BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

COMUNICACIÓN "A" **8280**	**17/07/2025**

A LAS ENTIDADES FINANCIERAS,
A LOS PROVEEDORES DE SERVICIOS DE PAGO,
A LAS INFRAESTRUCTURAS DEL MERCADO FINANCIERO:

Ref.: Circular
RUNOR 1-1910:

Lineamientos para la Respuesta y Recuperación ante Ciberincidentes (RRCI). Adecuaciones.

Nos dirigimos a Uds. para comunicarles que esta Institución adoptó la resolución que, en su parte pertinente, establece:

"1- Sustituir los puntos 1.1. y 1.2. del texto ordenado sobre Lineamientos para la Respuesta y Recuperación ante Ciberincidentes (RRCI) por lo siguiente:

"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.

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

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."

2- Incorporar como Sección 3. Notificación de ciberincidentes al texto ordenado sobre Lineamientos para la Respuesta y Recuperación ante Ciberincidentes (RRCI) lo siguiente:

"Sección 3. Notificación de ciberincidentes.

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 Superintendencia de Entidades Financieras y Cambiarias, 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 (cinco) 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 Superintendencia de Entidades Financieras y Cambiarias 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).

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

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).”

3- Establecer que los Proveedores de servicios de pago (PSP) incluidos en el Registro de PSP del Banco Central de la República Argentina, excluidos los proveedores de servicios de pago que ofrecen cuentas de pago (PSPCP), tendrán un plazo de 60 (sesenta) días hábiles a partir de la divulgación de esta comunicación para la implementación del texto ordenado sobre Lineamientos para la Respuesta y Recuperación ante Ciberincidentes (RRCI).”

Asimismo, se aclara que las presentes disposiciones dejan sin efecto la Comunicación B 11847.

Al respecto, les hacemos llegar las hojas que, en reemplazo de las oportunamente provistas, corresponde incorporar en el texto ordenado de la referencia. En tal sentido, se recuerda que en la página de esta Institución www.bcra.gob.ar, accediendo a “Sistema Financiero - MARCO LEGAL Y NORMATIVO - Ordenamientos y resúmenes - Textos ordenados de normativa general”, se encontrarán las modificaciones realizadas con textos resaltados en caracteres especiales (tachado y negrita).

Saludamos a Uds. atentamente.

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

BANCO CENTRAL DE LA REPUBLICA ARGENTINA

Héctor D. Domínguez
Subgerente General
de Análisis y Auditoría

Roberto A. Boccardo
Subgerente General
de Sistemas y Organización

ANEXO

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

- Índice -

Sección 1. Introducción.

1.1. Objetivo.
1.2. Sujetos alcanzados.

Sección 2. Lineamientos.

2.1. Gobierno.
2.2. Planificación y preparación.
2.3. Análisis.
2.4. Mitigación.
2.5. Restauración y recuperación.
2.6. Coordinación y comunicación.
2.7. Mejora continua.

Sección 3. Notificación de ciberincidentes.

3.1. Alcance.
3.2. Categorización.
3.3. Plazos para el reporte.
3.4. Consideraciones adicionales.
3.5. Modalidad del reporte.
3.6. Formato de la notificación.

Tabla de correlaciones.

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.

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.		