones realizados. Lo anterior aplica de igual manera en aquellas cuentas de usuario compartidas que utilice en conjunto con otros funcionarios.

P-7. El Banco Central de Costa Rica por medio de la División Servicios Tecnológicos, cuenta con mecanismos para proteger el proceso de autenticación y la gestión de sesiones inactivas en los sistemas de la institución, con el fin de facilitar los accesos que correspondan a cada usuario.

C-7.1. El Departamento de Infraestructura Tecnológica implementa servicios de directorios que permiten la gestión centralizada y estandarizada de usuarios y sus credenciales, así como los procesos de autenticación requeridos en las estaciones o servidores de la institución.

C-7.2. El Departamento de Infraestructura Tecnológica desconecta por seguridad, luego de un periodo de inactividad, todas las sesiones interactivas o remotas que se establezcan hacia los servidores y equipos de red, que soportan los sistemas críticos del Banco Central de Costa Rica.

L-7.2.1. El período de inactividad para desconexión en los servidores y equipos de red será establecido por el Departamento de Ciberseguridad del BCCR, según las buenas prácticas de la industria.

P-8. El Banco Central de Costa Rica por medio de la División Servicios Tecnológicos, implementa mecanismos para prevenir la fuga de información de acceso restringido, así como el acceso no autorizado a los datos gestionados mediante los sistemas de información institucionales.

C-8.1. La División Servicios Tecnológicos, requiere que los administradores de la información de la Unidad de Negocio generen y aprueben una solicitud formal cada vez que se solicite información de acceso restringido, se solicite una modificación directa o devolución a las bases de datos de

producción, o se asignen roles para acceder a los sistemas del Banco Central de Costa Rica.

L-8.1.1. El acceso a las bases de datos de la institución se permite para los siguientes tipos de usuarios:

a) Administrador de Base de Datos: Este tipo de usuario tiene control total de las bases de datos. Solamente miembros designados en el Departamento de Ciencia e Ingeniería de Datos se incluyen en este tipo de usuario.
b) Personal de Soporte: Este tipo de usuario tiene solamente permisos de lectura sobre las bases de datos u objetos de datos para los cuales brinda soporte según sus roles y funciones.
c) Usuario de Cuentas de Servicios: Usuario genéricos de las aplicaciones y utilizado para impersonalizar el acceso de los usuarios propios de la aplicación.
d) Usuario de aplicaciones de infraestructura cliente-servidor, que por el diseño de esta requieren ser creados como cuentas para los usuarios de la aplicación. Tendrán los accesos mínimos requeridos para el funcionamiento de la aplicación en cuestión.

L-8.1.2. El acceso de los usuarios a las bases de datos se permitirá solamente por los medios y herramientas autorizadas en la institución. La creación de dichos usuarios debe respetar lo siguiente:

a) La solicitud de creación de toda cuenta de usuario en las bases de datos de producción o en ambientes que contienen información de producción que no ha sido sometida al proceso de saneamiento de esta, deberá ser registrada en un caso de soporte y en el mismo se deberá incluir la justificación y autorización respectiva.
b) La creación de cuentas de usuario, necesarias para la puesta en marcha de un proyecto de desarrollo de software deberán ser registrados como un script de base de datos y sometidos al flujo normal de liberación de este por todos los ambientes de desarrollo, pruebas y producción.
c) No se permite acceso anónimo a las bases de datos. Esto incluye uso de usuarios genéricos administradores del motor de base de datos

(ejemplo: la cuenta sa), los cuales solamente se podrán mantener para planes de contingencia o recuperación y no para uso regular de usuarios administradores de base de datos, quienes deberán tener una cuenta que los identifique de manera personal.

d) Se permite la impersonalización del usuario de base de datos para una aplicación. Esto es delegar a la aplicación la identificación, autenticación y autorización del usuario del sistema y conectarse desde los componentes de la aplicación por medio de un usuario genérico para la misma. Si se realiza la impersonalización, la aplicación debe contar con una bitácora de eventos que registre y permita determinar las operaciones que está realizando cada uno de los usuarios a nivel aplicativo en el sistema.
e) Las conexiones a base de datos deben ser establecidas con modo de autenticación integrada de Windows, siempre que a nivel aplicativo y de infraestructura sea posible y que el motor de base de datos lo permita.
f) En caso de que se requieran usuarios propios del motor de base de datos, para la gestión de sus contraseñas se deben aplicar automáticamente las mismas políticas aplicables para las cuentas de usuario regulares.

L-8.1.3. La información de acceso restringido almacenada en las bases de datos de la institución debe estar claramente identificada, y para su manipulación se deben cumplir con lo siguiente:

a) Debe documentarse formalmente de manera detallada la información de acceso restringido que se debe proteger. En la confección de esta documentación participan tanto expertos de las áreas de tecnología, como expertos de las áreas de negocio del sistema.
b) La información anterior se utilizará para alimentar un proceso automático que sanea (ensucia) los datos de las bases de datos del sistema. El objetivo de este proceso es borrar, sustituir o modificar en los ambientes de prueba, desarrollo o similar, todo

aquel dato que se considere de acceso restringido, sustituyéndolo por un dato codificado.

c) El proceso anterior es aplicado en las bases de datos de los ambientes de prueba, desarrollo o similar, toda vez que se restauren datos de producción en dichos ambientes.
d) En el caso que se requiera mantener información de acceso restringido en un ambiente diferente al de producción, esta situación deberá ser justificada, aprobada y documentada por medio de un mecanismo oficial de registro de este tipo de requerimientos. Una vez que la situación que derivó la necesidad de mantener información de acceso restringido en un ambiente diferente al de producción desaparezca, los datos de acceso restringido deberán ser saneados o eliminados del ambiente correspondiente.
e) En el caso en que la situación anterior sea de carácter técnico o de negocio, el encargado de dar la aprobación será siempre el administrador de la información de la Unidad de Negocio.
f) Cualquier solicitud de información almacenada en las bases de datos de producción de la institución deberá ser justificada por escrito y aprobada por el responsable del activo de información.

L-8.1.4. Al realizar modificaciones directas a las bases de datos organizacionales, el encargado de dar la aprobación será siempre el administrador de la información de la Unidad de Negocio, indistintamente que la solicitud sea de carácter técnica o de negocio.

C-8.2. La División Servicios Tecnológicos brindará un mecanismo para que periódicamente, los administradores de la información de las distintas unidades de negocio puedan analizar las modificaciones directas realizadas a las bases de datos bajo su responsabilidad. El objetivo de este análisis es ayudar a la Unidad de Negocio a identificar los potenciales riesgos en sus operaciones y tomar las medidas correctivas que estime adecuadas para gestionar dichos riesgos.

C-8.3. La División Servicios Tecnológicos, implementa control de acceso en la asignación de roles técnicos para acceder a los sistemas críticos del Banco Central de Costa Rica, a través de una solicitud a la Mesa de Ayuda

aprobada y registrada por la administración correspondiente, de manera que se reduzca el riesgo de accesos y modificaciones no autorizadas.

P-9. El Banco Central de Costa Rica, mediante la División Servicios Tecnológicos, mantiene mecanismos para procurar que los usuarios tanto internos como externos solo tengan acceso a los sistemas específicamente autorizados para prevenir el acceso y la divulgación no autorizada de la información de la institución.

C-9.1. La División Servicios Tecnológicos, implementa control de acceso a los usuarios tanto internos como externos que acceden a los sistemas del Banco Central de Costa Rica de manera que se reduzca el riesgo de accesos y modificaciones no autorizadas.

L-9.1.1. Los usuarios que requieren el uso de dispositivos de seguridad exclusivos para el acceso a las aplicaciones específicas (tokens de seguridad) serán responsables de su uso adecuado.

L-9.1.2. Cuando no se estén utilizando, los dispositivos de seguridad anteriores deberán ser debidamente custodiados o almacenados bajo llave, por los usuarios responsables de ellos, y nunca deberán permanecer conectados al equipo cuando el usuario se ausente de la estación de trabajo.

L-9.1.3. Los dispositivos de seguridad anteriores son de uso personal y no deberán compartirse con otros usuarios por ninguna circunstancia.

## CIFRADO.

P-10. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, establece el uso de técnicas criptográficas para la protección de su información de acceso restringido que reside en la infraestructura tecnológica, con el fin de asegurar su confidencialidad, autenticidad e integridad.

C-10.1. Para todo sistema, transacción de comercio electrónico, o comunicación con entes externos, la División Servicios Tecnológicos configura canales cifrados seguros (sesiones HTTPS, sesiones autenticadas con certificados digitales en una o dos vías) para realizar dichas transacciones, y reducir el riesgo de divulgación o alteración de los datos.

L-10.1.1. El tamaño de las llaves (simétricas y asimétricas), algoritmo de resumen (hash) y demás atributos criptográficos, deben estar acorde con la practica internacional y ser

considerados robustos, es decir no deben utilizarse mecanismos considerados inseguros o vulnerables.

C-10.2. Para todo sistema que almacene o procese información considerada de máxima seguridad o cuando los acuerdos, leyes y regulaciones vigentes lo determinen, la División Servicios Tecnológicos implementa controles de cifrado de datos para reducir el riesgo de divulgación de los datos en caso de robo o pérdida de estos. Asimismo, se establecen métodos para la recuperación de información cifrada y la protección de las llaves correspondientes.

C-10.3. La División Servicios Tecnológicos configura los servicios que ofrece el Banco Central de Costa Rica y que así lo requieran, con firma digital como mecanismo de autenticación, y además verifica la autorización del usuario, de manera que se reduce el riesgo de transacciones no autorizadas y se resguarda la integridad de los datos en dichas transacciones.

## SEGURIDAD FÍSICA Y AMBIENTAL.

P-11. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, protege los equipos tecnológicos, conexiones de telecomunicaciones y eléctricas para reducir los riesgos ambientales, de pérdida, de daño, de robo, de interrupción y de oportunidades de acceso no autorizado, ubicándolos en zonas de seguridad adecuadas, brindándoles el mantenimiento adecuado, previniendo las fallas de suministros eléctricos.

C-11.1. Es responsabilidad del Departamento de Infraestructura Tecnológica que todo servidor y equipo de red que soporte directamente el procesamiento de información sea ubicado en un centro de datos debidamente equipado, que cuente con suministro de electricidad adecuada, control de acceso físico y mecanismos para controlar la temperatura y humedad, de manera que se reduzca la posibilidad de daños causados por el ingreso de personas no autorizadas o cambios en la climatización.

L-11.1.1. Es responsabilidad de todo funcionario la debida custodia del dispositivo de acceso físico (llaves físicas, tarjeta de acceso) que le ha sido asignado para proteger el acceso a las áreas seguras.

C-11.2. Es responsabilidad del Departamento de Infraestructura Tecnológica en conjunto con el Departamento de Servicios Institucionales mantener áreas seguras fuera del centro de datos (cuartos de cableado y telecomunicaciones) con controles preventivos, perímetros de seguridad

física definidos, control de acceso y controles de tipo disuasivo; para ubicar equipos y dispositivos que procesan información crítica o de acceso restringido.

L-11.2.1. Los cuartos de cableado y telecomunicaciones se protegen con control de acceso automatizado. Este control únicamente permite el ingreso a personal del Departamento de Infraestructura Tecnológica o personal de soporte del Departamento TI de Colaboración. El personal autorizado puede ingresar acompañado por personal de terceros, que por las funciones que deben realizar requieran acceso.

L-11.2.2. Los trabajos de mantenimiento o reemplazo de equipos, cableado o cualquier otro dispositivo que se encuentre en un área segura, por parte de terceros o personal del BCCR, son supervisados por personal del Departamento de Infraestructura Tecnológica.

L-11.2.3. El sistema de control de acceso almacena en bitácora los intentos exitosos y fallidos de ingreso a las áreas seguras. Dichos registros se guardan por espacio de 1 mes como mínimo.

L-11.2.4. Las áreas seguras cuentan con monitoreo de CCTV (Circuito Cerrado de Televisión). Debe existir un registro para que los visitantes anoten su ingreso. Para el personal interno, en caso de que no exista acceso controlado de forma electrónica o si el mismo no mantiene una bitácora, deberán de igual forma llenar la bitácora física. Este registro deberá ser resguardado para revisión en caso de presentarse alguna situación anormal.

L-11.2.5. Se deberá eliminar los derechos de acceso a las personas que dejan de laborar para la institución o cambian de funciones al momento en que esta situación sea comunicada por el Departamento de Gestión del Talento Humano.

## SEGURIDAD EN LA OPERATIVA.

P-12. El Banco Central de Costa Rica procura que toda manipulación, procesamiento, almacenamiento y comunicación de la información, que reside en la infraestructura tecnológica de la institución se hace a través de mecanismos seguros y de forma consistente para prevenir la divulgación no autorizada o uso inadecuado de los activos de información de la institución.

C-12.1. El Banco Central de Costa Rica establece mecanismos robustos para administrar el intercambio de información y software en la institución y con otras organizaciones manteniendo los principios de privilegio mínimo y necesidad de saber, para prevenir la pérdida, modificación, divulgación o mal uso de dicha información.

C-12.2. El Banco Central de Costa Rica establece que la comunicación mediante la tecnología Bluetooth no está permitida, salvo la conexión de dispositivos periféricos tales como: mouse, teclado, audífonos y otros que se encuentren debidamente autorizados por el Departamento TI de Colaboración.

P-13. El Banco Central de Costa Rica previene la modificación, divulgación, eliminación, destrucción, o cualquier daño que le pueda ocurrir a los medios físicos como lógicos de la institución, para reducir el riesgo de divulgación no autorizada de la información o mal uso de los activos.

C-13.1. El Departamento de Infraestructura Tecnológica, elimina la información guardada en los medios de almacenamiento bajo su responsabilidad, que se reutilicen o desechen con el fin de prevenir fuga o divulgación no autorizada de información de acceso restringido.

C-13.2. El Departamento TI de Colaboración, elimina la información guardada en los medios de almacenamiento bajo su responsabilidad, que se reutilicen o desechen con el fin de prevenir fuga o divulgación no autorizada de información de acceso restringido.

C-13.3. La División Servicios Tecnológicos mantiene una debida protección sobre los documentos digitales del Banco Central de Costa Rica según su clasificación de confidencialidad, integridad y disponibilidad.

L-13.3.1. Cuando sea requerido y posible, los documentos que sean producto de un proceso de certificación o que se encuentren en repositorios oficiales del BCCR deberán ser etiquetados indicando el nivel de confidencialidad asignado acorde con las Políticas Específicas de Seguridad de la Información. La etiqueta aplica tanto para documentos digitales como físicos.

P-14. El Banco Central de Costa Rica establece mecanismos para implementar, mantener y administrar la entrega de servicios de terceros, con el fin de proteger los activos de información de la organización.

C-14.1. Cuando el Banco Central de Costa Rica reciba servicios de terceros, éstos son normados mediante el uso de Acuerdos de Nivel de Servicio que deberán estar contemplados como parte del contrato respectivo, con

el fin de asegurar razonablemente que los servicios brindados cumplen con los requerimientos especificados por el Banco Central de Costa Rica.

C-14.2. Cuando el Banco Central de Costa Rica contrate servicios de computación en la nube a través de terceros, estos serán normados mediante el uso de Acuerdos de Nivel de Servicio y siguiendo las mejores prácticas de la industria, que deberán ser contempladas como parte del respectivo contrato. Es responsabilidad del Departamento de Ciberseguridad definir los requerimientos correspondientes, con el fin de asegurar razonablemente los servicios recibidos.

P-15. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, concientiza en temas de ciberseguridad a los funcionarios de la institución que deberán participar de forma obligatoria, para que se informen de las responsabilidades que se les confiere al ser usuarios de la plataforma tecnológica, promoviendo la cultura de uso seguro de la tecnología.

C-15.1. El Departamento de Ciberseguridad, colabora en el proceso encargado de inducción ejecutado por la División Transformación y Estrategia, con el fin de informar a los nuevos funcionarios sobre temas de ciberseguridad.

C-15.2. El Departamento de Ciberseguridad, realiza sesiones de entrenamiento evaluadas, de forma periódica, basadas en temas relevantes del contexto de ciberseguridad vigente, con el fin de promover el uso seguro de la tecnología.

L-15.2.1. Se realiza al menos una (1) sesión de entrenamiento anual registrada y evaluada para los funcionarios de la institución, la participación se hará constar por los medios pertinentes.

P-16. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, evalúa y refuerza los conocimientos de ciberseguridad de los funcionarios de la institución con el fin concientizar acerca de los riesgos a los que se ven expuestos.

C-16.1. El Departamento de Ciberseguridad, realiza ejercicios de evaluación de ciberseguridad, con el fin de valorar el nivel de concientización individual e institucional.

L-16.1.1. Se realiza al menos un (1) ejercicio de evaluación anual interna de ciberseguridad. Si producto del ejercicio de evaluación se detectan brechas en el nivel de concientización institucional, se realizarán ajustes en el programa a fin de reforzar las competencias que presenten deficiencias.

C-16.2. El Departamento de Ciberseguridad, realiza campañas de reforzamiento de ciberseguridad, con el fin de brindar información de interés y vigente, asociada al uso de la tecnología.

L-16.2.1. Se realizan reforzamientos anuales internos de ciberseguridad en forma de noticias y boletines para los funcionarios de la institución. Los registros generados por los reforzamientos (correos electrónicos, boletines) se almacenarán electrónicamente en la herramienta de colaboración institucional (Intranet).

## Documentación de procedimientos de operación.

P-17. El Banco Central de Costa Rica establece todos los procesos que deben seguirse para la administración y operación tecnológica de la institución, y vela porque los mismos se encuentren documentados, estandarizados, actualizados y disponibles para los usuarios que están autorizados a accederlos.

C-17.1. Las labores operativas que se realizan en la División Servicios Tecnológicos se documentan en el Sitio de Calidad del Banco Central de Costa Rica, para facilitar una uniformidad en las operaciones críticas del Banco Central de Costa Rica.

C-17.2. El Departamento de Ciberseguridad realiza evaluaciones para medir el nivel de cumplimiento de las políticas, controles y lineamientos de la seguridad tecnológica definidos en el Banco Central de Costa Rica.

## Gestión de cambios.

P-18. El Banco Central de Costa Rica mantiene procesos formales de control de cambios para cuando se implementen mejoras o se solucionen problemas en una aplicación, paquete de software, infraestructura tecnológica o sistema de información.

C-18.1. Cuando se requiera realizar un cambio o actualización a los sistemas del Banco Central de Costa Rica se siguen los procesos establecidos en el sitio de Calidad situado en el repositorio oficial de la institución.

## Gestión de la capacidad.

P-19. El Banco Central de Costa Rica planifica de forma anticipada la disponibilidad de los recursos tecnológicos y sus capacidades para proyectar las necesidades futuras de sus sistemas y para minimizar el riesgo de falla en los sistemas de información de la institución.

C-19.1. La División Servicios Tecnológicos implementa mecanismos de monitoreo y capacidad de los servidores, equipos de red y bases de datos propiedad del Banco Central de Costa Rica, para procurar la disponibilidad de sus servicios críticos.

## Separación de ambientes de desarrollo, prueba y producción.

P-20. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos establece una debida segregación de ambientes para sus sistemas de información, manteniendo distintos entornos para desarrollo, pruebas y producción; para reducir el riesgo de modificaciones accidentales o no autorizadas y de usos inadecuados de los activos de la institución.

C-20.1. Para cumplir con los principios de necesidad de saber y privilegio mínimo, el Departamento de Infraestructura Tecnológica implementa un debido control de accesos y asignación de privilegios según las labores que deba desempeñar cada funcionario, ayudando a reducir los riesgos de acceso, modificación, y utilización no autorizada de activos del Banco Central de Costa Rica.

P-21. El Banco Central de Costa Rica implementa controles para habilitar la separación de roles entre los funcionarios que realizan labores de desarrollo y soporte de aplicaciones e infraestructura tecnológica para prevenir accesos no autorizados y divulgación no autorizada de la información de la institución.

C-21.1. Para cumplir con los principios de necesidad de saber y privilegio mínimo, la División de Servicios Tecnológicos implementa un debido control de los accesos de los usuarios según su participación en el proceso de desarrollo y soporte, utilizando para ello las herramientas implementadas para el control de accesos.

## Protección contra código malicioso.

P-22. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos establece los mecanismos para prevenir, detectar y eliminar cualquier tipo de código malicioso en la plataforma tecnológica de la institución.

C-22.1. El Departamento de Infraestructura Tecnológica instala y mantiene actualizados, en todos los equipos del Banco Central de Costa Rica bajo su responsabilidad, aplicaciones y/o dispositivos que lo protegen de ataques de códigos maliciosos.

L-22.1.1. El Departamento de Infraestructura Tecnológica instala y configura herramientas que implementan filtrado y detección de amenazas en los medios electrónicos bajo su responsabilidad. Las recomendaciones y validaciones sobre estas herramientas se realizarán por parte del Departamento de Ciberseguridad.

C-22.2. El Departamento TI de Colaboración instala y mantiene actualizados, en todos los equipos del Banco Central de Costa Rica bajo su

responsabilidad, aplicaciones y/o dispositivos que lo protegen de ataques de códigos maliciosos.

L-22.2.1. El Departamento TI de Colaboración instala y configura herramientas que implementan filtrado y detección de amenazas en los medios electrónicos bajo su responsabilidad. Las recomendaciones y validaciones sobre estas herramientas se realizarán por parte del Departamento de Ciberseguridad

C-22.3. El Departamento de Ciberseguridad realiza periódicamente análisis de vulnerabilidades en los sistemas del Banco Central de Costa Rica, para reducir el riesgo de que la infraestructura se vea amenazada por la explotación de una vulnerabilidad presente en los sistemas.

C-22.4. El Departamento de Infraestructura Tecnológica realiza periódicamente procesos de parchado y actualización de aplicaciones en los equipos bajo su responsabilidad, con el propósito de prevenir posibles incidentes de seguridad por explotación de vulnerabilidades en los sistemas.

C-22.5. El Departamento TI de Colaboración realiza periódicamente procesos de parchado y actualización de aplicaciones en los equipos bajo su responsabilidad, con el propósito de prevenir posibles incidentes de seguridad por explotación de vulnerabilidades en los sistemas.

C-22.6. El Departamento de Infraestructura tecnológica implementa controles de acceso a Internet para todas las estaciones, servidores y usuarios, con el fin de cumplir con la reglamentación y leyes existentes y prevenir divulgación de información crítica o mal uso de los activos.

El Departamento de Infraestructura Tecnológica vela por el cumplimiento de los siguientes lineamientos:

L-22.6.1. Se proveerá acceso a Internet mediante las estaciones de trabajo brindadas por la organización a cada persona usuaria y dispositivos móviles de su propiedad.

L-22.6.2. Todo funcionario o persona que utilice el acceso a Internet a través de la infraestructura tecnológica del Banco Central estará sujeto al Lineamiento básico de acceso a Internet del Banco.

L-22.6.3. El Lineamiento básico de acceso a Internet establece lo siguiente:

a) Se prohíbe el acceso a sitios Web con contenido pornográfico.

b) Se prohíbe el acceso a sitios web cuyo contenido manifieste de cualquier manera, odio en contra de las creencias, orientación sexual, raza o lugar de origen u otra condición de discriminación.
c) Se prohíbe el acceso a sitios web cuyo contenido presente algún riesgo de seguridad a la infraestructura tecnológica del Banco Central, dicho riesgo será determinado por el Departamento de Ciberseguridad.
d) Siendo que el ancho de banda para acceso a Internet que utiliza el Banco Central es finito, en procura del buen uso de este activo, se limitará el ancho de banda utilizado por los funcionarios para navegar cualquier categoría o sitio que atente contra la disponibilidad del servicio de Internet para fines laborales.
e) El acceso a los sitios no clasificados (sin categoría) estará limitado por defecto.
f) Se permite el acceso a Internet a cualquier sitio que no esté afectado por los puntos anteriores.

L-22.6.4. Para apoyar el cumplimiento de esta política se implementan herramientas tecnológicas que clasifican los sitios de Internet según su contenido. Para la aplicación de estas políticas, la DST aceptará la clasificación de sitios web que realice el fabricante de los equipos de filtrado que utilice en su momento la Institución. Aquellos sitios a los cuales el lineamiento antes citado prohíba el acceso serán bloqueados. Las reglas de filtrado en esta herramienta estarán definidas con un alcance departamental como mínimo (un sitio o categoría se filtra para todos los usuarios de un departamento y no solo para algunos).

L-22.6.5. Reclasificación de sitios web: Cualquier funcionario podrá solicitar la reclasificación de un sitio web sin categoría o al considerarlo mal categorizado por la herramienta de filtrado a Internet. Estas solicitudes serán atendidas siguiendo las siguientes reglas:

a) Cuando se trate de sitios no clasificados, se realizará una solicitud a la Mesa de Ayuda de la División Servicios Tecnológicos, quienes ejecutarán sus procesos de clasificación de sitios no categorizados o escalarán el caso si es necesario.

b) Para reclasificación de sitios que se consideren mal clasificados o que hayan sido escalados por la Mesa de Ayuda, el Área de Telecomunicaciones analizará el sitio indicado en la solicitud. Si esta Área determina que dicho sitio no está cubierto por las prohibiciones indicadas en el Lineamiento básico de acceso a Internet lo clasificará en la categoría indicada o lo reclasificará. El Área de Telecomunicaciones podrá solicitar valoración y recomendación al Departamento de Ciberseguridad para la clasificación o reclasificación de sitios. Si luego de la valoración se determina que por su contenido el sitio analizado está afectado por las prohibiciones establecidas, la solicitud será rechazada.

L-22.6.6. Los directores de división o departamento podrán solicitar que se restrinja el acceso de sus funcionarios a determinados sitios web. La aplicación de estas restricciones se efectuará a nivel de departamento, como unidad mínima de administración de los sitios web y acceso de funcionarios.

C-22.7. La División Servicios Tecnológicos aplica procesos de endurecimiento (hardening) sobre la infraestructura de servidores de producción que soportan las operaciones críticas de la institución.

L-22.7.1. El proceso de endurecimiento de los servidores se realizará durante la instalación del software base, tomando en consideración las recomendaciones del fabricante y del Departamento de Ciberseguridad.

## Copias de seguridad de la información.

P-23. El Banco Central de Costa Rica por medio de la División Servicios Tecnológicos realiza copias de seguridad, para que la información digital y el software necesario para la operación de los procesos críticos de la institución, estén disponibles en caso de fallas, ataques o interrupciones.

C-23.1. La División Servicios Tecnológicos realiza periódicamente respaldos de la información que es utilizada o generada por los sistemas del Banco Central de Costa Rica, para procurar la disponibilidad e integridad de sus servicios críticos.

La División Servicios Tecnológicos vela por el cumplimiento de los siguientes lineamientos:

L-23.1.1. La información para respaldar, los periodos de retención y la periodicidad de ejecución de los respaldos será definida por los negocios responsables de dicha información. Para ello la División Servicios Tecnológicos documentará estos parámetros para cada tipo de información respaldada en la solución de respaldos institucional.

L-23.1.2. Cualquier información almacenada en las estaciones de trabajo de los funcionarios del BCCR, no será respaldada. Si el usuario o las dependencias requieren respaldos automáticos de sus archivos, deberán almacenarlos en la unidad de red o sección de la Intranet correspondiente.

L-23.1.3. Cuando se requiera respaldar información, fuera del ciclo normal de respaldos, o recuperar información de algún medio de respaldo, se sigue el proceso de Soporte Interno definido en el Sitio de Calidad de la institución.

L-23.1.4. Para las bases de datos, los respaldos de los sistemas críticos de la institución se copian en un servidor de respaldos cuya función es mantener un nivel de contingencia adicional al que por defecto posee el servidor de base de datos principal. Una vez copiados, los respaldos son restaurados en una base de datos contingente que se mantiene actualizada a un minuto de diferencia de la base de datos del servidor principal. Este esquema asegura que todos los respaldos realizados son apropiadamente restaurados y consecuentemente probados en un proceso automático de restauración.

L-23.1.5. No se deberá almacenar información personal en las unidades de red. Estos repositorios se utilizarán únicamente para almacenar y respaldar información con fines laborales.

L-23.1.6. Los datos almacenados en estos repositorios serán respaldados regularmente de acuerdo con las especificaciones establecidas para la Información de usuarios, por lo tanto, debido a los altos costos administrativos, no es factible la eliminación de datos específicos en los medios utilizados para respaldo de datos.

## Registro y gestión de eventos de actividad.

P-24. El Banco Central de Costa Rica cuenta con mecanismos para detectar actividades sospechosas, no autorizadas y posibles violaciones en el uso de los sistemas de

información provistos por la institución, realizadas tanto por usuarios privilegiados, como por usuarios regulares y no autorizados.

C-24.1. La División Servicios Tecnológicos implementa medidas legales y proporcionadas, para detectar y alertar de potenciales incidentes de seguridad que puedan afectar sus activos de información.

La División Servicios Tecnológicos vela por el respeto de los siguientes lineamientos:

L-24.1.1. La División Servicios Tecnológicos almacena de forma precisa y consistente las bitácoras que considere relevantes para colaborar en análisis posteriores que colaboren en el reforzamiento de los controles de seguridad.

L-24.1.2. Las bitácoras de los siguientes servidores deben al menos tener la retención que se indica a continuación:

a) Controladores de Dominio, 1 mes.
b) Bases de Datos, 6 meses.
c) Servidores ubicados en la DMZ que publican contenido en Internet, 1 mes.

L-24.1.3. Todo sistema crítico del BCCR donde se activen las bitácoras deberá registrar en sus bitácoras, como mínimo, la información que se indica a continuación:

**1. Servidores**

a) Usuario y/o máquina que generó evento.
b) Fecha y hora en que se generó el evento.
c) Tipo de evento o servicio.
d) Intentos fallidos y exitosos de acceso al sistema.
e) Intentos fallidos y exitosos de acceso a los recursos del sistema.
f) Uso de privilegios elevados.
g) Uso de utilidades y aplicaciones.
h) Cambios en las configuraciones de sistema.
i) Intentos de acceso y modificación de bitácoras.

**2. Equipo de Red**

a) Origen del evento (dirección IP).
b) Descripción del evento.
c) Si la conexión fue permitida o denegada.
d) Fecha y hora del evento.

**3. Máquinas de escritorio**

a) Modificaciones a las configuraciones del usuario.
b) Uso de utilidades y aplicaciones.

c) Uso de privilegios elevados.
d) Intentos fallidos y exitosos de acceso al sistema.
e) Intentos fallidos y exitosos de acceso a los recursos del sistema.

C-24.2. El Departamento de Infraestructura Tecnológica configura todos los equipos para el procesamiento de servicios críticos del Banco Central de Costa Rica para que sincronicen su reloj interno con la misma fuente común, para velar por la integridad de las transacciones.

C-24.3. La División Servicios Tecnológicos, implementa mecanismos para monitorear el estado de los sistemas críticos del Banco Central de Costa Rica, con el fin de mantener la disponibilidad, integridad y confidencialidad de la información.

C-24.4. La División Servicios Tecnológicos, implementa mecanismos para almacenar y analizar de forma precisa y consistente las bitácoras de los sistemas que soportan los sistemas críticos del Banco Central de Costa Rica, para colaborar en análisis posteriores que coadyuven en el reforzamiento de los controles de seguridad implementados.

## Gestión de Incidentes de Seguridad

P-25. El Banco Central de Costa Rica mantiene un proceso formal para la gestión de incidentes de seguridad tecnológica, que apoya el manejo rápido y consistente de incidentes de seguridad tecnológica para minimizar cualquier daño a las personas o a los activos de información del BCCR y reducir el riesgo de futuras brechas de seguridad.

C-25.1. La División Servicios Tecnológicos implementa un proceso de atención de incidentes de seguridad tecnológica con tareas y roles específicos para asegurar que tanto las sospechas, como los eventos e incidentes de seguridad tecnológica son reportados prontamente y escalados a las partes adecuadas con el fin de atender dichos reportes de manera apropiada.

L-25.1.1. Todos los usuarios del Banco Central de Costa Rica, tienen la obligación de reportar las sospechas, eventos o incidentes de seguridad tecnológica a la Mesa de Ayuda.

## Gestión de las vulnerabilidades técnicas.

P-26. El Banco Central de Costa Rica establece mecanismos para reducir los riesgos asociados al uso indebido intencional que pueda aprovechar las vulnerabilidades existentes, particularmente aquellas publicadas a nivel mundial, que afecten los diferentes sistemas que existen en la Institución.

C-26.1. El Departamento de Ciberseguridad realiza periódicamente análisis de vulnerabilidades en los sistemas críticos del Banco Central de Costa Rica, para reducir el riesgo de que la infraestructura se vea amenazada por la explotación de una vulnerabilidad presente en los sistemas.

C-26.2. El Departamento de Infraestructura Tecnológica realiza periódicamente procesos de parchado y actualización de software base de servidores, con el propósito de prevenir posibles incidentes de seguridad por explotación de vulnerabilidades en los sistemas.

C-26.3. El Departamento TI de Colaboración realiza periódicamente procesos de parchado y actualización de software base de equipos de usuario final, con el propósito de prevenir posibles incidentes de seguridad por explotación de vulnerabilidades en los sistemas.

## Restricciones en la instalación de software.

P-27. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos establece los procedimientos de instalación, custodia, uso y manejo del software, aplicaciones de escritorio y de los sistemas de información de la institución para mantener un adecuado nivel de seguridad.

C-27.1. La División Servicios Tecnológicos, con el propósito de proteger los activos de información del Banco, establece las Listas de Software Autorizado la cual contiene las aplicaciones y programas de software autorizados para su uso en las estaciones de trabajo de la Institución (equipos de escritorio y portátiles).

La División Servicios Tecnológicos vela por el cumplimiento de los siguientes lineamientos:

L-27.1.1. La Lista de Software Autorizado está publicada en la Intranet.

L-27.1.2. La Lista de Software Autorizado incluye el software mínimo (Software Base) que puede estar instalado en toda estación de trabajo de la Institución.

L-27.1.3. La Lista de Software Autorizado puede sufrir variaciones en cuanto a agregar, eliminar o actualizar elementos. Los pasos necesarios para mantener esta lista están establecidos en la guía “Mantenimiento de la Lista de Software Autorizado”.

L-27.1.4. Cualquier modificación que sufra la Lista de Software Autorizado para servidores, deberá ser autorizada por el Director del Departamento de Infraestructura Tecnológica, o por quien éste designe como encargado de dicha labor.

L-27.1.5. Cualquier modificación que sufra la Lista de Software Autorizado para equipos de usuario final, deberá ser autorizada por el director del Departamento de TI de Colaboración, o por quien éste designe como encargado de dicha labor.

L-27.1.6. El Departamento TI de Colaboración realiza periódicamente revisiones automáticas, con o sin previo aviso a todo el software instalado en las estaciones de trabajo de la Institución, con el propósito de detectar software no autorizado o que represente un riesgo para la institución.

L-27.1.7. Las revisiones periódicas de software se realizarán al menos una vez al año.

L-27.1.8. No está permitida la cancelación de los procesos automáticos utilizados para diagnosticar, revisar e inventariar el hardware y software instalado en los equipos computacionales de la Institución.

L-27.1.9. El software que no esté incluido en la Lista de Software Autorizado será eliminado del equipo donde se encuentre, sin responsabilidad por las consecuencias de tal eliminación.

C-27.2. Los equipos institucionales no deberán ser utilizados en entrenamientos, capacitaciones y cursos de índole técnica en donde se modifique la configuración, los controles de seguridad implementados o se instale software no autorizado. Para tal efecto cuando exista la necesidad justificada, el área interesada en la participación del funcionario en las actividades deberá solicitar recursos a la DST, especialmente configurados y preparados para este fin.

C-27.3. La División Servicios Tecnológicos no asume responsabilidad alguna por pérdidas o daños a información, archivos o programas ajenos al quehacer del Banco, que puedan producirse como resultado de sus esfuerzos por proteger los activos de información.

## Uso de dispositivos para movilidad.

P-28. El Banco Central de Costa Rica define, implementa y mantiene controles para procurar la protección, prevenir el acceso no autorizado y la divulgación no autorizada de la información que se almacena, procesa y transita por los dispositivos móviles controlados por la Institución.

C-28.1. El Departamento de TI de Colaboración implementa herramientas para la administración y el control de los dispositivos móviles utilizados

para fines laborales, con el fin de prevenir la divulgación, fuga o mal uso de información de acceso restringido de la institución.

L-28.1.1. Las portátiles que almacenen información de acceso restringido considerada de uso interno o un nivel superior de confidencialidad, cuentan con mecanismos de cifrado de almacenamiento.

L-28.1.2. Los dispositivos móviles que brinda la institución (computadoras portátiles, teléfonos inteligentes), cuentan con un certificado digital emitido por una Autoridad Certificadora interna, que será utilizado para identificar y autenticar el dispositivo en las distintas redes y sistemas.

L-28.1.3. La División Servicios Tecnológicos se reserva el derecho de determinar los dispositivos móviles que pueden ser utilizados para fines laborales.

L-28.1.4. Los funcionarios que deseen hacer uso de un dispositivo personal para fines laborales deberán solicitar su registro ante el Departamento de TI de Colaboración, con una solicitud a la Mesa de Ayuda de la DST con aprobación de su superior administrativo[3].

L-28.1.5. Al realizarse la solicitud de utilización de un dispositivo personal para fines laborales, el usuario deberá realizar la instalación de los programas y controles de seguridad que sean necesarios en sus dispositivos, el personal del Departamento de TI de Colaboración le indicará mediante una guía la configuración que debe realizar.

L-28.1.6. El usuario acepta y consiente que el Departamento de TI de Colaboración pueda:

a. Acceder a los datos de ubicación del dispositivo, con el fin de localizarlo cuando se encuentre perdido o haya sido objeto de robo.

b. Bloquear de forma remota el dispositivo.

c. Identificar las aplicaciones instaladas en el dispositivo, con el objetivo de determinar si existen aplicaciones

[3] No aplica en el caso de uso del correo institucional, el cual se regula en las Políticas específicas de Gestión de Información. Tampoco se incluyen aquellas aplicaciones que hayan sido definidas previamente como de libre acceso por parte de la institución

que representan riesgos de seguridad para la información del BCCR y Superintendencias.

d. Configurar de forma unilateral características de seguridad del dispositivo y su sistema operativo, con el objetivo de aumentar el nivel de protección de los datos almacenados en él.

e. Obtener y almacenar la siguiente información del dispositivo:

    i. Nombre de usuario
    ii. Correo electrónico
    iii. Número de teléfono
    iv. Tipo de dispositivo y modelo
    v. Versión del Sistema Operativo.
    vi. Operador.
    vii. Fecha/hora.
    viii. IMEI
    ix. Número de serie.
    x. Dirección MAC.
    xi. Almacenamiento utilizado/disponible.
    xii. ID de dispositivo.
    xiii. Nivel de la batería.

f. Borrar de forma unilateral las aplicaciones y los datos pertenecientes al BCCR y Superintendencias, en caso de sospecha de compromiso de la información, finalización del contrato laboral, o cuando se reduzca significativamente la seguridad inherente del dispositivo. Todas las demás configuraciones personales, aplicaciones y datos permanecerán en el dispositivo. La posibilidad de ejecutar esta acción está limitada al personal del Departamento de Ti de Colaboración.

g. Instalar aplicaciones y aplicar configuraciones para el uso de los sistemas en línea del BCCR, basado en roles

y responsabilidades de trabajo. Estas aplicaciones y configuraciones pueden ser removidas o modificadas en cualquier momento si cambian las responsabilidades del trabajo.

h. Enviar directamente al dispositivo, órdenes o comandos para procurar que las configuraciones y las aplicaciones estén actualizadas.

i. Suspender o desactivar de forma unilateral, los recursos y servicios utilizados para fines laborales a los que el usuario tenga acceso a través de su dispositivo móvil.

L-28.1.7. El funcionario que posea acceso a los recursos y servicios desde un dispositivo móvil tiene la responsabilidad de:

a. Salvaguardar toda la información del BCCR y Superintendencias que permanezca en el dispositivo móvil.

b. Informar sobre la pérdida del dispositivo móvil en el menor tiempo posible, a la Mesa de Ayuda.

c. Eliminar del dispositivo móvil toda la configuración de acceso a recursos y servicios del BCCR, antes de cambiarlo o deshacerse del mismo. De igual forma, deberá informar a la Mesa de Ayuda sobre el cambio del dispositivo.

d. Realizar la actualización periódica de aplicaciones y sistema operativo de su dispositivo móvil, así como acatar las indicaciones del personal del Departamento de TI de Colaboración o del Departamento de Ciberseguridad con respecto a configuraciones o actualizaciones de seguridad obligatorias.

## SEGURIDAD EN LAS TELECOMUNICACIONES.

P-29. El Banco Central de Costa Rica por medio de la División Servicios Tecnológicos define, implementa y mantiene controles para garantizar la confidencialidad, integridad y evitar la divulgación no autorizada de la información en su red, así como los datos que circulan por ella y los servicios que brinda.

C-29.1. Cuando se requiera proteger los datos que se transmiten a través de las redes, el área de Telecomunicaciones configura la segmentación de las

redes en los equipos que lo soportan, de acuerdo con las mejores prácticas de la industria, con el fin de evitar accesos no autorizados.

C-29.2. Los equipos y usuarios del Banco Central de Costa Rica se configuran y agrupan de acuerdo con sus funciones, de manera lógica, por el Departamento de Infraestructura Tecnológica con el fin de prevenir accesos y modificaciones no autorizadas, así como la propagación de amenazas tecnológicas.

El Departamento de Infraestructura Tecnológica tiene como objetivo garantizar el cumplimiento de los siguientes lineamientos:

L-29.2.1. Para las diferentes redes inalámbricas disponibles se deben aplicar las siguientes configuraciones:

a) Redes Inalámbricas Internas
   i. Solos los dispositivos administrados por la División Servicios Tecnológicos del Banco Central de Costa Rica deben conectarse a estas redes.
   ii. Los dispositivos en estas redes tendrán los mismos accesos y restricciones que las redes cableadas de los usuarios.
   iii. El método de autenticación utilizado será el Certificado Digital de la CA Interna, con una validez máxima de tres años y renovación automática.

b) Red Inalámbrica de Telefonía
   i. Solo los teléfonos IP inalámbricos administrados por la División Servicios Tecnológicos del Banco Central de Costa Rica y que soporten protocolos de autenticación autorizados por la DST deben conectarse a esta red.
   ii. Los dispositivos en esta red tendrán acceso únicamente a los sistemas y redes necesarios para establecer llamadas telefónicas.
   iii. Para la autenticación, se utiliza una cuenta local asignada a cada dispositivo.

c) Red Inalámbrica de Invitados.
   i. Dispositivos permitidos: Se permitirá el acceso a la red de dispositivos móviles de terceros que requieran acceso a Internet para realizar labores relacionadas con el BCCR.
   ii. Accesos permitidos: Los dispositivos conectados a esta red solo tendrán acceso a Internet, según con las políticas de navegación definidas por la institución para este servicio.

iii. Método de autenticación: El acceso a la red requerirá el uso de un nombre de usuario y contraseña, o, si es posible, la implementación de la autenticación multifactorial (MFA). Esta cuenta solo estará activa durante la estancia del invitado en la Institución. Todo usuario externo que necesite acceso a la red de invitados deberá solicitar al funcionario de la institución con quien se encuentre trabajando, la tramitación de sus credenciales.

d) Red para eventos especiales
   i. Dispositivos conectados a esta red: Esta red está diseñada para dispositivos de terceros no pertenecientes a la institución, que requieran acceso a Internet durante conferencias de prensa u otros eventos especiales organizados por el BCCR.
   ii. Accesos permitidos: Los dispositivos conectados a esta red tendrán acceso exclusivamente a Internet, siguiendo las políticas de navegación establecidas por la institución para este servicio.
   iii. Método de autenticación: La autenticación se llevará a cabo mediante una contraseña, la cual deberá ser modificada después de cada evento.

e) Red para colaboradores:
   i. Dispositivos permitidos: Se permitirá el acceso a la red a dispositivos de colaboradores que necesiten acceso a Internet para realizar labores relacionadas con el BCCR.
   ii. Accesos permitidos: Los dispositivos conectados a esta red solo tendrán acceso a Internet de acuerdo con las políticas de navegación definidas por la institución para este servicio.
   iii. Método de autenticación: El acceso a la red requerirá el uso de un certificado digital emitido por la CA interna de la institución.

C-29.3. Por defecto, se deniega el acceso a Internet para todos los servidores y equipos de infraestructura en general. Solo los servidores o equipos que requieran actualizaciones de firmas de antivirus, parches de seguridad o validación de licencias de software tendrán acceso a Internet. Cualquier otra aplicación o servicio que requiera una conexión permanente a Internet debe coordinarse con el Departamento de Ciberseguridad para evitar accesos no autorizados.

C-29.4. Solo el personal de Telecomunicaciones que utiliza equipos gestionados y autorizados por la División Servicios Tecnológicos puede acceder con privilegios de administrador para labores de gestión y soporte en los equipos de red en producción, administrados o propiedad del Banco Central.

C-29.5. Solo el personal de la División Servicios Tecnológicos, que utiliza equipos gestionados y autorizados por la División Servicios Tecnológicos puede acceder a los equipos de red en producción, administrados o propiedad del Banco Central, con los privilegios necesarios para realizar sus tareas, cumpliendo con los principios de privilegio mínimo y necesidad de saber.

P-30. El Banco Central de Costa Rica por medio de la División Servicios Tecnológicos establece controles sobre sus equipos de comunicación y cualquier acceso remoto que realicen los usuarios con el fin de prevenir el compromiso de la información de la institución.

C-30.1. Para el acceso remoto autorizado a las redes del Banco Central de Costa Rica, el Departamento de Infraestructura Tecnológica implementa protocolos seguros de comunicación, basados en las mejores prácticas de la industria, para garantizar la confidencialidad de la información.

C-30.2. Para el acceso remoto a los sistemas del Banco Central de Costa Rica, el Departamento de Infraestructura Tecnológica implementa mecanismos de autenticación robustos, de acuerdo con las mejores prácticas de la industria, para permitir únicamente el ingreso de usuarios autorizados a las redes institucionales de forma remota.

C-30.3. Para el acceso remoto autorizado a los sistemas del Banco Central de Costa Rica, el Departamento de Infraestructura Tecnológica implementa mecanismos de segmentación, siguiendo las mejores prácticas de la industria, para que los usuarios cumplan con los principios de privilegio mínimo y necesidad de saber.

C-30.4. Cuando se requiera acceder desde una red ajena a recursos ubicados en la red institucional, se debe establecer un canal seguro de comunicación desde el cliente origen hasta los recursos, para cumplir con los principios de integridad y confidencialidad de la información.

L-30.4.1. Cuando se requiera acceso para la administración de infraestructura tecnológica o de sistemas del Banco Central de Costa Rica, este se debe realizar desde una computadora portátil institucional, mediante la utilización de tecnologías como: VPN, VDI, portal de acceso remoto u otra modalidad de

conexión previamente aprobada por la División Servicios Tecnológicos.

L-30.4.2. Cuando se requiera acceso a la infraestructura o a los sistemas del Banco Central de Costa Rica, el Departamento de Infraestructura Tecnológica establece los canales desde los cuales se puede ingresar.

a) Desde una computadora portátil institucional, mediante la utilización de tecnologías como: VPN, VDI, portal de acceso remoto u otra modalidad de conexión previamente aprobada por la División Servicios Tecnológicos.
b) Desde una computadora personal o pública, utilizando un portal de acceso remoto o tecnologías de VDI.
c) Desde un cliente SINPE, Quiosco o Consola SINPE, utilizando un túnel VPN con autenticación mediante certificados digitales emitidos por la Autoridad Certificadora de Producción de SINPE o certificados digitales de Agente Electrónico emitidos por la Autoridad Certificadora de Persona Jurídica de SINPE.

### Intercambio de información con partes externas.

P-31. El Banco Central de Costa Rica protege las transacciones de comercio electrónico para prevenir transmisiones incompletas, enrutamientos erróneos, alteraciones o divulgaciones no autorizadas.

C-31.1. La División Servicios Tecnológicos incluye en sus contratos con terceros "Acuerdos de Confidencialidad" para prevenir la divulgación no autorizada de la información confidencial, cuando estos se consideren necesarios.

## ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.

P-32. El Banco Central de Costa Rica procura que los aspectos de seguridad son incorporados en los proyectos informáticos durante todas las etapas del ciclo de vida del desarrollo de sistemas o en la adquisición de paquetes de software para las aplicaciones del negocio, de manera que se mantenga un nivel adecuado de seguridad.

C-32.1. La División Servicios Tecnológicos recopila dentro de los requerimientos necesarios para poder satisfacer el objetivo del área

usuaria aquellos relacionados con la seguridad tecnológica, para todos los desarrollos de nuevas aplicaciones o mejoras a las existentes.

L-32.1.1. Las aplicaciones deben contemplar la administración de todos los controles de seguridad definidos en los requerimientos.

L-32.1.2. Todo proyecto de desarrollo interno o externo de aplicaciones informáticas deberá suscribirse a la metodología y estándares de seguridad definidos, para el desarrollo de sistemas de información en la institución.

P-33. El Banco Central de Costa Rica por medio de la División Servicios Tecnológicos establece que cada vez que se desarrolle un nuevo sistema o se aplique una mejora a los existentes, se utilicen criterios de aceptación para las pruebas que se realicen durante el desarrollo y antes de la puesta en marcha del sistema, validando datos de entrada y salida de las aplicaciones y reducir el riesgo de corrupción de datos, o de impacto a la confidencialidad, disponibilidad o integridad de los sistemas críticos de la institución.

C-33.1. Para todo nuevo sistema o mejora que se deba desarrollar en el Banco Central de Costa Rica, la División Servicios Tecnológicos aplica un plan de pruebas, para validar los datos de entrada y de salida de las aplicaciones que se desarrollan o mejoran en la institución, que el nuevo sistema cumple con los requerimientos especificados y evitar corrupción en el procesamiento, modificaciones deliberadas y la pérdida, la modificación o uso erróneo de datos del usuario en los sistemas de información.

L-33.1.1. Para la aplicación de los planes de pruebas, la División Servicios Tecnológicos configura ambientes individuales y aislados de manera lógica para los procesos de desarrollo, pruebas y pre-producción y capacitación.

## Parchado y actualización de sistemas

P-34. El Banco Central de Costa Rica por medio de la División Servicios Tecnológicos establece mecanismos para el proceso de actualización y parchado del software, aplicaciones de escritorio y de los sistemas de información de la institución para mantener un adecuado nivel de seguridad.

C-34.1. La División Servicios Tecnológicos es responsable de aplicar el proceso de actualizaciones y parches en todos los equipos y aplicaciones bajo su cargo, con el propósito de prevenir posibles incidentes de seguridad por explotación de vulnerabilidades en los sistemas.

L-34.1.1. Para llevar a cabo el proceso de aplicación de parches se deben seguir las siguientes reglas:

a) Todos los equipos, servidores y máquinas de escritorio, listados en los dominios administrados por el Banco Central de Costa Rica se deben parchar oportunamente según la criticidad de los parches a instalar, estos parches se instalan durante las ventanas de tiempo acordados con el negocio y se categorizan según criticidad de la siguiente manera:

| Tipo de parche | Caracteristicas | Tiempo mínimo del parche en ambiente de pruebas | Tiempo máximo para aplicar el parche desde su anuncio por parte del proveedor |
|---|---|---|---|
| Parches Verdes | Son los parches de seguridad y/o críticos emitidos por los proveedores de las aplicaciones que utiliza el Banco. Además, comprenden los parches que no presentan riesgo inmediato/evidente a la infraestructura de la institución, ya que de momento no existen "exploits" que se aprovechen de una vulnerabilidad en los sistemas. Incluye también los parches que mitigan vulnerabilidades con nivel de severidad 4 o menor según CVSS (Common Vulnerabilty Scoring System) Base Score. | 1 mes | 6 meses |
| Parches Amarillos | Corresponden a los parches que mitigan las vulnerabilidades con nivel de severidad entre 4.1 y 6.9 según CVSS (Common Vulnerabilty Scoring System) Base Score. | 1 semana | 8 semanas |
| Parches Rojos | Corresponden a los parches que mitigan las vulnerabilidades con nivel de severidad 7.0 o mayor según CVSS (Common Vulnerabilty Scoring System) Base Score. También incluye cualquier vulnerabilidad catalogada como "Día Cero". | El parche debe ser probado antes de instalarse en Producción. | 2 semanas |

b) Los responsables de adquirir software, ya sea este institucional o especializado, tal y como se define en las "Políticas específicas de compra y renovación de Hardware, Software y Servicios de TI", velarán por que no se utilicen

aplicaciones luego del EOL (End Of Life) ni luego del EOS (End of Support)[4] estipulado por el fabricante.

c) Para parchar software de uso institucional se utiliza una herramienta automatizada. En el caso de software de uso especializado, el parchado se realiza utilizando los medios que brinde el fabricante.
d) Todo parche debe seguir un proceso de pruebas según su criticidad y la guía correspondiente antes de ser instalados en los sistemas de producción del Banco.
e) El proceso de parchado debe realizarse según lo documentado en el Sitio de Calidad y en todos los casos el parchado se debe tomar como un cambio pre-aprobado a la hora de instalar los parches en el ambiente de producción.
f) Los parches para aplicar son los que hayan sido clasificados como críticos y/o de seguridad por el fabricante del producto.
g) El parchado de las herramientas utilizadas por los departamentos que realicen actividades de desarrollo de software se realizará como resultado del análisis de vulnerabilidades.
h) Las aplicaciones de software base de terceros que posean actualización automática, tendrán esta característica habilitada por defecto. Esta característica se deshabilitará únicamente para aplicaciones cuyas actualizaciones automáticas puedan causar conflicto con otras aplicaciones de la Lista de Software Autorizado o que su proceso de actualización no sea compatible con la infraestructura y políticas establecidas en este documento.
i) Todo equipo (servidor y máquina de escritorio) nuevo debe llevar como mínimo el mismo nivel de parchado que el resto de los equipos de la infraestructura del Banco a la fecha donde el mismo haya sido instalado.
j) Para las actualizaciones mayores de software tales como: Service Packs, actualizaciones de la función principal, mejoras de rendimiento y compatibilidad, cambios en el Sistema Operativo y/o cambios de versiones mayores de las aplicaciones instaladas, no aplica este lineamiento. Estas actualizaciones se gestionan y ejecutan a través del proceso de cambios definido por la División Servicios Tecnológicos.

[4] Fin de soporte se refiere a la fecha en que un fabricante deja de proporcionar revisiones automáticas, actualizaciones o asistencia técnica para una aplicación.

k) Todos los funcionarios de la institución responsables de un activo de información sujeto a procesos de parchado, debe seguir las recomendaciones de reinicio del equipo cuando así se le solicite. No está permitida la cancelación de los procesos automáticos utilizados para parchar o actualizar el hardware y software instalado en los equipos computacionales de la Institución.

l) El parchado de los equipos de red se realizará como resultado del análisis de vulnerabilidades. Además, el área de telecomunicaciones revisará la versión de sistema operativo instalada y la versión estable de sistema operativo más reciente liberada por el proveedor en cada equipo de red, para determinar si es necesario realizar la actualización.

m) En caso de que, en alguno de los procesos de análisis de vulnerabilidades realizado por el Departamento de Ciberseguridad, o en las revisiones del área de Telecomunicaciones, se determine que existe una vulnerabilidad que pueda afectar los equipos de red, el área de Telecomunicaciones utiliza la siguiente tabla para su atención:

| Tipo de vulnerabilidad | Características | Tiempo mínimo para probar el parche o vacuna para la vulnerabilidad | Tiempo máximo para aplicar el parche o vacuna desde su anuncio por parte del proveedor |
|---|---|---|---|
| Vulnerabilidades Amarillas | Corresponden a las vulnerabilidades con nivel de severidad entre 4 y 6.9 según CVSS (Common Vulnerabilty Scoring System) Base Score. | 2 semanas | 8 semanas |
| Vulnerabilidades Rojas | Corresponden a las vulnerabilidades con nivel de severidad 7.0 o mayor según (Common Vulnerabilty Scoring System) Base Score. También incluye cualquier vulnerabilidad catalogada como "Día Cero". | El parche debe ser probado antes de instalarse en producción. | 4 semanas |

C-34.2. La División Servicios Tecnológicos limita el acceso a los diferentes archivos de instalación de aplicaciones desarrolladas en el Banco Central de Costa Rica, así como las compradas a terceros mediante el uso de perfiles de acceso, para reducir el riesgo de accesos y modificaciones no autorizadas.

C-34.3. El Departamento de Ciberseguridad realiza periódicamente análisis de vulnerabilidades en los sistemas críticos del Banco Central de Costa

Rica, para reducir el riesgo de que la infraestructura se vea amenazada por la explotación de una vulnerabilidad presente en los sistemas.

C-34.4. El Departamento de Ciberseguridad recibe publicaciones y noticias mundiales para determinar la criticidad de un parche a aplicar y su aplicabilidad en los equipos y aplicaciones de la institución.