BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

LINEAMIENTOS PARA LA RESPUESTA Y RECUPERACIÓN ANTE CIBERINCIDENTES (RRCI)

-Última comunicación incorporada: "A" 8280-

Texto ordenado al 17/07/2025

B.C.R.A.	TEXTO ORDENADO SOBRE LINEAMIENTOS PARA LA RESPUESTA Y RECUPERACIÓN ANTE CIBERINCIDENTES (RRCI)

- Índice -

1.1. Objetivo.

Estos lineamientos están destinados a los sujetos contemplados en el punto 1.2., y se componen de una serie de prácticas efectivas de respuesta y recuperación ante ciberincidentes con el fin de limitar los riesgos en la estabilidad financiera e impulsar la ciberresiliencia del ecosistema en su conjunto. Por su carácter general, pueden ser también adaptados y adoptados por cualquier institución del sistema financiero, los proveedores de servicios de tecnología informática y/o comunicación y demás sectores.

La respuesta se refiere a las actividades que se inician en reacción a un ciberincidente detectado o reportado, mientras que la recuperación se encarga de las actividades que se ejecutan con el fin de restaurar los sistemas, servicios u operaciones que fueron perjudicados debido al ciberincidente.

El Banco Central de la República Argentina (BCRA) considera los lineamientos establecidos en la Sección 2. como una buena práctica en materia de respuesta y recuperación de incidentes, siendo de aplicación obligatoria la Sección 3.

1.2. Sujetos alcanzados.

- Entidades financieras.
- Proveedores de servicios de pago (PSP) incluidos en el Registro de PSP del BCRA.
- Infraestructuras del mercado financiero conocidas como sistemas de pago de importancia sistémica.

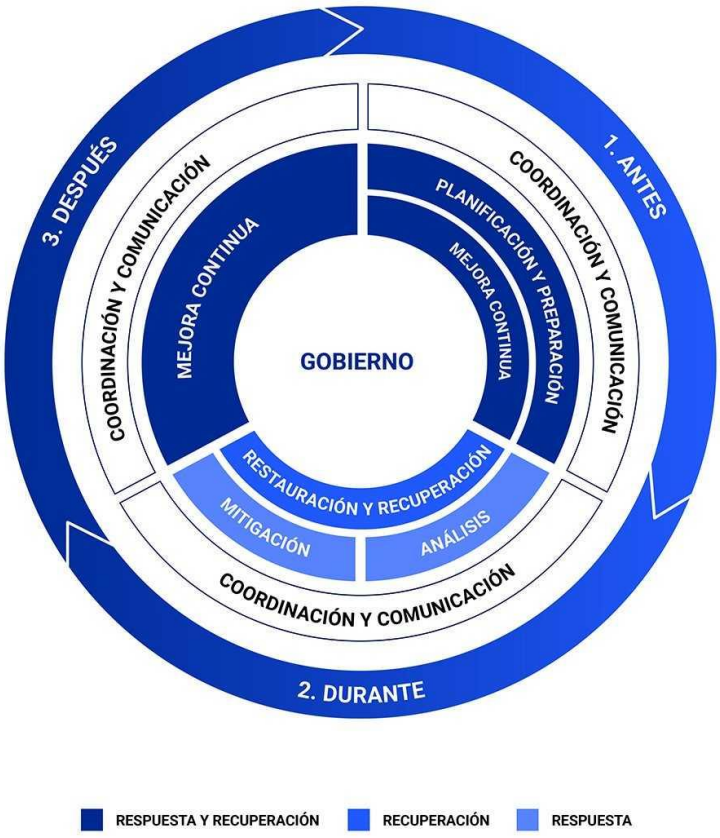
Los sujetos alcanzados analizarán efectivamente la implementación de los lineamientos pudiendo elegir implementar las prácticas que sean adecuadas para sus modelos de negocios, teniendo en cuenta su tamaño, complejidad o riesgos en relación con el ecosistema financiero.

Se dejará constancia escrita de los fundamentos de los criterios de implementación adoptados, los que deberán ser puestos a disposición de la Superintendencia de Entidades Financieras y Cambiarias (SEFYC), cuando esta lo solicite.

Los lineamientos de respuesta y recuperación ante ciberincidentes son los siguientes:

- Gobierno.
- Planificación y preparación.
- Análisis.
- Mitigación.
- Restauración y recuperación.
- Coordinación y comunicación.
- Mejora continua.

Cada uno de estos lineamientos tendrá una función primordial dependiendo del momento del ciberincidente: antes, durante y después del mismo.



2.1. Gobierno.

El presente lineamiento establece un marco de gobierno en el que se organizan y gestionan las actividades de respuesta y recuperación ante ciberincidentes, ajusta estas actividades a los objetivos de la continuidad del negocio, establece la estructura de la entidad y los roles necesarios para la coordinación de estas actividades entre las distintas funciones o unidades de negocio.

Define un marco para la toma de decisiones, asignando roles y responsabilidades de forma tal que se involucre a los participantes internos y externos necesarios cuando ocurre un ciberincidente.

Contar con el impulso de la dirección de la entidad, posibilitará la implementación de los mecanismos para promover las actividades de respuesta y recuperación y crear una cultura positiva, que acepte la eventual ocurrencia de los ciberincidentes, los enfrente y gestione apropiadamente.

2.1.1. Cultura.

Se espera que la dirección de la entidad acompañe la creación de un entorno organizacional donde se promueva reportar o escalar ciberincidentes mediante un canal establecido para tal fin, considerando:

2.1.1.1. El establecimiento de programas de capacitación para todos los niveles de la entidad, que fomenten comportamientos proactivos, donde se acepte la posibilidad de ocurrencia de los ciberincidentes y el aprendizaje en base a los errores.

2.1.1.2. Promover una cultura positiva hacia la gestión de ciberincidentes, logrando que se use esa información como fuente para mejorar la etapa de preparación.

2.1.1.3. Promover acciones continuas y sostenidas con proveedores y terceras partes en la preparación de las tareas de respuesta y recuperación ante ciberincidentes, para que puedan ser oportunas y adaptarse a las distintas situaciones.

2.1.2. Organización, roles, funciones y responsabilidades.

2.1.2.1. El gobierno de las actividades de respuesta y recuperación forma parte del gobierno general de la organización. Los objetivos y prioridades de estos lineamientos se tendrían que alinear con la gestión del riesgo general de la organización, de idéntica forma tienen que definirse los roles y responsabilidades y los procesos necesarios para facilitar la toma de decisiones.

2.1.2.2. La dirección de la organización es responsable de la definición de los objetivos de ciberresiliencia, como así también de que se implementen las políticas, procedimientos y controles relacionados.

2.1.2.3. Para las acciones de coordinación y comunicación ante un ciberincidente, es recomendable definir un rol de “coordinador”, pudiendo ser una persona o grupo. Dependiendo de la criticidad, el “coordinador” debe tener la capacidad de tomar decisiones durante el ciberincidente, para iniciar determinadas actividades y contactar a los involucrados.

2.1.2.4. Las actividades de respuesta y recuperación ante ciberincidentes ayudan a garantizar la seguridad y confiabilidad de los servicios financieros. La dirección de la entidad puede impulsar estas actividades no solo brindando su apoyo, sino también asignando el presupuesto necesario para la adquisición de herramientas tecnológicas o la implementación de programas de concientización, formación y comunicación en todos los niveles de la organización, entre otras.

2.1.3. Informes, métricas y rendición de cuentas de las actividades.

Una gestión eficaz se logra estableciendo métricas para evaluar el impacto de los ciberincidentes, para medir la eficiencia de las actividades de respuesta y recuperación, y elaborar los informes correspondientes a las autoridades. En función de la criticidad y/o prioridad del incidente, se definirá la urgencia de atención y el nivel de escalamiento adecuado, dado que por ejemplo un ciberincidente de alta criticidad, muy probablemente requerirá ser informado a la dirección de la entidad.

2.2. Planificación y preparación.

Este lineamiento trata el establecimiento y mantenimiento de las capacidades de la organización para responder, recuperarse y restablecer actividades críticas, sistemas y datos comprometidos en un ciberincidente hasta volver a la operación normal. Prepararse previo a la ocurrencia de un incidente juega un rol significativo en la efectividad de las actividades de respuesta y recuperación.

2.2.1. Políticas, planes y procedimientos.

2.2.1.1. La organización debería definir en sus políticas el nivel de involucramiento con las actividades de respuesta y recuperación ante ciberincidentes, de acuerdo con su tamaño, complejidad y riesgo. Las políticas pueden abarcar, entre otros temas, sobre la clasificación y evaluación de los incidentes, sobre la estrategia y el plan de comunicación que establezca a quién y cuándo informar, de acuerdo con escenarios y tiempos preestablecidos.

2.2.1.2. Los planes y procedimientos deberían incluir los criterios necesarios para saber cuándo activar las medidas y cómo responder ante ciberincidentes, de forma de acelerar las acciones. En su elaboración deberían participar las distintas áreas de la organización, para incorporar sus requerimientos.

2.2.2. Estrategia, canales y planes de comunicación.

2.2.2.1. Se deben establecer listas de contactos de todos los posibles involucrados, tanto internos como externos, a los que se deberían informar dependiendo de los escenarios y criterios identificados.

2.2.2.2. Resulta aconsejable establecer estrategias de comunicación con los participantes y cada uno de los públicos identificados. Los planes pueden incluir modelos de posibles contenidos a informar de acuerdo con el tipo de ciberincidentes teniendo en cuenta el canal de comunicación apropiado o disponible. Se considera conveniente evaluar la secuencia de información a publicar durante un incidente teniendo en cuenta la audiencia con la que se comparte y las necesidades de mantener informado a los involucrados de forma de reducir la incertidumbre y aumentar la confianza.

2.2.3. Escenarios y criterios de evaluación de incidentes.

2.2.3.1. Los planes y procedimientos deben incluir la criticidad de los posibles escenarios basados en eventos de baja probabilidad y alto impacto respaldados por información de inteligencia en amenazas. Estos escenarios pueden: i) evaluarse durante las pruebas del Plan de Continuidad del Negocio o del plan respuesta y recuperación, y ii) probarse de manera interna, con externos, con autoridades relevantes, proveedores de servicios o terceras partes, cuando corresponda.

2.2.3.2. La eficacia de las actividades de RRCI se pueden evaluar durante una prueba y ante los incidentes reales. Se recomienda la participación de observadores independientes para mantener una evaluación objetiva y obtener registros precisos de cada paso, así como la documentación de acciones y la toma de decisión realizada durante y después de un ciberincidente.

2.2.4. Infraestructuras para la recuperación.

Dependiendo del tamaño, la complejidad y el riesgo de la entidad, podría resultar necesario monitorear 24x7 o utilizar servicios de seguridad de un tercero para lograr el objetivo de identificar, detectar, responder e investigar ciberincidentes que pueden afectar a la infraestructura, servicios y/o clientes.

2.2.5. Recuperación ante desastres e infraestructura de resiliencia.

La resiliencia se construye mediante el uso de infraestructura diversificada y la replicación de sistemas críticos, sitios de recuperación ante desastres o sitios alternativos con diferentes perfiles de riesgo geográficos. Para ello es necesario identificar el riesgo en los terceros externos, evaluar y adoptar técnicas de mitigación cuando estén disponibles.

2.2.6. Capacidades y registros para la investigación.

El desarrollo de una adecuada gestión de “logs”, comprende herramientas para recopilar y almacenar registros del sistema que serán necesarios para la investigación y el análisis de incidentes. Los tipos de “logs” o registros que se recopilan y el período de retención deben definirse con anterioridad, en función a la clasificación de la información, de las normas y regulaciones vigentes. Las capacidades técnicas y forenses son necesarias para preservar la evidencia y analizar fallas de control, identificar problemas de seguridad y otras causas relacionadas con un ciberincidente. En caso de no contar con capacidades propias, se puede contratar un servicio de terceros. Es necesario que el personal que realiza el trabajo forense esté adecuadamente capacitado y siga procedimientos estandarizados para preservar la integridad de las pruebas, los datos y los sistemas durante las investigaciones.

2.2.7. Proveedores de servicios.

Para garantizar una respuesta adecuada durante los ciberincidentes, se estima necesario contar con un detalle de los servicios contratados a terceros, los proveedores de esos servicios, y de los datos clave de los acuerdos como la información de contacto del proveedor de servicios, el período de validez y los niveles de servicio acordados. También se tienen que revisar los acuerdos de servicio de los subcontratistas. En relación con la complejidad y tamaño del servicio, cabe evaluar los ciberincidentes de los proveedores, especialmente los riesgos de sus prácticas de ciberseguridad en almacenamiento de datos en terceros y/o vulnerabilidades de seguridad del "software" en la gestión de la cadena de suministro o sistemas de proveedores.

2.3. Análisis.

Este lineamiento hace referencia al análisis forense, la determinación de criticidad e impacto del ciberincidente y la investigación de la causa que lo originó o causa raíz.

2.3.1. Taxonomía de ciberincidentes.

2.3.1.1. Se requiere una taxonomía predefinida para clasificar ciberincidentes de acuerdo con parámetros tales como: tipo de incidente, actores de amenazas, vectores de amenazas y sus impactos, y un marco preestablecido de evaluación para priorizar la atención de los incidentes en función a la criticidad de los sistemas o servicios.

2.3.1.2. Contar con análisis preestablecidos de los ciberincidentes ayuda a priorizar la atención oportuna y asignar recursos para mitigar el impacto, restablecer servicios y recuperarse, al mismo tiempo, permite que se comunique la información con un lenguaje simple. Los niveles de criticidad se establecen para dar una respuesta inmediata, ya que las primeras horas después de un incidente suelen ser las más críticas para su contención. Asimismo, este enfoque permite una primera atención sin conocer de manera completa el incidente.

2.3.2. Investigación forense y análisis.

2.3.2.1. Para la investigación forense del incidente se requiere contar con "logs" o registros de auditoría de los sistemas y de los dispositivos. Analizar las alertas, indicadores (de seguridad y sistemas), investigar y correlacionar eventos posibilitará al equipo de respuesta determinar el impacto de un incidente y posiblemente identificar el origen. Para la respuesta, también se recuperan datos de los dispositivos informáticos involucrados en la interacción como los conectados a la red, procesos en ejecución, sesiones de usuarios, archivos abiertos, de los equipos relevantes sus configuraciones y contenidos de memoria, entre otros. La integridad de dichos datos debe asegurarse para un adecuado análisis.

2.3.2.2. Al momento de una investigación forense será importante que los sistemas de donde se obtengan los registros de sistemas se encuentren sincronizados.

2.3.2.3. Se recomienda contar con diversas fuentes de información tanto internas como externas para una evaluación rápida de las amenazas y de las causas de un ciberincidente.

2.4. Mitigación.

Este lineamiento se refiere a las medidas de mitigación que tienen como finalidad prevenir el agravamiento de la situación y erradicar o eliminar las consecuencias de los incidentes de manera oportuna para minimizar su impacto en las operaciones y servicios.

2.4.1. Contención, aislamiento y erradicación.

2.4.1.1. Las medidas de contención se despliegan de acuerdo con el tipo de ciberincidente para evitar que cause más daños tanto dentro de un sujeto alcanzado como a las demás con las que se conecta o relaciona. Contar con información sobre las ciberamenazas actuales, en forma de indicadores de compromiso y analizar los posibles impactos también contribuye en la definición de medidas de contención, en el monitoreo de la actividad de las redes y para la toma de decisiones. Ocurrido un incidente, la cobertura de los seguros podría ser de ayuda en la recuperación.

2.4.1.2. En caso de incidentes graves, para tomar la decisión de apagar, desconectar o aislar parte de los sistemas o redes como medida de mitigación o seguir brindando servicio, se deberán considerar los costos, el impacto en el “Negocio” y los riesgos operativos entre otros.

2.4.1.3. Luego de la obtención de evidencia y su preservación, todos los elementos que hubieran sido introducidos por los atacantes deben ser eliminados, tal como código malicioso y datos, entre otros. Asimismo, se tendrá que corregir las configuraciones o alteraciones a los sistemas que se hayan visto afectados. Entre las actividades para la erradicación del incidente se podría incluir tareas como, el parcheo de vulnerabilidades y su comprobación, entre otras.

2.4.2. Medidas para la “continuidad del negocio”.

Dependiendo de la criticidad del ciberincidente y de acuerdo con sus consecuencias o impacto, se podría activar el Plan de Continuidad del Negocio.

2.5. Restauración y recuperación.

Este lineamiento hace referencia a la restauración de los sistemas y activos afectados por un ciberincidente, las actividades que se realizan para recuperar las operaciones y los servicios afectados, a su estado habitual, de manera segura.

2.5.1. Priorización.

La priorización de las actividades de recuperación tiene que realizarse en función de la criticidad de los procesos de negocio, para recuperar los datos y los sistemas que les brindan soporte. Se resalta la importancia de contar con un listado actualizado de contactos internos y externos.

2.5.2. Recuperación de datos.

2.5.2.1. Para cumplir con los requisitos del negocio en la recuperación de datos, se requiere contar con la información necesaria tanto en locaciones propias como de terceros y, en este sentido, ocurrido un ciberincidente, se tiene que garantizar la integridad de los datos, es decir, que no se hayan manipulado ni corrompido antes de la restauración. Para garantizar la integridad, disponibilidad y legibilidad de los datos, también es necesario realizar pruebas de restauración periódicamente.

2.5.2.2. Es conveniente que las actividades de restauración cuenten con procedimientos automatizados, documentados y probados, así se reduce el riesgo de error humano que puede surgir en una restauración manual. Para restaurar los sistemas afectados, se suele utilizar imágenes e instantáneas del sistema que no se hayan comprometido, éstas se tienen que revisar, probar y almacenar de forma segura con regularidad para mitigar daños o destrucción.

2.5.2.3. Cuando no sea posible lograr la restauración de todos los sistemas, se pueden considerar las restauraciones parciales, tener previsto como se operará a un nivel de capacidad inferior; asimismo se definen hitos clave en la reinstalación y reconfiguración de los sistemas para asegurar recuperaciones efectivas.

2.5.3. Monitoreo.

Monitorear la red, los sistemas y los proveedores de servicios durante el proceso de restauración de los activos de la infraestructura tecnológica es primordial para detectar actividades anormales. Cuando corresponda y de acuerdo con su tamaño, complejidad y riesgos, es conveniente incluir en los acuerdos de servicio con el proveedor las capacidades de monitoreo durante la restauración de datos.

2.5.4. Validación.

Antes que los sistemas y los servicios vuelvan a la operación normal, se tiene que validar la integridad de los activos informáticos restaurados y asegurar que no se encuentren comprometidos, que sean funcionales y que cumplen con los requisitos de seguridad.

2.5.5. Registro de actividades.

Se deben documentar y registrar, en la medida de lo posible, todas las acciones encaradas desde el momento en que se detectó el incidente, hasta su resolución final, para posibilitar su seguimiento. Recuperadas las operaciones, los registros facilitarán poder revertir las acciones tomadas hasta restablecer las condiciones previas al incidente o solucionar problemas en caso de que las acciones de recuperación no tengan éxito. Será necesario registrar las herramientas y los artefactos, tales como “scripts”, cambios de configuración entre otros, utilizados en la restauración y recuperación para un futuro uso o para la mejora de procesos y/o sistemas actuales.

2.6. Coordinación y comunicación.

Durante el ciclo de vida de un ciberincidente, los sujetos alcanzados coordinan las partes interesadas de confianza para mantenerlos al tanto de la situación, para brindar una respuesta y atención común sobre las amenazas y mejorar la ciberresiliencia del sistema. Es necesario definir un lenguaje, una frecuencia y la granularidad necesaria para la comunicación de acuerdo con el tipo de público destinatario. La coordinación adecuada con los distintos actores involucrados tanto internos como externos, y con las autoridades permitirá que la comunicación sea oportuna y se alcancen los objetivos deseados.

2.6.1. Escalamiento oportuno.

Para un tratamiento oportuno hay que informar el incidente a cada grupo de interés sin demoras, de acuerdo con el marco de evaluación de la criticidad y los niveles de escalamiento previstos. También es importante que la comunicación a los proveedores de servicios se encuentre definida en los acuerdos de servicios. Es importante brindar las garantías razonables para asegurar que se brinda información completa y exacta en las comunicaciones tanto para las áreas internas como para las organizaciones externas.

2.6.2. Notificación de ciberincidentes.

2.6.2.1. Se debe reportar la información relevante de ciberincidentes a las autoridades según lo requieran y de acuerdo con los plazos establecidos por los marcos normativos correspondientes. Para respaldar la notificación efectiva y oportuna de ciberincidentes, tienen que desarrollar pautas internas sobre cuándo y a quién se debe informar los diferentes tipos de incidentes. Para mejorar la comprensión, se puede contar con ejemplos de diferentes tipos de incidentes y de informes.

2.6.2.2. Adicionalmente, los participantes que puedan verse afectados por posibles disrupciones originadas en un ciberincidente deberían ser informados para que puedan activar sus propios planes de respuesta y recuperación. La información compartida debe ser precisa, oportuna, clara y relevante; también deben mantenerse informadas con una frecuencia adecuada tanto las partes interesadas internas como externas, sin embargo, habrá que comunicar sin demora cuando sea urgente. Asimismo, deberán informarse las condiciones o restricciones al momento de la reanudación de los servicios críticos. En cada mensaje deben estar indicadas las acciones que se espera del destinatario, estableciendo de antemano la frecuencia.

2.6.3. Comunicación del ciberincidente al público.

Es necesario que la estrategia de comunicación esté predefinida y se recomienda un equipo de comunicación multidisciplinario conformado, entre otros, por representantes de las líneas de negocios afectadas, recursos humanos, prensa y comunicación, legales, tecnología y ciberseguridad, así como el coordinador de incidentes. Según el tipo de incidente, se puede solicitar la ayuda de otros especialistas. Para evitar la confusión en la comunicación, el vocero tendrá que consolidar la información y los distintos aspectos relevantes tanto de los expertos como de la gestión, para actualizar a los medios con información y mensajes consistentes. Se tiene que promover un uso estratégico de canales de comunicación como los medios convencionales y las redes sociales.

2.6.4. Intercambio de información.

2.6.4.1. Se recomienda que las organizaciones compartan información sobre ciberamenazas y ciberincidentes, estrategias efectivas de ciberseguridad y prácticas de gestión de riesgos, a través de plataformas o por los medios que crean conveniente implementar. Sera muy útil compartir información técnica, como indicadores de compromiso y vulnerabilidades que están siendo aprovechadas, tan pronto como esté disponible, asegurando el anonimato necesario para cumplir con sus acuerdos de confidencialidad.

2.6.4.2. Los canales de comunicación tienen que estar formalizados y garantizar la disponibilidad, integridad y confidencialidad de la información que se comparta. También es necesario que los participantes validen periódicamente la disponibilidad de los canales de comunicación y la lista de contactos.

2.7. Mejora continua.

Este lineamiento hace referencia a los procesos que se deben considerar para mejorar las actividades y capacidades de RRCI a través de las lecciones aprendidas en la resolución de los ciberincidentes y del uso de herramientas proactivas, en particular la realización de ejercicios, pruebas y simulacros. Las lecciones aprendidas se utilizan para mejorar o seleccionar e implementar controles como medidas de mitigación, incluidos cambios en las políticas, planes y guías.

2.7.1. Iniciativas.

Es sustancial compartir conocimientos y habilidades con los demás participantes, generar espacios o foros para debatir sobre incidentes y estrategias de mitigación contra vulnerabilidades de ciberseguridad y amenazas. Es importante que las autoridades colaboren para promover el intercambio de información y buenas prácticas. El intercambio permite que los participantes se beneficien de la información contribuyendo a una comprensión mutua y a mejorar las capacidades de respuesta y recuperación.

2.7.2. Análisis posterior al incidente.

Una vez cerrado el ciberincidente, se debería revisar si se siguieron los procedimientos establecidos y si las acciones realizadas fueron efectivas, así como: i) la rapidez en la respuesta a las alertas de seguridad, ii) la oportunidad para determinar el impacto de los incidentes y su gravedad, iii) la calidad en la realización del análisis forense, iv) la eficacia en el escalamiento dentro de la entidad, y v) la eficacia de la comunicación, tanto interna como externa.

2.7.3. Ejercicios.

Los ejercicios pueden ser tanto internos como con terceros, probar los planes de contingencia y la gestión de crisis, la relación con proveedores o pares, para preparar y mejorar la coordinación entre los diversos actores involucrados. Estos ejercicios incluyen diferentes escenarios para validar la efectividad de la coordinación de las actividades de respuesta y recuperación. Para mejorar la ciberresiliencia es recomendable la participación de las autoridades nacionales en la materia en estos ejercicios.

2.7.4. Información confiable.

Identificar fuentes confiables de información para mejorar las actividades de respuesta y recuperación, como informes reconocidos sobre ciberincidentes; análisis de amenazas y tendencias; publicaciones de reguladores y supervisores; los cambios del entorno por diversos escenarios como desarrollos tecnológicos; o mejores prácticas de gestión de riesgos cibernéticos.

2.7.5. Lecciones aprendidas.

Es necesario que las lecciones aprendidas sean validadas con los actores involucrados, tanto internos como externos; las unidades de negocio afectadas por el ciberincidente, las personas con responsabilidades en la respuesta y recuperación y la dirección de la entidad son los que tienen que estar más comprometidos con esta actividad. Las lecciones aprendidas tienen que transformarse en acciones correctivas para la mejora o incorporación de controles y procedimientos, y a estas acciones se le debe dar seguimiento; incluir también, a la revisión de métricas, planes, normas guías y programas de capacitación.

3.1. Alcance.

Los sujetos obligados deberán notificar los ciberincidentes que afecten la normal prestación de servicios hacia los clientes o pongan en riesgo la disponibilidad, integridad y/o confidencialidad de la información.

A los fines de esta normativa, se deberán notificar a la Gerencia de Auditoría Externa de Sistemas de la SEFYC, aquellos incidentes que afecten, como mínimo:

- La prestación normal de los servicios brindados a los clientes por cualquier medio.
- La ejecución de transacciones que deben realizarse en una franja horaria determinada.
- El intercambio de información con otros sujetos obligados y sus prestadores de servicios asociados con relación a la operatoria de los clientes.
- Los datos o la información de los clientes por pérdida o divulgación no autorizada o fraudulenta.

Los incidentes originados en las terceras partes y en toda su cadena de prestadores que tengan vinculación con los sujetos obligados, también deberán ser notificados cuando afecten la disponibilidad para la normal prestación de servicios hacia los clientes, o pongan en riesgo la integridad y confidencialidad de la información.

3.2. Categorización.

3.2.1. Incidentes críticos.

3.2.1.1. Los que afecten a la disponibilidad de los fondos de los clientes para cualquier operatoria.

3.2.1.2. Los relacionados con la función del sujeto obligado en los esquemas de pago, sistemas de compensación o liquidación de valores, incluida cualquier función o tecnología que respalde contingentemente a dichos servicios, propia o provista por terceras partes.

3.2.1.3. Los que tengan impacto en la operatoria de otros participantes de uno o más esquemas de pago, conforme a lo definido en el texto ordenado sobre Proveedores de Servicios de Pago.

3.2.2. Incidentes importantes.

3.2.2.1. Los que tengan un impacto parcial sobre la operatoria de los clientes o entidades, al menos en un servicio o producto.

3.2.2.2. Los que causen interrupciones no críticas en los servicios, pero conlleven la activación de acciones contingentes para restablecerlos.

3.2.2.3. La pérdida o divulgación no autorizada o fraudulenta de datos críticos o confidenciales de clientes.

3.2.3. Incidentes no relevantes.

No deberán ser notificados todos aquellos incidentes que no impliquen una alteración en la normal prestación de los servicios y productos a los clientes o a otros sujetos obligados.

3.3. Plazos para el reporte.

Los sujetos obligados deberán reportar los incidentes importantes y críticos a la Gerencia de Auditoría Externa de Sistemas respetando los siguientes plazos de comunicación:

3.3.1. Notificación inicial.

Dentro de la primera hora de ocurrido o detectado el incidente; se deberá incluir toda la información disponible sobre el mismo.

3.3.2. Reportes subsiguientes.

Desde la notificación inicial y hasta la resolución del incidente, se deberán proporcionar actualizaciones sobre el estado de situación de este, incluidas las tareas y planes de remediación aplicados. Si el incidente se prolonga durante más de una hora, los sujetos obligados deberán informar frecuentemente a la Gerencia de Auditoría Externa de Sistemas sobre las acciones realizadas hasta su normalización.

3.3.3. Reporte de cierre.

Con posterioridad a la contención, recuperación y resolución del incidente, dentro de un período no mayor a 5 días corridos, los sujetos obligados deberán remitir un reporte final, con indicación del análisis y estado de avance en la resolución de la causa que lo originó o causa raíz.

Todas las comunicaciones deberán ser remitidas por correo electrónico a la casilla audext.incidente@bcra.gob.ar, respetando las indicaciones del punto 3.6. “Formato de la notificación”.

3.4. Consideraciones adicionales.

Conforme a lo establecido en los presentes lineamientos y en el texto ordenado sobre Requisitos Mínimos para la Gestión y Control de los Riesgos de Tecnología y Seguridad de la Información, los sujetos obligados deberán alinear sus procesos de respuesta y recuperación ante incidentes con los requisitos establecidos para la gestión de continuidad de negocio, y considerar las lecciones aprendidas para la actualización de todo el ciclo de vida de la gestión de incidentes. Los requisitos de notificación son complementarios y no reemplazan al resto de las disposiciones mencionadas y vigentes.

3.5. Modalidad del reporte.

3.5.1. Notificación inicial.

El reporte deberá mantener el formato establecido y la ubicación de cada uno de los ítems consignados en el punto 3.6. “Formato de la notificación” e incluir, como mínimo, la siguiente información:

- Código de entidad.
- *ID* del incidente.
- Tipo de notificación.
- Fecha y hora de detección.
- Descripción.
- Criticidad.
- Información de la clase de evento (interno o generado por una tercera parte).
- En caso de origen en una tercera parte, informar cuál.
- Sistemas y servicios involucrados.
- Canales de atención afectados.
- Alternativa de atención a los clientes afectados.
- Datos de contacto.

Cuando los detalles específicos no se encuentren disponibles en el momento de la notificación inicial, se deberá indicar información aún no disponible en los campos que correspondan.

3.5.2. Reportes subsiguientes.

Deberán ser remitidos conforme a lo indicado en el punto 3.5.1. y contener una actualización de la información presentada en el reporte inicial, indicando el *ID* del incidente original.

3.5.3. Reporte de cierre.

Deberá incluir, como mínimo, la siguiente información:

- Código de entidad.
- *ID* del incidente original.
- Servicio afectado.
- Categorización.
- Volumen de clientes afectados.
- Cronología, que incluya: los eventos detectados, los pasos y acciones ejecutados para la contención y recuperación, y las medidas provisorias tomadas para mitigar el impacto, junto con su justificación y las aprobaciones solicitadas para su ejecución.
- En el caso de incidentes críticos en los que no se activen planes de continuidad, incluir una descripción que justifique la decisión tomada.
- Sectores internos involucrados.
- Sectores internos afectados.
- Terceras partes y sus prestadores de servicios involucrados y acciones mitigantes a implementar.

- Resultado del análisis de causa raíz.
- Medidas provisorias de mitigación y razones para su aplicación.
- En caso de corresponder, medidas tomadas para:
  - la notificación a las autoridades.
  - la notificación a terceros que pudieran ser afectados.
  - informar al público en general.
- Planes de acción para evitar la recurrencia.
- Fecha de resolución.

La Gerencia de Auditoría Externa de Sistemas podrá solicitar más información sobre las medidas adoptadas para la resolución de los incidentes reportados. La SEFYC también estará facultada para solicitar a los sujetos obligados un plan de encuadramiento para evitar o reducir al mínimo la ocurrencia de incidentes similares en el futuro.

3.6. Formato de la notificación.

3.6.1. Notificación inicial y Reportes subsiguientes.

3.6.1.1. Asunto del correo electrónico. Incidente Reportado por: XXXXX – NOMBRE ENTIDAD (se deberá dejar solo un espacio luego de los dos puntos. XXXXX es el número de entidad en cinco dígitos completando con ceros a la izquierda; luego del guion consignar el nombre).

3.6.1.2. Cuerpo del correo electrónico. *ID* de incidente: XXXXXX (se deberá dejar solo un espacio luego de los dos puntos. Asignar un número de identificación único para cada incidente. Para tipos de notificación 02 indicar el *ID* original).
Tipo de notificación: XX (detallar solo el código numérico según la siguiente tabla):
01 - Inicial (ver detalle en el punto 3.3.1.).
02 - Subsiguiente (ver detalle en el punto 3.3.2.).
Descripción del incidente: (texto libre).
Fecha y hora: dd/mm/yyyy hh:mm (respetar el formato de fecha, no incluir los paréntesis).
Servicio afectado: (texto libre con la descripción del servicio o sistemas afectado).
Canal afectado: XX (informar solo el código numérico según la siguiente tabla – si corresponde más de un canal separar con punto y coma):
01 - Punto de Venta (POS, WebPOS, código QR, entre otros).
02 - Banca por Internet.
03 - Aplicaciones móviles o Billeteras digitales.
04 - Cajeros automáticos.
05 - Sucursal o centro de atención.
06 - Todos los servicios al cliente.
07 - Ninguno de los anteriores.
Criticidad del evento: XX (detallar según la siguiente tabla – indicar solo el número):
01 - Crítico: (ver detalle en el punto 3.2.1.).
02 - Importante: (ver detalle en el punto 3.2.2.).

Clase de evento: XX (detallar según la siguiente tabla – indicar solo el número):
01 - Interno (originado dentro de la entidad).
02 - Terceros (originado por una tercera parte).
Tercero originante: (texto libre - detallar solo si informa clase de evento 02, caso contrario indicar no aplica).
Alternativa de atención: (texto libre - detallar alternativa de atención para los clientes afectados).
Datos de contacto: (texto libre – informar como mínimo: nombre y apellido, cargo o sector, correo electrónico y teléfono).

3.6.2. Reportes de cierre.

3.6.2.1. Asunto del correo electrónico. Incidente reportado por: XXXXX – NOMBRE ENTIDAD (se deberá dejar solo un espacio luego de los dos puntos. XXXXX es el número de entidad en cinco dígitos completando con ceros a la izquierda; luego del guion consignar el nombre).

3.6.2.2. Cuerpo del correo electrónico. *ID*: XXXXXX (dejar solo un espacio luego de los dos puntos, indicar el *ID* original).
Tipo de notificación: 03 (se debe informar siempre el código 03).
Descripción del incidente: (texto libre).
Servicio afectado: (texto libre según lo indicado en punto 3.5.3.).
Categorización: (texto libre según lo indicado en punto 3.5.3.).
Volumen de clientes afectados: (texto libre según lo indicado en punto 3.5.3.).
Cronología: (texto libre según lo indicado en punto 3.5.3.).
Incidente crítico sin plan de continuidad: (texto libre según lo indicado en punto 3.5.3).
Sectores internos involucrados: (texto libre según lo indicado en punto 3.5.3.).
Sectores internos afectados: (texto libre según lo indicado en punto 3.5.3.).
Prestadores de servicios: (texto libre según lo indicado en punto 3.5.3.).
Análisis de causa raíz: (texto libre según lo indicado en punto 3.5.3.).
Medidas de mitigación: (texto libre según lo indicado en punto 3.5.3.).
Notificaciones: (texto libre según lo indicado en punto 3.5.3.).
Planes de acción para evitar la recurrencia: (texto libre según lo indicado en punto 3.5.3).
Fecha y hora de resolución: (dd/mm/yyyy hh:mm) (respetar el formato de fecha, no incluir los paréntesis).

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

B.C.R.A.	ORIGEN DE LAS DISPOSICIONES CONTENIDAS EN EL TEXTO ORDENADO SOBRE LINEAMIENTOS PARA LA RESPUESTA Y RECUPERACIÓN ANTE CIBERINCIDENTES (RRCI)

TEXTO ORDENADO			NORMA DE ORIGEN				OBSERVACIONES
Secc.	Punto	Párr.	Com.	Anexo	Punto	Párr.	
1.	1.1.		"A" 7266				Según Com. "A" 8280.
	1.2.		"A" 7266				Según Com. "A" 8280.
2.	2.1.		"A" 7266				
	2.2.		"A" 7266				
	2.3.		"A" 7266				
	2.4.		"A" 7266				
	2.5.		"A" 7266				
	2.6.		"A" 7266				
	2.7.		"A" 7266				
3.	3.1.		"A" 8280		2.		
	3.2.		"A" 8280		2.		
	3.3.		"A" 8280		2.		
	3.4.		"A" 8280		2.		
	3.5.		"A" 8280		2.		
	3.6.		"A" 8280		2.		

Comunicaciones que componen el historial de la norma

Últimas modificaciones:

17/07/25: “A” 8280

Últimas versiones de la norma - Actualización hasta:

16/07/25

Texto base:

Comunicación “A” 7266: Lineamientos para la respuesta y recuperación ante ciberincidentes (RRCI).

Comunicaciones que dieron origen y/o actualizaron esta norma:

“A” 8280: Lineamientos para la Respuesta y Recuperación ante Ciberincidentes (RRCI). Adecuaciones.