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

NT-RCS

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.

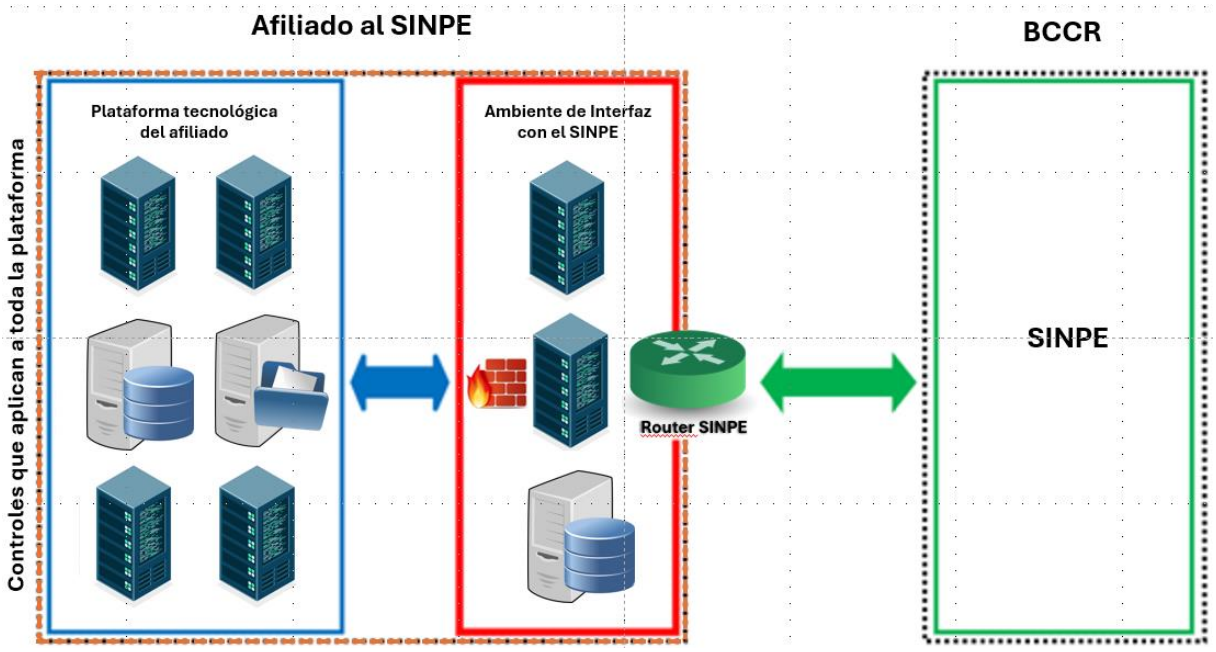
La presente norma técnica tiene por objetivo ampliar el alcance de los controles de seguridad de la información, para extender el radio de acción hasta ciertas áreas tecnológicas propias de las entidades participantes en el SINPE, fortalecer la red de seguridad del sistema y prevenir riesgos de ciberataques.

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.

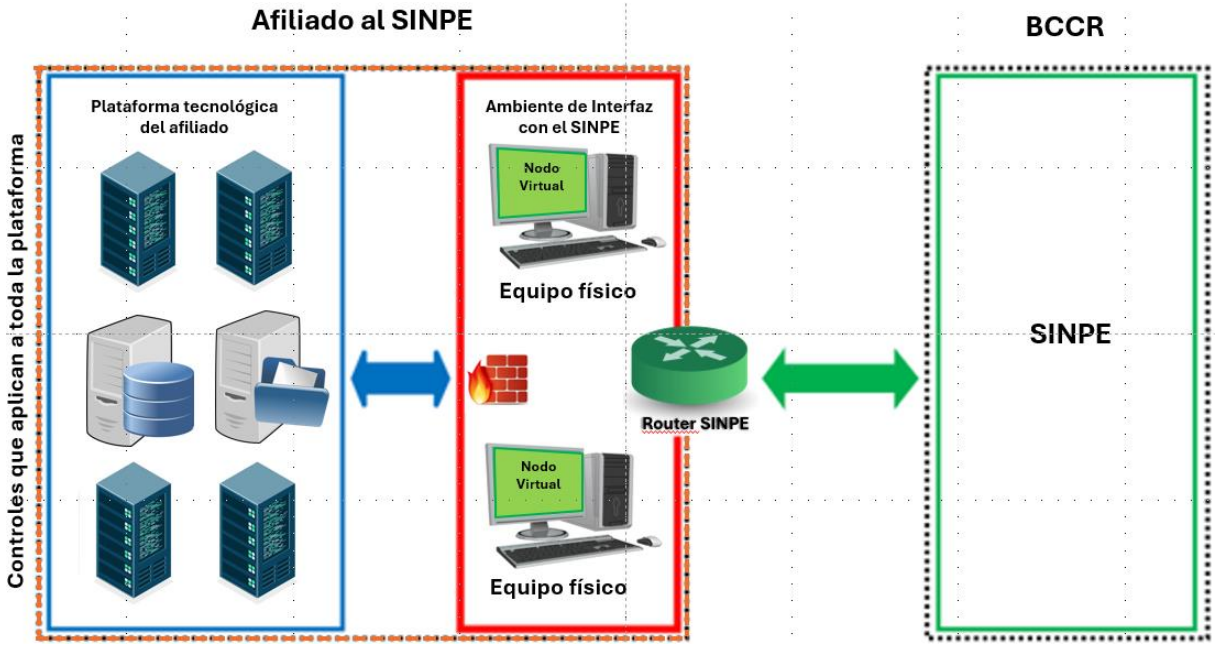
2. Alcance

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 descritos en esta Norma aplican para el Ambiente de Interfaz con el SINPE (AIS), a excepción de los controles en los apartados 6.8 y 6.9; asociados con la protección del correo electrónico, la navegación por Internet y la protección contra código malicioso. Dichos apartados atienden aspectos que actualmente son los principales vectores para la generación de ciberataques, por lo cual deben ser aplicados en toda la plataforma tecnológica de la entidad afiliada y no limitarse al AIS.

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. Normativa relacionada

Siglas	Nombre del documento
RSP	Reglamento del Sistema de Pagos
NC-RPS	Normativa Complementaria - Requisitos para participar en el SINPE
NC-GDR	Normativa Complementaria - Gestión de Riesgos
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 para el período siguiente de evaluación.

5.1. Ámbito de aplicación

Esta norma técnica regula los siguientes ámbitos de las entidades afiliadas.

- Plataforma tecnológica requerida para la operación con el SINPE.
- Servidores y otros equipos interconectados al SINPE.
- Usuarios del SINPE y aquellos con acceso a la plataforma del AIS.
- Capa de intercambio de datos entre el AIS y la plataforma de la entidad afiliada.
- Equipos de conexión al SINPE.

Para la correcta interpretación del ámbito de aplicación antes descrito, es importante tener en cuenta las siguientes consideraciones:

- Para algunos controles se podrá requerir su aplicación más allá del AIS. Esto será indicado en el detalle de cada control.
- En los casos donde la entidad afiliada utilice los servicios de un tercero para cualquiera de los aspectos considerados en el ámbito de aplicación de esta norma, los mismos serán contemplados dentro del alcance de la evaluación y la responsabilidad de su cumplimiento recaerá siempre en la entidad afiliada.

5.2. Tipos de controles

Cada entidad afiliada debe cumplir con los siguientes controles, según corresponda. El ícono junto a cada tipo de control se utilizará para facilitar su identificación.

Es de vital importancia considerar que los controles pueden ser actualizados de acuerdo con las variaciones en las condiciones del entorno de ciberseguridad. Así mismo, su nivel de cumplimento podrá modificarse o podrán incluirse nuevos requerimientos según sea necesario para la protección y el resguardo de la ciberseguridad del SINPE.

5.2.1. Controles obligatorios

Controles de acatamiento obligatorio que deben de ser atendidos de forma integral y en todos sus aspectos. Si cualquiera de estos controles no se satisface adecuadamente, el informe completo se considerará en incumplimiento y deberá indicarlo de esta forma.

5.2.2. Controles opcionales

Controles que permiten reforzar la postura de ciberseguridad de la entidad afiliada y del SINPE. Es importante que se valore su cumplimiento y revisión. Estos controles podrán pasar a ser obligatorios en próximas versiones de la norma.

5.2.3. Controles No Aplicables

Controles que no aplican según la categoría de conexión al SINPE en que se encuentre catalogada la entidad. Estos controles no deben ser evaluados.

5.3. Tipos de conexión con el SINPE

Cada entidad afiliada puede representar diferentes niveles de exposición a riesgos de ciberseguridad para el SINPE, dependiendo de cuáles sean los canales que utilice para realizar sus transacciones e interacciones y de cuáles sean los servicios autorizados específicamente a la entidad.

Con base en lo anterior, se han definido dos categorías en las que se puede clasificar una entidad afiliada. De acuerdo con la categoría que corresponda, se determina el nivel de cumplimiento que será exigible a cada entidad mediante la indicación de cuáles controles le son aplicables y cuáles no.

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

Entidades que utilizan al menos un servicio por medio del consumo de *web services* expuestos por el SINPE. Algunos ejemplos de estos servicios son: PIN y MONEX (cuando se usan *web services* para reportar al BCCR). En estos casos, se exigirá el cumplimiento de más controles para garantizar la protección de todo el sistema.

Cuando una entidad consume este tipo de servicios a través de un proveedor, igualmente le aplicará la clasificación de Categoría 1 y se realizará la evaluación correspondiente. Esto será indistinto del esquema de comunicación que se utilice entre la entidad responsable y su proveedor; aplicando incluso cuando el uso de estos servicios se realice desde terminales específicas aprovisionadas por el tercero. Estas consideraciones también son aplicables cuando los servicios son aprovisionados por otras entidades del mismo grupo de interés económico, instituciones que trabajan en conjunto o similares; así como en el caso de entidades adquiridas por otra afiliada o entidades que están siendo intervenidas, entre otros.

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

Entidades que no utilizan ningún servicio con exposición mediante *web services*, es decir, que solo utilizan determinados servicios, accediendo a ellos directamente desde la terminal conectada a SINPE. Algunos servicios bajo este esquema son AES y MIL.

Cuando una entidad afiliada que se ubica en esta categoría solicite autorización para el acceso a nuevos servicios que requieren conexión mediante *web services*; deberá cumplir con los requisitos definidos para la Categoría 1, previo a ser autorizada para el uso de los nuevos servicios. Para ello, la entidad interesada deberá seguir el proceso de revisión y cumplimiento definido en esta norma para la categoría correspondiente.

5.4. Cumplimiento

Las entidades afiliadas al SINPE y las interesadas en afiliarse, deberán cumplir con los requisitos aquí descritos para que se mantenga vigente su afiliación o se les permita ingresar según corresponda.

5.4.1. Informe de auditoría

La entidad deberá presentar un informe de cumplimiento emitido por parte de un auditor, en el que se especifique que la entidad cumple con la totalidad de los controles aplicables, según la categoría correspondiente. En caso de que alguno de los controles no se cumpla de acuerdo con los términos establecidos en esta norma, el informe deberá indicar que la entidad se encuentra en incumplimiento y deberá seguirse el proceso de remediación aquí definido.

El informe no podrá tener más de seis meses de emitido y el periodo auditado deberá dar continuidad al periodo equivalente del último informe presentado por la entidad; de manera que no queden periodos descubiertos entre auditorías. Para el caso de entidades en proceso de afiliación, el primer periodo auditado podrá variar según el criterio de la auditoría.

Para la elaboración del informe se deberá seguir el esquema indicado en el

Anexo de esta norma, incluyendo como mínimo la información que allí se solicita. En caso de que el informe no contenga la información requerida, o cuando la misma no sea fácilmente identificable; se considerará que el informe está en incumplimiento hasta que se corrija y sea presentado como corresponde. Lo anterior no altera de ninguna manera, los plazos definidos para el cumplimiento de la norma, los cuales se indican más adelante.

En caso de que la entidad utilice servicios de proveedores externos, deberá incluir los informes de cumplimiento de la parte atendida por estos proveedores. En el informe debe quedar explícitamente detallado, cuál es el alcance de cada informe, cuáles controles son atendidos por los proveedores externos y cuáles por la propia entidad. La entidad es siempre responsable por el cumplimiento de la totalidad de los controles que le aplican, según lo establecido en esta norma.

5.4.2. Atestados del auditor

Con la finalidad de garantizar que las labores de auditoría y presentación de resultados sean ejecutadas con el conocimiento, experiencia y respaldo necesarios; la persona a cargo del informe deberá contar, al menos, con alguna de las siguientes certificaciones:

- ISACA
  - Auditor Certificado de Sistemas de Información – CISA.
  - Gestor Certificado de Seguridad de la Información – CISM.
- ISC2
  - Profesional Certificado en Seguridad de Sistemas de Información – CISSP.
  - Profesional Certificado en Seguridad de Sistemas – SSCP.
- ISO
  - Auditor Líder ISO 27001.

Los atestados correspondientes, deberán ser anexados en el informe de auditoría. La entidad es responsable de verificar y dar garantía ante el BCCR de que la persona a cargo de la auditoría y responsable por el informe cumpla con los atestados exigidos por esta norma. En caso de que se incumpla este requisito, el BCCR dará como inválido el informe presentado.

El BCCR no tendrá relación o coordinación con los auditores, por lo que toda consulta o coordinación debe ser realizada directamente por medio del afiliado y su Responsable de Servicios.

5.4.3. Presentación del informe

El informe debe ser remitido al Departamento Sistema Nacional de Pagos Electrónicos del BCCR, por medio de un caso creado por la persona **Responsable de Servicios** o **Informático Titular** de la entidad. Además, deberá ser acompañado por un oficio formal, firmado digitalmente por un **Representante Legal** o autoridad equivalente de la entidad.

Para la creación del caso y presentación del informe, se deberá utilizar exclusivamente el canal seguro establecido por el BCCR en la asistencia de Atención al Ciudadano. Para el caso de nuevas entidades el canal designado será por medio de la extranet, el cual debe ser coordinado por el personal que le atiende en su conexión. Debido a la criticidad de la información contenida en los informes, estos no se recibirán por otro canal que no sea el antes indicado. No se atenderá ningún informe remitido por medios como el correo electrónico u otros no oficiales, pues se considera que son canales no seguros.

En el caso de la extranet, las credenciales de acceso para el sitio donde se deberá incluir los documentos requeridos, serán remitidas únicamente al Responsable de Servicios designado por la

entidad. Es responsabilidad exclusiva de la entidad mantener actualizada la información de la persona responsable y gestionar ante el BCCR el otorgamiento de nuevas credenciales en caso de ser necesario.

5.4.4. Periodicidad

El informe de cumplimiento deberá ser presentado durante el primer semestre de cada año, con fecha límite al 30 de junio. Dicho informe tendrá validez por un año, en un periodo que va desde el 1 de julio del año en curso hasta el 30 de junio del año siguiente, cuando ya se debe haber presentado el siguiente informe. La entidad afiliada deberá estar atenta a la respuesta del BCCR sobre el estado de su informe y garantizar que el correo electrónico de su Responsable de Servicios se encuentra en funcionamiento; en caso contrario, deberá dar seguimiento para la certeza de las comunicaciones oficiales.

Las entidades interesadas en participar del SINPE, deberán cumplir con la totalidad de los requisitos aplicables para poder afiliarse. Y en este caso, el informe tendrá validez desde que sea aceptado por el BCCR y hasta el próximo 30 de junio.

5.4.5. Incumplimiento

Cuando el informe establezca controles con incumplimiento, la entidad debe aportar un plan remedial para solventar las brechas detectadas. Dicho plan remedial deberá incluir acciones concretas que aseguren el cumplimiento del control y su ejecución deberá finalizarse a más tardar el 31 de octubre del año en curso. Una vez atendidos los incumplimientos, la entidad deberá presentar un nuevo informe que incluya el seguimiento al plan remedial establecido y la evaluación de los controles nuevamente. Para la presentación del nuevo informe, se debe seguir todo lo indicado en los apartados anteriores.

En el caso de que un informe presente puntos a resolver detectados en la revisión por parte del BCCR, la entidad deberá atender estas observaciones en un plazo no mayor a 1 mes natural posterior a la notificación oficial del BCCR. Una vez realizadas las acciones requeridas, la entidad deberá enviar nuevamente el informe completo, con los ajustes necesarios y evidencia clara de cómo fueron atendidas las observaciones.

Otro elemento que será considerado como incumplimiento, es cuando se detecte que la auditoría ha realizado copia de algún otro informe. Esto debilita la confianza en el informe realizado al detectarse incongruencias en el mismo, y podrá conllevar una solicitud de cambio en el equipo de auditoría.

Una vez agotados las opciones y plazos para solventar incumplimientos, si los mismos siguen presentes, se considerará que la entidad está en condición de incumplimiento de la norma y 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 entorno de ciberseguridad del SINPE, el BCCR podrá ordenar la apertura de un proceso sancionatorio para determinar las acciones correspondientes.

5.4.6. Incidentes de Ciberseguridad

En caso de que una entidad afiliada enfrente un incidente de ciberseguridad, este deberá ser reportado oportunamente mediante los canales establecidos por el BCCR. Según el tipo de incidente la entidad deberá:

- **Incidente que no afecta el Ambiente de Interfaz con el SINPE:** acatar lo dispuesto en la Norma Complementaria de Gestión de Riesgos.

- **Incidente que afecta el Ambiente de Interfaz con el SINPE:** acatar lo dispuesto en la Norma Complementaria de Gestión de Riesgos. Posteriormente, deberá realizar una recertificación de los controles que fueron ajustados o modificados producto de la atención del incidente de ciberseguridad.

La ejecución de la recertificación incluye:

- Verificar el cumplimiento efectivo de los controles afectados en el incidente y las debilidades observadas, y si estas se deben a fallas en la implementación, mantenimiento o diseño del control. Si existe una duda razonable de que otros controles fueron vulnerados, el auditor debe incluirlos en dicha recertificación
- Establecer si los controles nuevos o ajustados, serán adecuados para la mitigación de futuros incidentes, procurando validar que sean efectivos.
- Este informe debe ser enviado bajo el mismo proceso con el cual se envía el informe de cumplimiento anual y será requisito para la reconexión de la entidad.

6. Detalle de los controles

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

- **Tipos de controles**: validar si el control es obligatorio, opcional o no aplicable. Esto, según la indicación en cada control y lo que se define en el apartado 5.2.
- **Tipo de afiliado**: valorar si la entidad está catalogada como **categoría 1** o como **categoría 2** de acuerdo con lo establecido en el apartado 5.3.

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 instaladas, las versiones de software que cuenten con el debido soporte y que no hayan concluido su ciclo de vida.			

6.2.2	Establecer una lista de software autorizado	**Categoría 1**	**Categoría 2**
		+	+
Se deberá definir y mantener un listado del software autorizado o permitido para su instalación en el Ambiente de Interfaz con el SINPE. Actualizar, al menos cada 6 meses, la lista de software autorizado. De manera complementaria, se deberán implementar controles para detectar y eliminar el software que no forme parte de la lista autorizada 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 en efectivo y valores, identificación y nombre del cliente origen y destino de las transacciones.			
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 de la entidad afiliada y el Ambiente de Interfaz con el SINPE (AIS). El cifrado debe hacerse mediante protocolos considerados seguros por las buenas prácticas internacionales. *NOTA: Este control se debe implementar entre la plataforma tecnológica de la entidad afiliada y el ambiente AIS, por ejemplo, entre aplicaciones o sistemas transaccionales de la entidad que intercambian información con los nodos del SINPE o con otros aplicativos (propios o de terceros) que integran el AIS. Este control NO se trata de asegurar que la comunicación está cifrada entre los nodos de conexión y el SINPE (BCCR), ya que esa parte es gestionada por el BCCR.*			
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.

		Categoría 1	Categoría 2
6.4.1	Establecer y mantener un proceso de configuración seguro	+	+
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	+	+
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.

		Categoría 1	Categoría 2
6.5.1	Establecer y mantener un inventario de cuentas	+	+
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 documentado un proceso de gestión de vulnerabilidades para toda la infraestructura del Ambiente de Interfaz con el SINPE que cubra al menos, análisis, priorización y remediación de vulnerabilidades. Revisar y actualizar esta 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 dicho ambiente. 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 un proceso de parchado o aplicación de actualizaciones y ejecutarlo, al menos de forma semestral, para toda la infraestructura del Ambiente de Interfaz con el SINPE.			

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.

NOTA: Estos controles se deben implementar en toda la plataforma tecnológica de la entidad afiliada.

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 peligrosos o no aprobados. Documentar y aprobar formalmente las excepciones.			
6.8.2	Implementar protección contra correo no deseado	**Categoría 1**	**Categoría 2**
		⊕	⊕
Implementar una solución o herramienta de filtrado de correo con el propósito de reducir la cantidad de mensajes de correo no deseado (*spam, phishing, etc.*) que llegan a la bandeja de correo de los usuarios. Mantener actualizada la solución para garantizar un filtrado efectivo.			
6.8.3	Implementar protección antimalware a nivel de correo electrónico	**Categoría 1**	**Categoría 2**
		⊕	⊕
Implementar protección antimalware para el correo electrónico, como el análisis de archivos adjuntos y el espacio aislado. Estas técnicas de protección deberán aplicarse en el servidor o plataforma de correo electrónico, antes de que los correos sean entregados a los usuarios. Gestionar las actualizaciones necesarias para mantener una protección efectiva.			
6.8.4	Bloquear archivos innecesarios	**Categoría 1**	**Categoría 2**
		⊕	⊕
Establecer e implementar una política de bloqueo de archivos adjuntos en el correo electrónico para restringir el envío o recepción de archivos riesgosos, desconocidos, con versiones descontinuadas o vulnerables; archivos innecesarios para el trabajo, entre otros. Revisar y actualizar 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 plataforma tecnológica de la entidad, como una medida para prevenir infecciones que pudieran generar fugas de información, denegación de servicios o daños a los activos.

NOTA: Estos controles se deben implementar en toda la plataforma tecnológica de la entidad afiliada.

6.9.1	Implementar y mantener software contra código malicioso	**Categoría 1**	**Categoría 2**
			
Implementar software de protección contra código malicioso en todos los *endpoints* de la plataforma tecnológica. Asegurarse de incluir este software como parte de la configuración inicial de nuevos equipos de usuario, máquinas virtuales, servidores y cualquier *endpoint*. Llevar a cabo revisiones periódicas para asegurar la correcta aplicación de este control.			
6.9.2	Actualizar de forma automática las firmas contra código malicioso	**Categoría 1**	**Categoría 2**
			
Configurar las actualizaciones automáticas para la solución de protección contra código malicioso, de manera que se asegure la protección más actualizada contra amenazas de este tipo sin requerir intervención humana.			
6.9.3	Utilizar herramientas de protección basadas en comportamiento	**Categoría 1**	**Categoría 2**
			
Implementar software de protección contra código malicioso basado en comportamiento, en todos los *endpoints* de la plataforma tecnológica. Asegurarse de incluir este software como parte de la configuración inicial de nuevos equipos de usuario, máquinas virtuales, servidores y cualquier *endpoint*. Configurar las actualizaciones automáticas para la solución de protección contra código malicioso basada en comportamiento, de manera que se asegure la protección más actualizada contra amenazas de este tipo sin requerir intervención humana. Llevar a cabo revisiones periódicas para asegurar la correcta aplicación de este control.			

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 entidad 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 la entidad 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 que interactúan con el Ambiente de Interfaz con SINPE. El proceso debe incluir elementos tales como: ⊡ Una política de manejo de vulnerabilidades de las aplicaciones durante todo su ciclo de vida. ⊡ Un proceso de identificación, asignación, remediación y pruebas de remediación de las vulnerabilidades reportadas en las aplicaciones. 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:

- **Información de la entidad:** nombre y código de la entidad afiliada o en proceso de afiliación a la que corresponde el informe. Detalle del periodo evaluado que cubre el informe. Debe incluir dentro del informe los proveedores que le brindan soporte relacionados con el SINPE y que serán parte de la evaluación.
- **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 este apartado se deberá indicar el código y nombre de la entidad afiliada, o en el caso de informes a nivel de grupo, los datos de cada entidad afiliada que se incluye en su alcance.
- **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	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,	El auditor deberá indicar para cada control su condición en los siguientes términos: **“Cumple”** o **“No cumple”**.

ID del control	Detalle del control	Detalle de cumplimiento validado por la auditoría	Estado de cumplimiento
	utilizar como criterio de auditoría.	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 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 en 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.