BANCO CENTRAL DE COSTA RICA

DIVISIÓN SISTEMAS DE PAGO

NORMA TÉCNICA

REQUISITOS DE CIBERSEGURIDAD PARA PARTICIPAR EN EL SINPE

SERIE DE NORMAS Y PROCEDIMIENTOS

Público

sinpe

NT-RCS

BANCO CENTRAL DE COSTA RICA

DIVISIÓN SISTEMAS DE PAGO

N O R M A T É C N I C A

R E Q U I S I T O S D E C I B E R S E G U R I D A D P A R A P A R T I C I P A R E N E L S I N P E

SERIE DE NORMAS Y PROCEDIMIENTOS

Público

sinpe

Tabla de contenido

Sistema Nacional de Pagos Electrónicos

1. Introducción

La presente norma establece los requisitos y disposiciones de carácter complementario al Reglamento del Sistema de Pagos y el marco normativo emitido por el Banco Central de Costa Rica (BCCR) para regular los aspectos relacionados con los controles de ciberseguridad que deben cumplir los afiliados al Sistema Nacional de Pagos Electrónicos (SINPE).

El creciente desarrollo del SINPE ha llevado a la aceleración de los procesos de digitalización de los movimientos de fondos en el ámbito interbancario, derivando en un aumento en el acceso de los clientes a los canales digitales de las entidades que operan en el SINPE y, por ende, en una mayor cantidad de transacciones en línea que incrementa los riesgos de ciberataques al sistema.

La plataforma tecnológica del SINPE, desde hace más de 15 años cuenta con una certificación internacional en seguridad de la información, la cual implica cumplir con una serie de requisitos y controles tecnológicos establecidos con el propósito de proteger la confidencialidad, integridad y disponibilidad de la información que administra el sistema, para mantener la confianza en el sistema de intercambio de pagos por parte de las entidades financieras, instituciones públicas, usuarios y público.

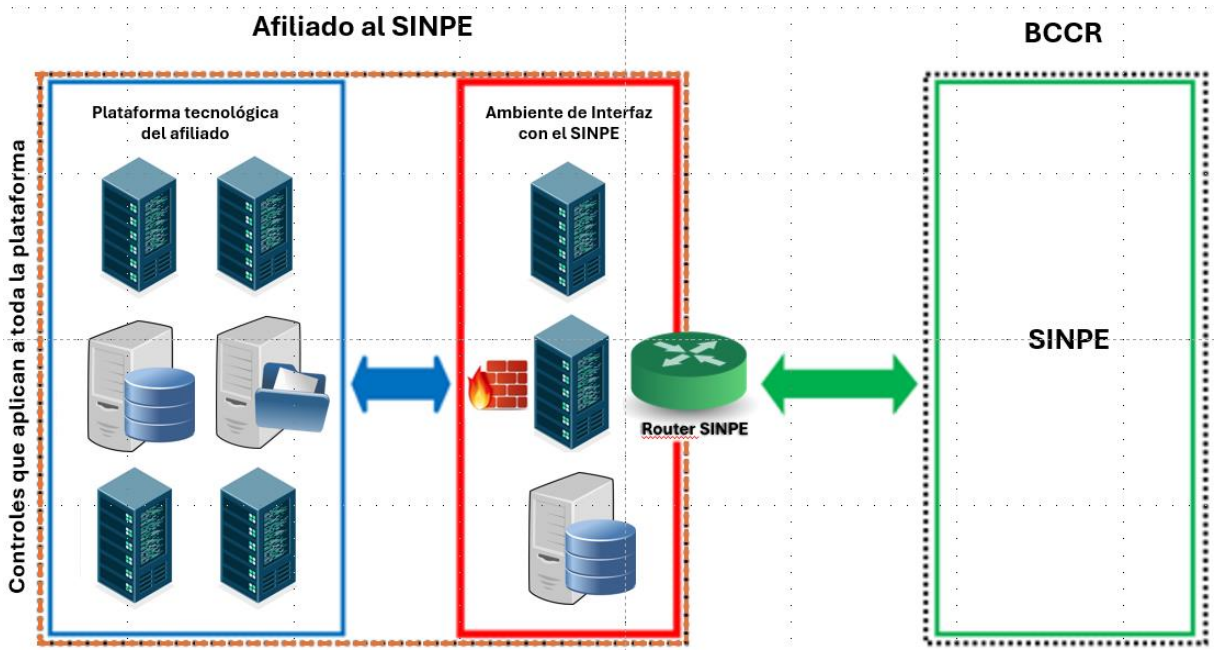
La presente norma técnica tiene por objetivo ampliar el alcance de los controles de seguridad de la información, para extender el radio de acción hasta ciertas áreas tecnológicas propias de las entidades participantes en el SINPE, fortalecer la red de seguridad del sistema y prevenir riesgos de ciberataques.

Las entidades afiliadas al SINPE deberán cumplir una serie de regulaciones dirigidas a adoptar marcos de ciberseguridad adecuados para la protección del sistema, considerando los servicios particulares que cada afiliado tiene autorizados, de manera que el nivel de rigurosidad de los controles esté determinado por el nivel de exposición que tienen los servicios por medios digitales.

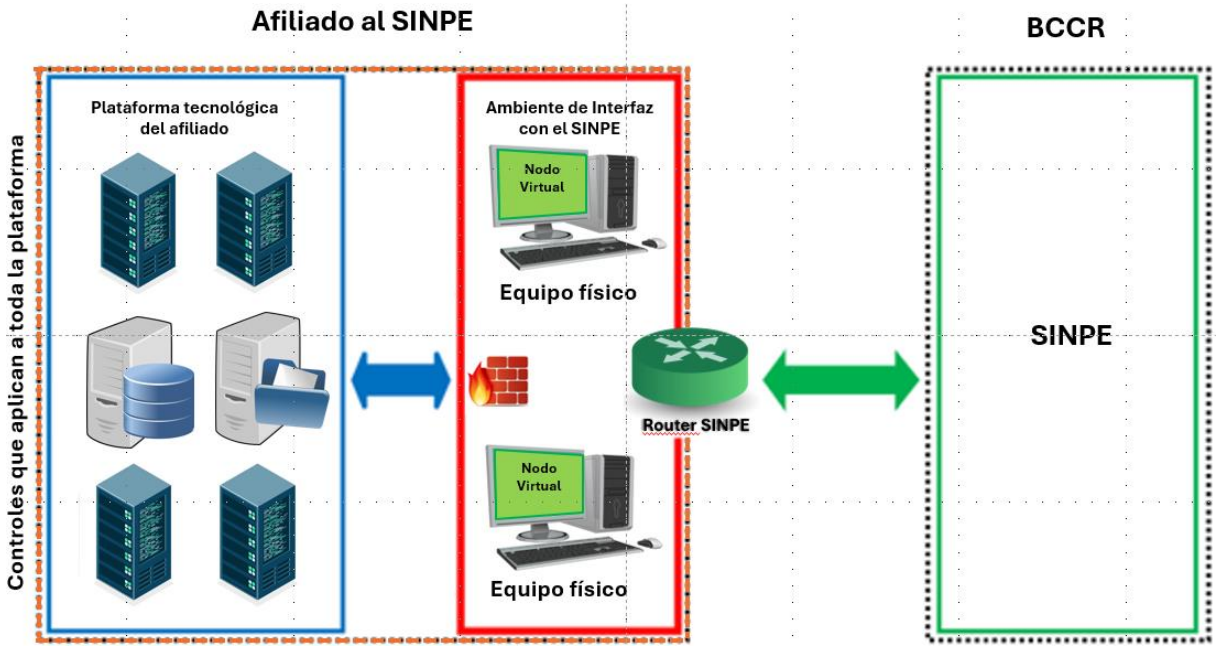
2. Alcance

La presente norma técnica es de acatamiento obligatorio por parte de los afiliados al SINPE, y como tal,constituye un requisito para adquirir y mantener la condición de afiliado.

El siguiente diagrama resume la relación que mantienen los afiliados con la arquitectura tecnológica del SINPE, en el caso del consumo de servicios por medio de web services (Categoría 1):



El siguiente diagrama ejemplifica la arquitectura de los afiliados que consumen los servicios del SINPE a través de los nodos virtuales (Categoría 2):



Los controles acá descritos, aplican para el Ambiente de Interfaz con el SINPE, a excepción de los controles asociados con la protección del correo electrónico y la navegación por Internet, así como los controles asociados a la protección contra código malicioso (Apartados 6.8 y 6.9 respectivamente), que, por ser los principales vectores para la generación de ciberataques, deben ser aplicados a la totalidad de la organización.

3. Términos empleados

Para los fines del presente documento, se entenderá por:

- **AAA (Autenticación, Autorización y Auditoría):** mecanismos concebidos para permitir el acceso de los usuarios legítimos a los activos conectados a la red e impedir accesos no autorizados, implementando mecanismos de autenticación, autorización y bitácoras de auditoría. Autenticación se refiere a la identidad, autorización a los privilegios qué tiene la identidad y auditoría registra las acciones realizadas.
- **Activos de servicios tecnológicos:** servicios de procesamiento y comunicaciones.
- **Activos de software:** software de aplicación, software de sistemas, herramientas de desarrollo, utilitarios y otros elementos lógicos pertenecientes a la infraestructura tecnológica.
- **Activos tecnológicos físicos:** computadoras, equipos de comunicaciones, medios removibles y otros elementos físicos pertenecientes a la infraestructura tecnológica.
- **Ambiente de interfaz con el SINPE (AIS):** conjunto de elementos tecnológicos del afiliado que participan en el procesamiento, almacenamiento y transmisión de transacciones hacia y desde el SINPE.
- **Ambiente:** combinación de hardware y software para realizar una o varias tareas específicas. Generalmente existen ambientes de pruebas, ambientes de desarrollo, ambientes de preproducción y ambientes de producción.
- **Análisis de vulnerabilidades:** proceso para definir, identificar, clasificar y priorizar las debilidades del sistema, con el fin de proporcionar una evaluación de las amenazas previsibles y reaccionar de manera apropiada.
- **Autenticación multifactor (MFA):** agrega una capa de protección al proceso de inicio de sesión. Cuando se accede a una cuenta o aplicación, los usuarios deben pasar por una verificación de identidad adicional que consiste, por ejemplo, en escanear su huella digital o especificar un código que reciben en su teléfono.
- **Autenticación:** acto o proceso de confirmar que algo o alguien es quien dice ser.
- **BCCR:** Banco Central de Costa Rica.
- **Cambio significativo:** cualquier modificación o alteración en los sistemas o su entorno que pueda afectar su postura de seguridad; por ejemplo: cambios de reglas de firewall en accesos públicos; cambios sobre los controles de segmentación de la red; cambios de infraestructura; nuevos equipos; nuevo software o uso de otros protocolos, y cambio de proveedores de servicios o cambio en el intercambio de datos, entre otros.
- **Ciberseguridad:** práctica de defender las computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos, de ataques maliciosos.
- **Cifrado:** proceso de codificación o encriptación de datos para que solo pueda leerlos alguien con los medios para devolverlos a su estado original.
- **CIS:** Center for Internet Security.
- **Código malicioso:** tipo de código informático o script diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.

- **Confidencialidad:** cualidad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Configuración segura:** proceso de asegurar un sistema mediante la reducción de su superficie de vulnerabilidad. La reducción de las formas de ataque disponibles generalmente incluye cambiar las contraseñas predeterminadas, la eliminación de software innecesario, nombres de usuario o inicios de sesión innecesarios y la desactivación o eliminación de servicios innecesarios.
- **CSP (Cloud Solution Provider):** Proveedor de Soluciones en la Nube; es una empresa que proporciona recursos de procesamiento escalables a los que las empresas pueden acceder a pedido en una red, lo que incluye servicios de procesamiento, almacenamiento, plataforma y aplicaciones basados en la nube.
- **Datos en reposo:** estado de los datos cuando están almacenados, y no se están moviendo de un lugar a otro (en tránsito) ni están siendo cargados en la memoria para ser utilizados por un programa informático (en uso).
- **Datos confidenciales o de acceso restringido:** son todos aquellos que la entidad establezca de conformidad con el marco legal vigente en materia de protección de datos, políticas internas, y otros criterios que consideren relevantes.
- **Datos en tránsito:** Se refiere a los datos que se envían de un sistema a otro, esto puede ser por medio de una red empresarial privada o Internet. Esto incluye la comunicación dentro de la carga de trabajo entre los recursos, así como la comunicación entre otros servicios y usuarios finales.
- **Disponibilidad:** la cualidad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Eventos de riesgos:** situaciones que ocurren en un lugar particular o durante un período determinado y que podría generar consecuencias económicas, legales o reputacionales para una compañía.
- **Firewall:** cortafuegos; es un programa informático o un hardware que provee protección a una computadora (ordenador) o a una red frente a intrusos, bloqueando los accesos no permitidos.
- **HTTPS (o Hypertext Transfer Protocol Secure):** protocolo que permite establecer una conexión segura entre el servidor y el cliente; está basado en el protocolo HTTP, pero implementa cifrado basado en la seguridad de textos TLS para crear un canal cifrado.
- **Integridad:** cualidad de salvaguardar la exactitud y estado completo de la información.
- **IPS (Intrusion Prevention System):** software utilizado para proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva.
- **NIPS (Network-based Intrusion Prevention Systems):** tipo de IPS que se instala directamente en la red, con el fin de analizar, detectar y bloquear amenazas avanzadas en tiempo real en las redes.
- **OWASP® Open Worldwide Application Security Project®:** fundación sin fines de lucro que trabaja para mejorar la seguridad del software.
- **Plataforma tecnológica del afiliado al SINPE (PTA):** infraestructura y aplicativos propios del afiliado que forman parte de las soluciones de negocio.
- **Protecciones antimalware:** programas diseñados para prevenir, detectar y remediar software malicioso en los dispositivos informáticos individuales y sistemas TI.
- **Segmento de red:** es una porción o subdivisión de una red informática que se separa lógica o físicamente del resto de la red. Los segmentos de red se utilizan para organizar y gestionar mejor el tráfico de datos y mejorar la seguridad, ya que permiten controlar y limitar el acceso entre diferentes partes de la red.

- **SNMP v3 (o Simple Network Management Protocol):** protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.
- **Software:** conjunto de instrucciones, datos o programas, utilizados para operar computadoras y ejecutar tareas específicas.
- **SSH (Secure SHell):** protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente.
- **Usuario final:** se refiere a los usuarios internos de la entidad afiliada al SINPE.
- **Vulnerabilidad:** debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información.

4. Documentos aplicables y anexos

Siglas	Nombre del documento
RSP	Reglamento del Sistema de Pagos
NC-RPS	Normativa Complementaria - Requisitos para participar en el SINPE
NC-AES	Normativa Complementaria - Administración de Esquemas de Seguridad

5. Particularidades

Los afiliados del SINPE deben cumplir con los controles que se detallan en los siguientes apartados. Esta norma se revisará de forma anual, y se notificará en diciembre de cada año los ajustes aplicados, que entrarán a regir a partir del siguiente año.

5.1. Alcance

Esta norma técnica regula los siguientes ámbitos de los afiliados.

- Infraestructura requerida para operar el SINPE.
- Equipos de conexión al SINPE.
- Usuarios del SINPE.
- Capa de intercambio de datos.
- Servidores interconectados al SINPE.

5.2. Tipos de controles

Cada afiliado debe cumplir con los siguientes controles.

5.2.1. Controles obligatorios

Controles de acatamiento obligatorio para los afiliados que deben de ser atendidos de forma integral y completa.

5.2.2. Controles opcionales

Controles que fortalecen aún más el ambiente de ciberseguridad, debido a lo cual, es importante que sean valorados por cada afiliado para su cumplimiento. En una etapa posterior podrían convertirse en obligatorios.

Los controles opcionales pueden ser actualizados de acuerdo con las variaciones en las condiciones de seguridad. Su nivel de cumplimento podrá modificarse o podrán incluirse nuevos requerimientos que se consideren convenientes para la protección de la seguridad del sistema.

5.2.3. Controles No Aplicables

Es el caso de los controles que no aplican para el tipo de conexión indicada, en este caso el control no debe ser evaluado.

5.3. Tipos de conexión con el SINPE

Los servicios autorizados a cada afiliado pueden tener diferentes niveles de exposición a riesgos de ciberseguridad, debido a los canales que utilice para realizar sus transacciones con el SINPE, aspecto que debe considerarse para determinar el grado de cumplimiento que se le exigirá.

5.3.1. Uso de servicios con conexiones vía web services - Categoría 1

Afiliados que mantienen algún servicio por medio del consumo de web services expuestos por el SINPE, mediante los cuales establecen la comunicación fuera de la plataforma propia del SINPE. En estos casos, el afiliado tendrá mayores niveles de cumplimiento para garantizar la protección de todo el sistema, debido a esa interacción con web services.

5.3.2. Uso de servicios en el cliente SINPE directamente - Categoría 2

Afiliados que no poseen servicios con exposición a web services, por lo que solo utilizan determinados servicios del SINPE expuestos directamente en la terminal conectada a SINPE (servicios AES o MIL, por ejemplo).

Cuando un afiliado ubicado inicialmente en la categoría 2 solicite autorización para el acceso a servicios con conexión vía web service, previo a ser autorizado para su uso deberá cumplir con los requisitos definidos para dicha categoría.

5.4. Cumplimiento

Los afiliados actuales y los interesados en afiliarse al SINPE deberán presentar un informe de cumplimiento de parte de un auditor, con no más de un tres meses de emitido, en el que se especifique que la entidad cumple a cabalidad con los controles establecidos, según sea el nivel de riesgos en el que se ubique.

Con la finalidad de garantizar que las labores sean ejecutadas por expertos certificados, el profesional a cargo del informe de cumplimiento deberá contar con al menos una de las siguientes certificaciones:

- **ISACA:** Certified Information Systems Auditor (CISA) -solicitado por las ODM's-.
- **ISO:** ISO 27001 Lead Auditor.
- **GIAC:** GIAC Systems and Network Auditor (GSNA).

La entidad que presenta el informe de cumplimiento es responsable de verificar y dar garantía ante el BCCR de que el auditor elegido cumple con los atestados exigidos por esta norma, para ello deberá incluir en el informe la evidencia respectiva. En caso de que el auditor incumpla con los atestados exigidos, el BCCR dará como inválido el informe presentado.

5.4.1. Periodicidad

Los afiliados y las entidades interesadas en afiliarse al SINPE deben cumplir con los siguientes requisitos:

- El informe de cumplimiento tendrá una validez de un año, que abarca el periodo que va desde el 1 de julio del año en curso hasta el 30 de junio del año siguiente y deberá ser presentado durante el semestre previo.
- El informe debe ser enviado con un oficio formal firmado digitalmente por el Gerente General o el Representante Legal de la entidad al Departamento Sistema Nacional de Pagos Electrónicos del BCCR, por medio de un caso enviado por el Responsable de Servicios Titular de la entidad. El informe deberá indicar, al menos, los siguientes datos:
  - Entidad afiliada o en proceso de afiliación al que corresponde el informe.
  - Declaración de cumplimiento de la normativa y calidades del auditor
  - Periodo al que corresponde el mismo.
  - En caso de que el afiliado utilice servicios de proveedores externos, deberán incluir los informes de cumplimiento de la parte atendida por estos proveedores. En el informe de cumplimiento debe quedar explícitamente detallado, los alcances de cada informe, la parte atendida por los proveedores externos y la parte atendida por la propia entidad. El afiliado es responsable por el cumplimiento del 100% de los controles establecidos en la norma.
- Los nuevos interesados en participar en el SINPE deberán cumplir con la totalidad de los requisitos para poder afiliarse. El informe de cumplimiento deberá ser enviado por nuestro canal seguro en la extranet, para lo cual se le enviará a la persona responsable designada por la entidad, los accesos para que pueda subir el mismo al sitio definido.

  No serán recibidos por otro canal que no sea el antes indicado, tanto para afiliados como para los de nuevo ingreso al SINPE, por lo que de recibirse por medios como correo electrónico u otros no serán atendidos, debido a que son canales no seguros para enviar informes con los datos que se solicitan.

Cuando el informe de cumplimiento del auditor establezca controles incumplidos total o parcialmente, el afiliado debe aportar un plan remedial para solventar las brechas detectadas y su atención deberá finalizarse a más tardar el 31 de octubre del año en curso, aportando los documentos solicitados en este mismo apartado.

En el caso de que el informe luego de la primer versión (atendiendo el plan remedial), presente puntos a resolver detectados por parte de la revisión del BCCR, se deberá atender las observaciones en un plazo no mayor a 1 mes contado a partir de haber sido informado oficialmente por el BCCR y deberá enviar nuevamente el informe completo, con los puntos a subsanar y su clara evidencia de cómo fueron atendidos.

5.4.2. Incumplimiento

Ante incumplimientos por parte de las entidades de los controles dispuestos en la presente norma técnica, se procederá de la siguiente forma:

- **Entidad en proceso de afiliación:** no se autorizará la afiliación de la entidad al SINPE hasta que cumpla todos los requisitos establecidos.
- **Entidad afiliada:** la situación se pondrá en conocimiento de sus máximas autoridades y del órgano de supervisión que corresponda. Dependiendo del impacto que provoque el incumplimiento en el ambiente de seguridad, el BCCR podrá ordenar la apertura de un procedimiento administrativo con el propósito de determinar la verdad real de los hechos.

6. Pruebas por realizar

En este apartado se detallan los controles que cada entidad debe cumplir; ya sea para afiliarse o para mantener su condición de afiliado al SINPE, para lo cual deberán considerar:

- **Tipos de controles**: obligatorio ⊕, opcional ⊖ y no aplicable ⊘.
- **Tipo de afiliado**: considerar si se clasifican como **categoría 1** (al menos un servicio a través del consumo de web services) o **categoría 2** (todos sus servicios los consumen directamente en el cliente SINPE).

En el caso de que la entidad disponga de un proveedor de servicios y éste sea el encargado de realizar la certificación parcial de los controles, el informe deberá ser integrado, identificando claramente qué controles estuvieron a cargo del auditor. La nota de envío del informe debe ser suscrita por el Gerente General o Representante Legal de la entidad, quien asume la responsabilidad del informe.

6.1. Inventario y control de los activos de hardware

Objetivo: identificar la totalidad de los activos que necesitan ser monitoreados y protegidos, así como apoyar en la identificación de activos no autorizados y no administrados.

6.1.1	Establecer y mantener un inventario de la infraestructura	**Categoría 1**	**Categoría 2**
		⊕	⊕
Establecer y mantener un inventario preciso, detallado y actualizado del Ambiente de Interfaz con el SINPE. Asegúrese de que el inventario contenga como mínimo: el nombre del dispositivo, la dirección de red (si es estática) y la función o servicio. Revisar y actualizar el inventario al menos una vez al año.			
6.1.2	Establecer y mantener un diagrama de red detallado	**Categoría 1**	**Categoría 2**
		⊕	⊕
Establecer y mantener un diagrama de red preciso, detallado y actualizado del Ambiente de Interfaz con el SINPE. El diagrama deberá incluir información detallada de la red, así como información de los protocolos y puertos utilizados. Revisar y actualizar el diagrama de red al menos una vez al año o cuando ocurran cambios significativos en la infraestructura.			

6.2. Inventario y control de los activos de software

Objetivo: mantener una gestión activa y un adecuado control de los activos de software para prevenir ataques.

6.2.1	Establecer y mantener un inventario de aplicaciones	**Categoría 1**	**Categoría 2**
		⊕	⊕
Elaborar y mantener un inventario detallado de todo el software instalado en la infraestructura del Ambiente de Interfaz con el SINPE. El inventario de software debe documentar el nombre, el fabricante, la versión y el propósito. Revisar y actualizar el inventario al menos una vez al año. Únicamente deberán mantenerse las versiones de software que cuenten con el debido soporte.			

6.2.2	Establecer una lista de software autorizado	**Categoría 1**	**Categoría 2**
		⊕	⊕
Para el Ambiente de Interfaz con el SINPE, se deberá mantener una lista actualizada del software autorizado. Implementar controles para eliminar el software no autorizado o fuera de soporte de los equipos. Actualizar al menos cada 6 meses la lista de software autorizado y documentar las excepciones con el debido plan remedial.			

6.3. Protección de los datos

Objetivo: mantener una adecuada privacidad de los datos confidenciales o de acceso restringido durante todo su ciclo de vida, sin importar el medio en que se encuentren.

6.3.1	Establecer y mantener procedimientos adecuados para la gestión de datos	**Categoría 1**	**Categoría 2**
		⊕	⊕
Establecer y mantener procedimientos adecuados para la identificación y gestión de datos confidenciales o de acceso restringido que dé cobertura a aquellos relacionados con el SINPE. Como mínimo, deben considerarse los siguientes aspectos: la confidencialidad, requerimientos legales, el propietario y el manejo adecuado. Los datos confidenciales o de acceso restringido establecidos en el SINPE son: saldos de las cuentas de valores y efectivo, monto de las transacciones del SINPE en efectivo y valores, identificación y nombre del cliente origen y destino de las transacciones del SINPE.			
6.3.2	Cifrar los datos confidenciales en tránsito	**Categoría 1**	**Categoría 2**
		⊕	⊘
Deben cifrarse los datos en tránsito (canal de comunicación), transmitidos entre la Plataforma Tecnológica del Afiliado y el Ambiente de Interfaz del SINPE identificados en los respectivos procedimientos. El cifrado debe hacerse mediante protocolos considerados seguros por las buenas prácticas internacionales.			

6.3.3	Política de disposición y/o destrucción de medios y hardware	Categoría 1	Categoría 2
		⊖	⊖
Definir una política para la gestión del ciclo de la información en medios de almacenamiento (incluido el hardware), cuándo se cumple su tiempo máximo de operación y se debe dar de baja, o debe enviarse fuera de la organización por temas de soporte.			
6.3.4	Cifrar datos confidenciales en reposo	**Categoría 1**	**Categoría 2**
		⊖	⊖
Deben cifrarse los datos de acceso restringido o confidenciales identificados con los procedimientos respectivos, que se encuentran en reposo (almacenados en bases de datos, discos duros, o cualquier otro medio de almacenamiento utilizado por la entidad).			

6.4. Configuración segura

Objetivo: establecer la línea base de configuración requerida para mantener la seguridad de la infraestructura.

6.4.1	Establecer y mantener un proceso de configuración seguro	**Categoría 1**	**Categoría 2**
		⊕	⊕
Establecer y mantener un proceso seguro de la configuración (hardening) basado en un marco de ciberseguridad internacionalmente aceptado (por ejemplo: CIS) para la infraestructura del Ambiente de Interfaz con el SINPE. Deben establecerse mecanismos de revisión anuales de cumplimiento de esta configuración y deberán documentarse las excepciones.			
6.4.2	Implementar y administrar un firewall	**Categoría 1**	**Categoría 2**
		⊕	⊕
Implementar un firewall para controlar con mínimo privilegio todas las comunicaciones entre el Ambiente de Interfaz con el SINPE y cualquier otra red, incluida la salida a Internet, para restringir conexiones innecesarias y permitir una adecuada segmentación de redes. La configuración de las reglas del firewall debe incluir una lista documentada de todos los servicios, protocolos y puertos, incluida la justificación de negocio y la aprobación para cada una de dichas reglas. Las reglas del firewall deberán revisarse al menos cada seis meses.			

6.5. Administración de cuentas y control de accesos

Objetivo: establecer los mecanismos mínimos necesarios para prevenir accesos no autorizados a los activos.

6.5.1	Establecer y mantener un inventario de cuentas	**Categoría 1**	**Categoría 2**
		+	+

Establecer y mantener un inventario de todo el personal con acceso al Ambiente de Interfaz con el SINPE, el cual debe contener todas las cuentas de usuario, así como de administración y servicio. Las cuentas, los roles y sus privilegios, deben revisarse al menos de forma semestral y estar aprobados por el superior jerárquico. Las cuentas inactivas por más de 90 días deberán ser deshabilitadas.

Como mínimo, el inventario debe contener los siguientes elementos:

- ⊡ El nombre de la persona responsable de la cuenta.
- ⊡ El detalle de la cuenta de usuario (FQDN).
- ⊡ El tipo de cuenta (usuario, servicio, administración).
- ⊡ El dominio.
- ⊡ El departamento.

6.5.2	Establecer una política de contraseñas	**Categoría 1**	**Categoría 2**
		+	+

Implementar una política de contraseñas en las cuentas que se identificaron en el inventario del apartado 6.5.1. Establecer y mantener un inventario de cuentas, donde cada usuario tenga una contraseña única con al menos las siguientes características:

- ⊡ Si utiliza Autenticación Multifactor (MFA), contraseñas de al menos 8 caracteres.
- ⊡ Si no tiene implementado Autenticación Multifactor (MFA), contraseñas de al menos 14 caracteres.
- ⊡ Que implementen mecanismos para forzar su complejidad, de acuerdo con las mejores prácticas internacionales.
- ⊡ Las contraseñas deberán cambiarse al menos cada 90 días naturales, cuando no se utilice Autenticación Multifactor (MFA).

6.5.3	Restringir los privilegios de administrador	**Categoría 1**	**Categoría 2**
		+	+

Establecer y mantener un inventario de las cuentas de tipo administración y servicio, identificadas en el inventario del apartado 6.5.1. Para estas cuentas, deberán restringirse las actividades que son propias de usuario final, por ejemplo: navegación por Internet y acceso al correo electrónico.

6.5.4	Establecer un proceso para conceder accesos	**Categoría 1**	**Categoría 2**
		⊕	⊕
Establecer y seguir un proceso para otorgar, revocar o modificar los accesos a la infraestructura del Ambiente de Interfaz con el SINPE, a fin de garantizar que los usuarios tengan acceso a los sistemas y datos necesarios para realizar sus funciones, siguiendo siempre el principio de mínimo privilegio y necesidad de saber.			
6.5.5	Implementar Autenticación Multifactor para los accesos privilegiados	**Categoría 1**	**Categoría 2**
		⊕	⊖
Implementar Autenticación Multifactor (MFA) para todos los accesos administrativos a la infraestructura del Ambiente de Interfaz con el SINPE.			

6.6. Gestión de vulnerabilidades

Objetivo: establecer un proceso adecuado para gestionar las vulnerabilidades de la infraestructura, para minimizar el riesgo de sufrir un incidente de ciberseguridad asociado a la explotación exitosa de la debilidad de un activo.

6.6.1	Establecer y mantener un proceso de gestión de vulnerabilidades	**Categoría 1**	**Categoría 2**
		⊕	⊕
Establecer y mantener un proceso de gestión de vulnerabilidades documentado que incluya al menos cobertura de análisis y remediación. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios significativos que puedan afectar este control.			
6.6.2	Realizar análisis de vulnerabilidades internos y externos	**Categoría 1**	**Categoría 2**
		⊕	⊕
Realizar escaneos de vulnerabilidades internos y externos al menos una vez por semestre para la infraestructura del Ambiente de Interfaz con el SINPE y los servicios externos que se conectan con la misma; todos los hallazgos detectados deberán corregirse de acuerdo con los procesos documentados.			

6.6.3	Realizar una gestión de parches y actualizaciones	**Categoría 1**	**Categoría 2**
		⊕	⊕
Implementar y ejecutar un proceso de parchado o aplicación de actualizaciones al menos de forma semestral.			

6.7. Gestión de bitácoras de auditoría

Objetivo: establecer una gestión adecuada de las bitácoras de auditoría, mantener un monitoreo de la infraestructura que permita detectar situaciones anómalas y realizar análisis forense cuando sea requerido.

6.7.1	Recopilar registros de auditoría	**Categoría 1**	**Categoría 2**
		⊕	⊖
Debe existir un proceso para gestionar bitácoras de auditoría que, como mínimo, aborde la recopilación, revisión y retención de los registros. Deben recopilarse los registros de auditoría de toda la infraestructura del Ambiente de Interfaz con el SINPE. Como mínimo, el registro debe incluir los siguientes elementos: ⊡ El origen del evento. ⊡ La fecha. ⊡ El nombre de usuario. ⊡ La marca de tiempo. ⊡ El dominio. ⊡ Las direcciones de origen. ⊡ Las direcciones de destino.			
6.7.2	Almacenar de forma adecuada los registros de auditoría	**Categoría 1**	**Categoría 2**
		⊕	⊖
Los registros de auditoría deben almacenarse de acuerdo con lo que establece el proceso de gestión, en caso de ser requerido para análisis de eventos. El mínimo de retención solicitado es de 90 días.			
6.7.3	Estandarizar la hora de los registros de auditoría	**Categoría 1**	**Categoría 2**
		⊕	⊖
Con la finalidad de mantener la seguridad, precisión y disponibilidad de los registros de tiempo en los sistemas de registro de eventos (bitácoras o logs). Debe estandarizarse la hora, configurando al menos dos orígenes de hora sincronizados dentro de la infraestructura.			

6.7.4	Realizar revisiones de los registros de auditoría	**Categoría 1**	**Categoría 2**
		⊕	⊖
Realizar revisiones, al menos semanalmente, de los registros de auditoría para detectar posibles anomalías o eventos anormales que podrían representar una amenaza.			

6.8. Protección del correo electrónico y la navegación por Internet

Objetivo: definir mecanismos de protección para el usuario final ante posibles eventos de riesgo asociados a los principales vectores de ataque, en este caso el correo electrónico y la navegación en Internet**.**

6.8.1	Aplicar filtrado de navegación	**Categoría 1**	**Categoría 2**
		⊕	⊕
Aplicar y mantener actualizados los filtros de navegación para limitar la conexión de los activos a sitios web potencialmente maliciosos o no aprobados.			
6.8.2	Implementar protección contra correo no deseado	**Categoría 1**	**Categoría 2**
		⊕	⊕
Implementar y mantener una herramienta de filtrado de correo no deseado.			
6.8.3	Implementar protección antimalware a nivel de correo electrónico	**Categoría 1**	**Categoría 2**
		⊕	⊕
Implementar y mantener protecciones antimalware del servidor de correo electrónico, como el análisis de archivos adjuntos y el espacio aislado.			
6.8.4	Bloquear archivos innecesarios	**Categoría 1**	**Categoría 2**
		⊕	⊕
Establecer una política de bloqueo en el correo electrónico de archivos adjuntos riesgosos o innecesarios. Revisar la lista de bloqueo al menos de forma semestral.			

6.9. Defensa contra código malicioso

Objetivo: implementar controles para la protección contra código malicioso en la infraestructura de la organización, como una medida para prevenir infecciones que pudieran generar fugas de información, denegación de servicios o daños a los activos.

6.9.1	Implementar y mantener software contra código malicioso	**Categoría 1**	**Categoría 2**
		⊕	⊕
Implementar software de protección contra código malicioso en todos los activos del Ambiente de Interfaz con el SINPE.			
6.9.2	Actualizar de forma automática las firmas contra código malicioso	**Categoría 1**	**Categoría 2**
		⊕	⊕
Configurar las actualizaciones automáticas de las herramientas contra código malicioso.			
6.9.3	Utilizar herramientas de protección basadas en comportamiento	**Categoría 1**	**Categoría 2**
		⊖	⊖
Usar software contra código malicioso basado en el comportamiento.			

6.10. Recuperación de datos

Objetivo: establecer mecanismos para la recuperación de la información ante incidentes que pudieran afectar su disponibilidad.

6.10.1	Establecer y mantener un proceso de recuperación de datos	**Categoría 1**	**Categoría 2**
		⊕	⊘
Establecer y mantener un proceso de recuperación de datos del Ambiente de Interfaz con el SINPE. En el proceso debe establecerse el alcance de las actividades de recuperación, la priorización de la recuperación, las pruebas de recuperación y la seguridad de los datos de respaldo. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios significativos que puedan afectar este requisito.			

6.11. Gestión de la infraestructura de red

Objetivo: definir los controles básicos que permitan establecer un nivel de seguridad aceptable de las comunicaciones, frente a eventuales ataques contra la red.

6.11.1	Establecer y mantener una arquitectura de red segura	**Categoría 1**	**Categoría 2**
		⊕	⊕
La red donde se ubican los equipos del Ambiente de Interfaz con el SINPE debe segmentarse de forma que permita separar este ambiente del resto de la red empresarial. Dicha segmentación deberá permitir las comunicaciones estrictamente necesarias, bloqueando el tráfico entre la red empresarial y el Ambientes de Interfaz con el SINPE. Las comunicaciones permitidas deberán ser debidamente documentadas.			
6.11.2	Utilizar mecanismos seguros para la administración de red	**Categoría 1**	**Categoría 2**
		⊕	⊕
Utilizar protocolos seguros de administración de red de acuerdo con las mejores prácticas de la industria, como son: SSH, SNMP v3 y HTTPS. Implementar mecanismos de identidad AAA (Autenticación, Autorización y Auditoría) para el acceso administrativo a la infraestructura de red.			
6.11.3	Gestionar el control de acceso para activos remotos	**Categoría 1**	**Categoría 2**
		⊕	⊕
Utilizar mecanismos seguros e inspección de estado de salud, para establecer conexiones remotas a la red empresarial, por ejemplo: VPN.			

6.12. Monitoreo y defensa de la red

Objetivo: definir mecanismos para monitoreo y respuesta efectivos, que permitan responder de forma rápida ante posibles amenazas.

6.12.1	Implementar un IPS en la red	**Categoría 1**	**Categoría 2**
		⊕	⊘
Debe implementarse una solución de prevención de intrusiones entre las redes organizacionales y la red del Ambiente de Interfaz con el SINPE. Las implementaciones de ejemplo incluyen el uso de un sistema de prevención de intrusiones en la red (NIPS) o un servicio equivalente de proveedor de servicios en la nube (CSP).			

6.12.2	Implementar una solución de Detección y Respuesta para punto final (Endpoint Detection and Response)	**Categoría 1**	**Categoría 2**
		⊕	⊖
Implementar una solución de detección y respuesta a nivel de host.			
6.12.3	Realizar el filtrado en la capa de aplicación	**Categoría 1**	**Categoría 2**
		⊕	⊘
Realizar filtrado del tráfico externo, de forma que puedan identificarse las aplicaciones para bloquear o permitir, según corresponda. Entre las implementaciones de ejemplo se incluye un firewall de próxima generación.			

6.13. Concientización en Ciberseguridad y formación de habilidades

Objetivo: definir un programa de concientización en ciberseguridad que permita complementar los controles definidos, para abordar el riesgo asociado a los ataques dirigidos a las personas que interactúan con los servicios de SINPE.

6.13.1	Establecer y mantener un programa de concientización en ciberseguridad	**Categoría 1**	**Categoría 2**
		⊕	⊕
Establecer y mantener un programa de concientización sobre ciberseguridad. El propósito del programa es educar al personal sobre cómo interactuar con los activos y datos de la empresa de manera segura. Realice la capacitación al momento de contratar y, como mínimo, anualmente.			
6.13.2	Llevar a cabo capacitación en habilidades y concientización sobre ciberseguridad para roles específicos	**Categoría 1**	**Categoría 2**
		⊖	⊖
Llevar a cabo capacitación en habilidades y concientización sobre ciberseguridad para funciones específicas. Por ejemplo: cursos de administración de sistemas seguros para profesionales de TI, capacitación en prevención y concientización de vulnerabilidades de OWASP® Top 10 para desarrolladores de aplicaciones web y capacitación avanzada en concientización sobre ingeniería social para roles de alto perfil, entre otros.			

6.14. Gestión de proveedores de servicios

Objetivo: establecer mecanismos que permitan asegurar de forma básica las relaciones con terceros, y definir las responsabilidades en cuanto a la protección de la información y los activos.

6.14.1	Establecer y mantener una política de gestión de proveedores de servicios	**Categoría 1**	**Categoría 2**
			
Establecer y mantener una política de gestión de proveedores de servicios para aquellos contratos relacionados con la implementación de servicios de interacción directa con el SINPE. Como mínimo, la política debe abordar la clasificación, el inventario, la evaluación, el seguimiento y requisitos de ciberseguridad; así como la finalización de la relación con los proveedores de servicios. Revisar y actualizar la política anualmente o cuando ocurran cambios significativos.			

6.15. Seguridad en las aplicaciones

Objetivo: establecer controles básicos de seguridad en el desarrollo de las aplicaciones, para prevenir vulnerabilidades en el código que pudieran ser explotadas por los atacantes. En el caso de que el afiliado no desarrolle sus propias soluciones informáticas, debe asegurar que su proveedor aplica estos controles.

6.15.1	Ambientes de producción y no producción debidamente separados	**Categoría 1**	**Categoría 2**
			
Mantener entornos separados para sistemas de producción y no producción, además no se deberán utilizar los datos confidenciales o de acceso restringido de producción en los ambientes no productivos.			
6.15.2	Establecer y mantener un proceso de desarrollo de aplicaciones seguro	**Categoría 1**	**Categoría 2**
			
Establecer y mantener un proceso de desarrollo de aplicaciones seguro. En el proceso, deben abordarse elementos tales como: estándares de diseño de aplicaciones seguras, prácticas de codificación segura, capacitación de desarrolladores, gestión de vulnerabilidades, seguridad de código de terceros y procedimientos de prueba de seguridad de aplicaciones. Revisar y actualizar la documentación anualmente o cuando ocurran cambios significativos.			

6.15.3	Establecer y mantener un proceso para gestionar las vulnerabilidades de las aplicaciones	**Categoría 1**	**Categoría 2**
			
Establecer y mantener un proceso para gestionar las vulnerabilidades de las aplicaciones. El proceso debe incluir elementos tales como: ⊡ Una política de manejo de vulnerabilidades. ⊡ Un proceso de admisión, asignación, remediación y pruebas de remediación de las vulnerabilidades reportadas. Revisar y actualizar la documentación anualmente o cuando ocurran cambios significativos.			
6.15.4	Implementar verificaciones de seguridad a nivel de código	**Categoría 1**	**Categoría 2**
			
Implementar en el ciclo de desarrollo de las aplicaciones prácticas o actividades que permitan realizar comprobaciones de seguridad en el código.			

6.16. Gestión de respuesta ante incidentes

Objetivo: definir procedimientos adecuados de respuesta ante incidentes de ciberseguridad, para responder de la forma más eficiente a los ataques, así como definir las estrategias de comunicación a otros interesados ante un evento de este tipo.

6.16.1	Designar personal para administrar el manejo de incidentes	**Categoría 1**	**Categoría 2**
			
Asignar las responsabilidades al personal encargado de gestionar el proceso de atención de incidentes. El personal de administración es responsable de la coordinación y documentación de la respuesta a incidentes y los esfuerzos de recuperación. Esta responsabilidad puede asignarse a empleados internos de la empresa, personal de proveedores externos o mediante un enfoque híbrido. Las responsabilidades deberán revisarse anualmente o cuando ocurran cambios significativos.			

6.16.2	Establecer y mantener un proceso de atención de incidentes de ciberseguridad	**Categoría 1**	**Categoría 2**
		⊕	⊕

Establecer y mantener un proceso de atención de incidentes de ciberseguridad.
El proceso debe considerar, como mínimo, los siguientes aspectos (no implica necesariamente un documento independiente para cada uno de ellos):

- ⊡ Declaración de incidentes.
- ⊡ Roles y responsabilidades.
- ⊡ Triage o determinación de severidad.
- ⊡ Procedimientos detallados de respuesta (playbooks).
- ⊡ Plan de comunicación (escalamiento, información de contacto y plantillas para comunicación).

El proceso y su documentación deberán revisarse anualmente o cuando ocurran cambios significativos.

6.16.3	Establecer y mantener información de contacto para comunicar incidentes de ciberseguridad	**Categoría 1**	**Categoría 2**
		⊕	⊕

Establecer y mantener la información de contacto de las partes que necesitan ser informadas de incidentes de ciberseguridad. Los contactos pueden incluir personal interno, proveedores externos, proveedores de seguros, agencias gubernamentales u otras partes interesadas. Verificar los contactos anualmente para asegurarse de que la información está actualizada.
En el caso de un incidente relacionado con el Ambiente de Interfaz con el SINPE, deberá informarse de forma inmediata al Centro de Atención del Ciudadano del BCCR y seguir el proceso establecido para la atención de incidentes de ciberseguridad.

6.16.4	Ejecutar ejercicios de respuesta a incidentes	**Categoría 1**	**Categoría 2**
		⊕	⊕

Ejecutar ejercicios y escenarios de respuesta a incidentes de ciberseguridad, aplicables al Ambiente de Interfaz con el SINPE, para el personal clave involucrado en el proceso de respuesta, con el propósito de prepararse para responder a incidentes reales. Los ejercicios deben probar los canales de comunicación, la toma de decisiones y los flujos de trabajo. Como mínimo, se deben realizar pruebas anualmente.

7. Anexo

A continuación, se detallan cada uno de los apartados que deberá incluir el informe de auditoría que se envíe al BCCR:

- **Resumen ejecutivo:** se debe ofrecer una visión general del informe, en el que se destaquen los principales hallazgos, recomendaciones y conclusiones sobre el cumplimento de los puntos evaluados.
- **Introducción:** indicar el propósito y alcance de la auditoria. Se incluye la metodología utilizada y los estándares o marcos de referencia de ciberseguridad utilizados para emitir el informe.
- **Marco Organizacional:** información sobre la entidad auditada, en la que se debe considerar el tipo de clasificación a la cual pertenece (categoría 1 o 2), políticas y enfoque que tiene hacia la ciberseguridad. En el caso de grupos financieros en el alcance deben indicar cada una de las entidades que abarca el informe.
- **Equipo de auditores:** se debe indicar el equipo de auditores que participaron en la auditoria y las certificaciones que lo califican para emitir el informe, siendo una declaración de la entidad que cumple los requisitos establecidos en esta norma técnica para emitir su criterio sobre los puntos a evaluar. Se deberá incluir la evidencia de la verificación de los atestados de los auditores.
- **Alcance de la auditoria:** deberán identificar, sistemas, activos y procesos sujetos a esta evaluación.
- **Metodología:** se deberá indicar los procedimientos, técnicas y herramientas empleadas para evaluar la ciberseguridad de la entidad.
- **Hallazgos de la auditoria:** se deberá indicar por cada apartado su cumplimiento o si se detectaron hallazgos o incumplimientos, el detalle de los mismos. En este apartado debe estar dentro del informe y no como anexos y debe contener al menos los siguientes datos en una tabla: número de control, nombre y detalle, evidencia de la revisión realizada y estado del control.

ID del control	Detalle del control	Detalle de cumplimiento validado por la auditoría	Estado de cumplimiento
Se debe indicar el número del control específico como aparece en la norma técnica vigente.	Se debe indicar el nombre del control que está siendo evaluado como aparece en la norma técnica vigente. El auditor también puede optar por transcribir el texto completo del control, siempre que no se altere el contenido a utilizar como criterio de	Se debe indicar cuál fue la evidencia de cumplimiento y sustantiva revisada como parte del proceso de auditoría. Además, se debe describir cómo dicha evidencia satisface cada uno de los aspectos que solicita la normativa. Para ello se puede presentar una descripción o, si es más conveniente, alguna captura o transcripción de las evidencias. Es de vital importancia que se haga referencia a todos los aspectos solicitados por la normativa y no solamente al asunto central del control. Si el auditor realizó alguna prueba adicional para determinar el cumplimiento del control, se deberá indicar la prueba efectuada y el resultado de cumplimiento resultante. Cuando la normativa requiera la actualización o revisión periódica del control, el auditor deberá obtener información suficiente para determinar que se satisface	El auditor deberá indicar si se cumple o no el control.

	auditoría.	el requisito, tanto en su formalidad como en su aplicación. Se deberá agregar también, cualquier comentario adicional que el auditor tenga sobre la revisión, incluyendo recomendaciones, excepciones, faltantes de información y cualquier detalle relevante. Finalmente, el auditor deberá emitir su criterio sobre el cumplimiento del control específico, con base y como conclusión a todo el detalle anteriormente expuesto.	

- **Conclusión de la auditoria:** se deberá indicar el resultado final de la auditoria, en la cual indica si cumplen todos los controles o los que no están acorde con lo solicitado en esta norma técnica.
- **Plan de Mitigación:** en caso de no contar con el cumplimiento al 100%, deberá incluir el plan de mitigación para cumplir en la fecha establecida en esta norma técnica.
- **Anexos:** podrán incluir documentos adicionales relevantes, que proporcionen la evidencia del cumplimiento de las pruebas realizadas, entre otros.

En el caso que se requiere un plan de mitigación al volver a remitirlo, debe ser enviado con el informe completo, actualizando los controles que quedaron pendientes con el plan de mitigación y su envío es de la misma forma que el informe inicial.