BANCO CENTRAL DE COSTA RICA

Políticas Específicas de Gestión de la Información

Sistema Interno de Gestión del Banco Central de Costa Rica

HISTORICO DE VERSIONESY CONTROL DE CAMBIOS A LA POLITICA

Versión:	**Fecha de creación:**	**Aprobado por:**	**Cambios realizados:**
6.0	30-diciembre-de 2024	Aprobación de la Gerencia del Banco Central de Costa Rica	Inclusión de consideraciones que sustentan las políticas. Ajuste en los nombres de las dependencias. En apartado "aspectos generales" se incluye la P-3 y P-4 y en "aspectos organizativos la P-6. Se eliminan labores que atiende el Área de Comunicación y se ajustan otros aspectos para alinearlos con la operativa y procedimientos actuales. Actualización integral del apartado relativo a las herramientas de colaboración. Atiende informe de Auditoría Interna AI-0027-2023.
5.0	27 de diciembre de 2023	Aprobación de la Gerencia del Banco Central de Costa Rica	Ajuste en los nombres de las dependencias e inclusión del capítulo V relativo a las herramientas de mensajería Webex y Microsoft Teams
4.0	20 de abril de 2018	Aprobación del Director de la División Transformación y Estrategia.	Se realizaron ajustes menores de redacción y se incluyeron los controles C-5.3. y C-6.4.
3.0 (Vigente)	30 de noviembre de 2016	Aprobación del Director de la División Transformación y Estrategia.	Se modifica el control C-11.6 de la Política P-11.
2.0	3 de junio de 2015	Aprobación del Director de la División Transformación y Estrategia.	Se incorpora el inciso e al control C-11.6 de la PolíticaP-11. Se incluye el control C-12.3 a la política P- 12.
1.1	19 de marzo de 2015	Aprobación del Director de la División Transformación y Estrategia.	En esta versión se modifica el control C-6.1 y se agregan los controles C-6.4, C-6.5 y el lineamiento L-6.5.1 a las políticas específicas de Intranet.

Versión:	**Fecha de creación:**	**Aprobado por:**	**Cambios realizados:**
1.0	25 de junio de 2014	Aprobación de la Subgerente del Banco Central de Costa Rica	Para fines de publicación y facilidad de consulta y mantenimiento, se incluyen únicamente los apartados correspondientes a Sistemas de Información, Intranet, Correo Electrónico y Sitio Web contenidos en el Capítulo 4 “Operación del Sistema Interno de Gestión”. En esta versión se agregan los controles C-9.2, C- 9.3, C-11.5, C-11.6, C-12.1 y C-12.2 a las políticas específicas para Correo electrónico. Política Específica del Sistema Interno de Gestión, la cual contiene seis capítulos: • Capítulo 1. Generalidades del Sistema Interno de Gestión. • Capítulo 2. Responsabilidad de la dirección. • Capítulo 3. Gestión de los recursos. • Capítulo 4. Operación del Sistema Interno de Gestión. • Capítulo 5. Evaluación del Sistema Interno de Gestión. Capítulo 6. Análisis y mejora del Sistema Interno de Gestión.

Consideraciones que sustentan la emisión de estas políticas específicas:

A. La Junta Directiva aprobó las Políticas de Alto Nivel para seguridad de la información mediante el artículo 16 del acta de la sesión 5441-2009.
B. La Gerencia es la responsable de la aprobación de las políticas específicas derivadas de las políticas de alto nivel aprobadas por la Junta Directiva.

C. El *Código de Ética para los directores de la Junta Directiva del Banco Central de Costa Rica, miembros del Consejo Nacional de Supervisión del Sistema Financiero, Gerente, Subgerente, Superintendentes e Intendentes y personal del Banco Central de Costa Rica y sus órganos de desconcentración máxima a*probado por la Junta Directiva del Banco Central de Costa Rica en el artículo 8 del acta de la sesión 5477-2010 del 3 de noviembre del 2010, establece:

- que las personas funcionarias deberán actuar con rectitud, independencia, imparcialidad, discreción, atendiendo el interés público y deberán evitar toda situación que pueda dar lugar a un conflicto de intereses. Deberán ser conscientes de la importancia de su cargo, tener en cuenta el carácter público de sus funciones y comportarse de modo que se promueva la confianza del público en el Banco Central de Costa Rica.
- El Banco espera que su personal se trate mutuamente con respeto y cortesía. Por tanto, el Banco rechaza conductas de hostigamiento sexual o cualquier expresión de odio o prejuicio basada en criterios de discapacidad, raza, religión, preferencias sexuales o cualquier otro tipo de preferencias de carácter estrictamente personal de sus servidores y colaboradores. El Banco tiene las mismas expectativas de buen trato cuando su personal se relaciona con los usuarios de sus servicios, proveedores y personas externas a la Institución.

D. La Estructura de organización y funciones del Banco Central de Costa Rica establece los objetivos generales para los siguientes departamentos:
   - División Transformación y Estrategia, Departamento de Calidad y Mejora Continua: administrar el proceso de gestión institucional de procesos, servicios, información, comunicación, archivo central, gobierno corporativo, control interno, seguridad de la información, continuidad de negocios y reorganizaciones administrativas; dotándolo de metodologías, herramientas y promoviendo los cambios culturales necesarios que permitan a la Entidad alcanzar sus objetivos estratégicos.

   Adscritos a la División de Servicios Tecnológicos

   - Departamento TI de Colaboración: diseñar, implementar, operar y mejorar las soluciones tecnológicas que conforman el escritorio digital, las que facilitan la comunicación y colaboración y las que apoyan la administración institucional (como bienes, personas, finanzas y estrategia), de manera que las distintas áreas de la

institución ejecuten sus procesos y alcancen sus objetivos y metas de trabajo de forma eficiente de la mano de la tecnología.

- Departamento de Ciberseguridad: gestionar y fortalecer la ciberseguridad, con base en las mejores prácticas en la materia, con la finalidad de proteger las soluciones tecnológicas de la Institución ante la creciente amenaza cibernética en un mundo cada vez más digitalizado.

E. Las políticas específicas de gestión documental fueron aprobadas en diciembre de 2021 y establecen los siguientes mandatos:
   - son de acatamiento obligatorio para todos los funcionarios y colaboradores de la institución, a fin de garantizar el logro de los objetivos establecidos para el Sistema Institucional de Gestión Documental, así como para propiciar el aprovechamiento de tecnologías de información que apoyan la gestión institucional y la protección de su patrimonio documental mediante el uso apropiado de sus documentos en cualquier soporte, cumpliendo con las condiciones establecidas sobre integridad, confidencialidad y oportunidad. Su incumplimiento será sancionado de acuerdo con lo que establece el Reglamento Autónomo de Servicios.
   - Todo funcionario generador o receptor de documentos oficiales en cualquier soporte, los organizará en los espacios físicos o virtuales conforme a su naturaleza y a las reglas de la institución que se determinan.

F. El informe de Auditoría Interna AI-0027-2023 fechado el 26 de enero del 2023 recomendó:
   - R1. (Prioridad 2) Definir en coordinación con la División Servicios Tecnológicos y remitir a aprobación del nivel competente, el modelo de gobernanza que incluya las políticas y la definición de otros aspectos de control interno pertinentes para la gestión de las herramientas institucionales de mensajería instantánea, con el fin de establecer disposiciones que regulen el uso por parte los funcionarios, la protección de la información enviada o recibida por estos medios y el tratamiento de las comunicaciones de usuarios internos con dominios externos.

G. 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.

POLÍTICAS ESPECÍFICAS DE GESTIÓN DE LA INFORMACION

I. Aspectos generales

P-1. La División Transformación y Estrategia, a través del Departamento Calidad y Mejora Continua, debe proporcionar, a todas las dependencias del Banco Central y sus órganos desconcentrados, herramientas que permitan garantizar que la información institucional se procesa de manera organizada, uniforme, consistente, segura y oportuna, con el propósito de lograr la consecución de los objetivos institucionales.

P-2. Todos los funcionarios del Banco Central de Costa Rica y los ODM deben cumplir con la normativa, con el propósito de propiciar el aprovechamiento de tecnologías de información que apoyan la gestión institucional, a fin de hacer un manejo apropiado de la información cumpliendo con las condiciones establecidas en integridad, confidencialidad y oportunidad.

P-3. La División Transformación y Estrategia es la responsable de administrar y regular las herramientas de información digitales disponibles en el Banco, con el objetivo de estandarizar y alinear la generación y divulgación de la información del Banco Central de Costa Rica.

P-4. Todas las personas funcionarias del BCCR y sus ODM tienen las siguientes responsabilidades respecto a las herramientas de mensajería y colaboración:

a. Cada usuario es responsable de la administración y gestión de la información compartida en las herramientas cuyo propósito es facilitar la comunicación y colaboración.
b. Cumplir las regulaciones del Código de Ética y las buenas costumbres al utilizar las herramientas de colaboración.
c. Activar y mantener encendida la cámara de su computadora durante las reuniones virtuales. La no activación de la cámara deberá ser la excepción y solo estará permitida por razones fuera de control de la persona funcionaria, por ejemplo, cortes temporales de la electricidad o de Internet.
d. Se debe evitar el uso de avatares en las sesiones virtuales oficiales de la institución.
e. Las herramientas de comunicación permiten el uso de fondos virtuales para aquellos funcionarios que deseen utilizar dicha opción. En la Intranet de la institución se pueden descargar cortinas oficiales o se podrá elegir un fondo o

imagen externa siempre y cuando estos mantengan un carácter formal y apropiado para el entorno laboral.

f. Los contenidos cargados, subidos o compartidos a través de las herramientas institucionales deben ser de carácter profesional, respetuoso y alineadas con los valores y ética institucionales. Se prohíbe el contenido ofensivo, discriminatorio o inapropiado, todas las imágenes deben estar relacionadas con el trabajo y el entorno profesional. Asimismo, se debe garantizar que no infrinjan derechos de autor ni contengan información confidencial o sensible. Cada persona funcionaria es responsable de seleccionar imágenes que cumplan con estas directrices, asegurando el respeto y la integridad de la comunicación institucional.

P-5. Para los efectos de esta política, se aplica la siguiente terminología:

- Activo de información: todo aquello que tenga valor informativo, para la organización, con respecto a la seguridad de la información.
- BCCR: Banco Central de Costa Rica.
- Herramienta de colaboración: aplicación diseñada para facilitar la colaboración, comunicación y trabajo entre personas, equipos o grupos. Permite a las personas funcionarias compartir información, colaborar en documentos, proyectos y comunicarse en tiempo real de forma eficiente para facilitar la interacción y creación de información pertinente. Incluyen, pero no se limitan a: mensajería instantánea o chats, teleconferencias y otras.
- Chat: espacio destinado a conversaciones rápidas y ocasionales, facilitando una comunicación ágil, flexible y sencilla entre los miembros.
- Equipo de trabajo: espacio diseñado para la colaboración estructurada en proyectos o grupos de trabajo, promoviendo la organización, el trabajo en espacios compartidos, la integración de herramientas y la centralización de información. La DST eliminará los equipos de trabajo que tienen más de 60 días naturales de inactividad o desuso.
- Canal de equipo en Teams: un espacio creado para facilitar la colaboración efectiva en proyectos o grupos de trabajo. Promueve la organización, el trabajo en entornos compartidos, la integración de herramientas y la centralización de información, optimizando la comunicación y el flujo de trabajo entre los miembros del canal.
- Institución: Banco Central de Costa Rica (BCCR), incluyendo sus Órganos de Desconcentración Máxima (ODM).

II. Aspectos de implementación y gestión

Intranet

P-6. La División Transformación y Estrategia, mediante el Departamento Calidad y Mejora Continua, es responsable de administrar y regular la Intranet, como, gestor documental y plataforma de trabajo, para garantizar el cumplimiento de las buenas prácticas y normas, nacionales e internacionales.

P-7. Toda información documental generada y recibida en el cumplimiento de sus deberes, por las diferentes dependencias se almacena en el espacio de la Intranet destinado a cada División, respetando las disposiciones establecidas por el Departamento Calidad y Mejora Continua y los plazos de conservación de acuerdo con lo normado en la Ley del Sistema Nacional de Archivos, Ley 7202, para garantizar la confiabilidad e integridad de la información.

- La información derivada por las dependencias del Banco debe estar agrupada por procesos, de acuerdo con la estructura establecida en el Sitio de Calidad, con excepción de la Correspondencia. No se permite el uso de carpetas, por lo que el agrupamiento de archivos dentro de bibliotecas se realiza mediante valores en metadatos con el fin de facilitar la navegación, manejo de permisos y otros aspectos de gestión de la Intranet.
- Toda correspondencia interna oficial se gestiona digitalmente y se autentica mediante firma digital para brindarle los niveles de seguridad que ofrece la Intranet y disminuir el consumo de papel. Si por requerimiento legal o conveniencia, en casos calificados, se requiere una versión impresa de la correspondencia interna oficial, esta debe ser firmada físicamente por el responsable.
- La correspondencia entrante y saliente se almacena en los espacios de la Intranet correspondientes al área emisora y destinataria, y se convertirá en un registro no editable en el momento de su despacho.
- La modificación de los metadatos de la correspondencia se solicitará mediante un caso puesto en la lista de solicitudes de administración de la Intranet y será evaluado e implementado por el Departamento de Calidad y Mejora Continua, siempre que cumpla con las características de la información y cuando el cambio no altere datos sensibles sobre el trámite de la correspondencia.
- Si por requerimiento legal o conveniencia, en casos calificados, se requiere una versión impresa de un documento, ésta será firmada físicamente y la versión digitalizada del documento firmado se almacena en la Intranet.

P-8. Los comunes o carpetas de red no están permitidos como repositorios de información institucional no estructurada.

- Toda gestión relacionada con la creación y conservación de carpetas de red o comunes que deban existir, por limitaciones de la Intranet relacionadas con el tipo de archivos a almacenar, requiere de autorización expresa del Departamento Calidad y Mejora Continua antes de ser atendida por la División de Servicios Tecnológicos.

P-9. El Departamento Calidad y Mejora Continua es el encargado de definir la estructura general de permisos y de asignar los roles a los usuarios de la Intranet, de acuerdo con las necesidades de las áreas de negocio, así como de crear grupos de usuarios y vistas, para garantizar la seguridad de la información en los espacios de uso institucional, exceptuando el de Proyectos.

Correo electrónico

P-10. El Banco Central de Costa Rica dispone del correo electrónico como un medio de comunicación oficial, tanto a lo interno como a lo externo del Banco, el cual es administrado y regulado por el Departamento Calidad y Mejora Continua para garantizar el cumplimiento de las buenas prácticas.

- El correo electrónico se debe utilizar como medio para la recepción de datos, únicamente en aquellos casos en que no existe una aplicación específica. En este caso, los datos se administrarán en un buzón de correo y tendrán asociado un responsable de administración de buzón, que se encargará de la limpieza, mantenimiento y solicitudes de gestión sobre el buzón.
- El envío masivo de correos se realiza bajo las siguientes circunstancias:
    a. Cuando se trate de un buzón albergado en la infraestructura en la tierra, los límites por cada envío serán de un máximo de 1000 destinatarios cada 5 minutos y con un límite de 50 destinatarios de un mismo dominio.
    b. Cuando se trate de un buzón albergado en la nube, la cantidad máxima de envío por día será de 1000 destinatarios o el límite diario que indique el proveedor del servicio; los límites por cada envío serán de un máximo de 500 destinatarios cada 5 minutos y con un límite de 50 destinatarios de un mismo dominio.
    c. Para los dos puntos anteriores, el usuario generador deberá verificar la validez de las direcciones incorporadas y deberá gestionar los mensajes de error devueltos.

P-11. La División Transformación y Estrategia, a través del Departamento Calidad y Mejora Continua, es la responsable de administrar y regular las funcionalidades del correo electrónico, como lo son los buzones de correo de servicio, las cuentas de usuario, buzones de fax y los buzones de correo individuales, con el objetivo de garantizar la calidad de las herramientas de comunicación utilizadas a nivel institucional.

a) Toda solicitud relacionada con la creación, modificación o eliminación de buzones compartidos, listas de distribución o buzones de fax debe ser realizada por el director de Departamento solicitante o el funcionario a quien este designe y debe ser dirigida al Departamento Calidad y Mejora Continua mediante la herramienta designada oficialmente.

b) A cada buzón de correo se le asigna un espacio máximo de capacidad de almacenamiento de acuerdo con las capacidades establecidas por la administración del servicio. Luego de sobrepasado el límite establecido, se podrán recibir correos, pero no enviarlos.

c) El espacio asignado a cada buzón será ampliado en aquellos casos donde se presente la debida justificación ante la Dirección del Departamento Calidad y Mejora Continua y se dé la aprobación por parte de éste.

d) Los buzones de correo de servicio se crean para el envío y recepción de mensajes relacionados con un servicio particular del Banco, que permite su identificación tanto a lo interno como a lo externo, bajo un nombre representativo (sigla o acrónimo), tal como sigue: <acrónimo>@bccr.fi.cr.

e) Los mensajes del correo electrónico se consideran comunicaciones oficiales, por ello, deben cumplir con los siguientes estándares para mantener la imagen institucional:

- Deben incluir la firma identificadora[1] de correo según formato oficializado en el espacio "Diseño Institucional" de la Intranet.
- El fondo debe cumplir con el formato oficializado en el espacio "Diseño Institucional" de la Intranet, no se permite el uso de plantillas personalizadas.
- Utilizar las opciones de confirmación de entrega y de lectura sólo en casos de importancia, con el fin de no generar tráfico innecesario en la red.

f) Los mensajes provenientes de una cuenta de correo de servicio deben incluir la firma identificadora del funcionario que lo emite, con el fin de personalizar la atención de los servicios.

[1] La firma identificadora corresponde a la identificación del funcionario dueño de una cuenta de correo mediante la cual se indica su nombre, puesto, división a la que pertenece, teléfono, fax y logotipo del Banco.

g) El Departamento Calidad y Mejora Continua es el responsable de coordinar la creación de listas de distribución, bajo un nombre representativo (sigla o acrónimo), tal como sigue: <acrónimo>@bccr.fi.cr.

h) La creación de una lista de distribución requiere de una solicitud ante el Departamento Calidad y Mejora Continua. La creación de listas de distribución está restringida a equipos de trabajo o comisiones, con el fin de facilitar la comunicación entre sus miembros, con una duración permanente o temporal, por el periodo de tiempo solicitado por su responsable.

- Las listas de usuario temporales se eliminan una vez cumplida la fecha máxima de vigencia especificada en la solicitud de su creación, previa comunicación al usuario.

i) La responsabilidad de solicitar y del uso adecuado de las listas de distribución de correo corresponde a los directores de departamento o coordinadores de las comisiones.

j) El envío de correo a la lista de distribución denominada "Todo el personal" está permitido únicamente para ciertas dependencias, funcionarios y para los fines que el Departamento de Calidad y Mejora Continua autorice.

k) El envío masivo a todos los funcionarios de una división es permitido solo a aquellos funcionarios a los que se les haya concedido permiso, a solicitud del director de la división correspondiente.

l) Cada una de las dependencias del Banco Central de Costa Rica cuenta con un buzón de fax asociado al correo electrónico, para fines estrictamente relacionados con sus funciones.

- El plazo de entrega de nuevos buzones de fax queda supeditado a la disponibilidad de licencias y números de teléfono.

P-12. El Banco Central de Costa Rica provee a todos sus funcionarios una cuenta de correo electrónico única y personal, con su respectivo buzón asociado, la cual debe ser empleada como una herramienta de comunicación e intercambio de información directamente relacionada con las tareas y responsabilidades del funcionario. El uso que el funcionario haga de esta herramienta de trabajo para otros fines será su responsabilidad, enfrentando de manera personal las posibles consecuencias derivadas.

a. El alias de usuario para la cuenta de correo electrónico se define bajo el siguiente esquema: primer apellido, inicial del segundo apellido e inicial del nombre del funcionario; así como cualquier otro carácter necesario para distinguir entre dos usuarios con el mismo identificador, de la siguiente manera:<aliasdelusuario>@bccr.fi.cr.

b. A las personas que, sin ser parte de la planilla del Banco, se encuentran realizando labores habituales en la Institución se les asigna una cuenta de correo de manera temporal durante el periodo en que desarrollen dichas actividades, la cual se rige bajo las mismas políticas específicas aplicables a los funcionarios.

c. Es responsabilidad del titular de la cuenta de correo electrónico:

    1. Toda actividad relacionada con el uso de su cuenta de correo.
    2. Velar por la protección de la información confidencial, crítica o privada del Banco, que reciba o envíe por este medio.
    3. El contenido del mensaje difundido.

d. Los correos electrónicos cuyo emisor sea desconocido, de dudosa procedencia, o que aparenten provenir de una fuente conocida, pero que presentan características irregulares, deben ser eliminados inmediatamente; los adjuntos provenientes de dichas fuentes no deben ser abiertos.

e. Los funcionarios del Banco que por sus funciones requieran revisar el correo electrónico en sus dispositivos móviles, deben solicitar al Departamento Calidad y Mejora Continua la autorización de la configuración, previa autorización de su director de Departamento.

f. Los funcionarios que tienen acceso al correo electrónico a través de un dispositivo móvil tienen las siguientes responsabilidades:

    1. Salvaguardar toda la información del Banco que permanezca en el dispositivo móvil.
    2. Informar sobre la pérdida del dispositivo móvil.
    3. Eliminar del dispositivo móvil toda la configuración de acceso al correo, antes de cambiarlo o venderlo, asimismo deberá informar al Departamento Calidad y Mejora Continua sobre el cambio del dispositivo.
    4. Cuando se efectué el cambio periódico de contraseñas del usuario de dominio, el funcionario deberá reconfigurar su dispositivo móvil con la nueva contraseña.
    5. Mantener actualizada la identificación del dispositivo personal en uso en la lista de dispositivos del correo (disponible en https://mail.bccr.fi.cr/owa, opciones, teléfono) y eliminar los dispositivos que ya no tenga en uso de esta.

P-13. La División de Servicios Tecnológicos es responsable de establecer o modificar los

parámetros de seguridad y la configuración del correo electrónico, los cuales en su implementación deben contar con el visto bueno del Departamento Calidad y Mejora Continua.

a) El Departamento de Infraestructura Tecnológica implementará equipos especializados de seguridad o configuraciones en los servidores de correo electrónico que impidan el acceso de correo malicioso que pueda interrumpir el adecuado funcionamiento de una o más cuentas de correo electrónico, filtrando software, ejecutables, imágenes o cualquier otro tipo de contenido que esté considerado como peligroso para la infraestructura.
b) El Departamento de Infraestructura Tecnológica validará con los parámetros internacionales los formatos, extensiones y archivos que son definidos como maliciosos y que puedan afectar la infraestructura e implementará las medidas necesarias para garantizar el adecuado filtro de los correos.
c) El Departamento de Infraestructura Tecnológica implementará los mecanismos necesarios de seguridad, tanto en la infraestructura del Banco como en los equipos móviles, que permitan bloquear y desbloquear los dispositivos móviles que tengan acceso directo al correo electrónico institucional.

Sitio Web

P-14. El Banco Central de Costa Rica dispone de un sitio web como herramienta de comunicación oficial hacia lo externo del Banco, el cual es administrado y regulado por la División Transformación y Estrategia, mediante el Departamento Calidad y Mejora Continua, como responsable de promover la implementación y cumplimiento de las buenas prácticas y normas, nacionales e internacionales.

P-15. El Departamento Calidad y Mejora Continua, en coordinación con la División de Servicios Tecnológicos, debe brindar las facilidades necesarias para que las Áreas de Negocio autorizadas puedan publicar documentos en el Sitio Web del Banco.

a) Los documentos publicados deben ser creados en un formato seguro, por ejemplo, Word, formato PDF o con firma digital. Cuando se requiera otro formato, debe enviarse la solicitud al Departamento Calidad y Mejora Continua para analizar el caso.
b) Las Áreas de Negocio que publiquen documentos en el Sitio Web deben utilizar las plantillas que diseñe el Departamento Calidad y Mejora Continua para los diferentes tipos documentales, ubicadas en el espacio Diseño Institucional de la Intranet.
c) Las Áreas de negocio son responsables de revisar y mantener actualizado el contenido de sus espacios, con el fin de conservar siempre en el sitio la información

vigente. Deberán solicitar mediante caso en la herramienta establecida para este propósito la publicación de contenido

P-16. La División Transformación y Estrategia, mediante el Departamento Calidad y Mejora Continua, es responsable de definir los estándares para las publicaciones en el Sitio Web y de velar por su cumplimiento; por lo tanto, tiene la facultad de ajustar el sitio cuando la documentación incumpla las disposiciones de contenido y forma, con el fin de garantizar el adecuado uso de la identidad corporativa y una efectiva comprensión del mensaje a comunicar.

La información publicada en el Sitio Web del Banco Central de Costa Rica debe ser actualizada de manera oportuna por los responsables de ésta.

P-17. El Departamento Calidad y Mejora Continua es responsable de los cambios de diseño y presentación del sitio Web del Banco, para mantener la imagen institucional y la claridad del mensaje.

El área de negocio solicitante debe justificar la creación de un nuevo espacio o la modificación de uno existente por medio de una solicitud ante el Departamento Calidad y Mejora Continua.

Herramientas institucionales de colaboración

P-18. El Banco Central pone a disposición de las personas funcionarias herramientas de colaboración para favorecer una interacción fluida y segura que permita el intercambio de información laboral por voz, texto u otros mecanismos.

P-19. Todas las personas funcionarias que utilizan las herramientas institucionales de colaboración deben ser conscientes que se pueden generar activos de información que son de relevancia para los diversos procesos del banco, por lo tanto, se establece que dichos activos de información se deben gestionar de acuerdo con las políticas vigentes aplicables para garantizar el resguardo, la integridad y la disponibilidad de la información, con las propiedades que corresponden. Las herramientas institucionales de colaboración no son repositorios permanentes ni gestores oficiales de información. La información compartida o generada en estas plataformas debe trasladarse a los repositorios oficiales permanentes para su procesamiento como activo de información y almacenamiento.

P-20. El BCCR define que las herramientas de colaboración no son el medio oficial de la organización para la asignación de labores o la creación de solicitudes, por lo tanto, las personas funcionarias deben utilizar los medios ya establecidos por la institución para la

adecuada gestión de estas tareas, de manera que se asegure el registro, atención y trazabilidad requeridas.

P-21. Todas las personas funcionaras al utilizar las herramientas de colaboración pueden realizar reuniones con participación híbrida (presencial y remota a la vez). Se debe implementar mecanismos integradores que garanticen una participación equitativa, balanceada y justa para todos los asistentes, independientemente de su ubicación. Por ejemplo, utilizar la funcionalidad de "levantar la mano" que incluya tanto a los participantes presenciales como a los remotos.

P-22. El Departamento Calidad y Mejora Continua establece las siguientes condiciones para la grabación de sesiones llevadas a cabo mediante las herramientas de colaboración, para que su uso vaya acorde a las funciones y políticas de la Institución:

a. Las personas funcionarias son responsables de conocer que las herramientas de colaboración permiten la grabación de las sesiones, por tanto, si la persona funcionaria considera que la grabación es un activo de información tiene la responsabilidad de almacenar esa grabación en el gestor documental que le corresponde.
b. Los archivos compartidos durante la reunión deben mantener el resguardo definido durante el proceso según la clasificación de seguridad de la información, estos archivos deberán conservarse en la Intranet o en el espacio correspondiente según las políticas y procedimientos aplicables.
c. Todo el personal está autorizado a generar una grabación de una sesión siempre que haya consentimiento de todos los involucrados. Las personas funcionarias que participan de una reunión que está siendo grabada otorgan su consentimiento implícito a la grabación al unirse a la misma.
d. Las herramientas de colaboración almacenan las grabaciones de las sesiones de manera temporal por un plazo de 60 días naturales como máximo. Tras el vencimiento de este periodo, las grabaciones serán eliminadas automáticamente. Si se desea conservar la grabación, esta deberá ser almacenada en la Intranet o en el espacio designado según las normativas aplicables, donde pueda estar disponible para su consulta.

P-23. Las cámaras deben permanecer encendidas durante las sesiones de trabajo o reuniones, se considera una excepción, cuando la calidad de la reunión se mejore quitando la transmisión de video.

P-24. Se podrán compartir enlaces o documentos de trabajo que son de carácter transitorio,

o no relevante, en los casos que se considere necesario según los procedimientos vigentes, las versiones finales deberán ser trasladadas a la intranet o en el espacio designado según las normativas aplicables, donde pueda estar disponible como resguardo de los activos de los procesos.

Autorización para la instalación y uso de aplicaciones relacionadas con las herramientas de colaboración

P-25. El Departamento TI de Colaboración define que todas las personas funcionarias pueden solicitar la instalación y uso de aplicaciones o complementos que se puedan integrar con las herramientas de colaboración a la DST por los medios oficiales que esta división establezca. Dichas solicitudes deben incluir la justificación pertinente para garantizar que su uso vaya acorde a las funciones y políticas del Banco.

Sesiones o usuarios externos a la institución

P-26. En los casos en los que se presente la necesidad de agregar a un usuario o un dominio externo al del Banco Central en las herramientas de colaboración, se deberá solicitar la valoración y aprobación a la DST a través de los medios oficiales establecidos por esta división, para cumplir con lo estipulado en las Políticas aplicables.

P-27. Las personas usuarias que requieran agregar o invitar a personas externas a la organización a grupos o equipos de trabajo internos deben cumplir con los cuidados establecidos en las políticas de seguridad de la información. En particular, deben asegurarse de que la información compartida con los usuarios externos no comprometa la confidencialidad de la institución, con el fin de atender las normativas vigentes aplicables.