CODIGO	**:**	I1X
NOMBRE	**:**	Incidentes de Ciberseguridad
SISTEMA	**:**	Instituciones
PERIODICIDAD	**:**	Mensual
PLAZO	**:**	10 días hábiles.

Mediante este archivo los bancos informarán todos los incidentes en materia de Ciberseguridad ocurridos en el mes en curso, incluida la información actualizada de incidentes reportados en el periodo anterior, que aún no hayan sido corregidos. Se entenderá por incidente de ciberseguridad todo evento que ponga en riesgo o afecte negativamente los activos de información de la institución presentes en el ciberespacio, incluso aquellos que no hayan sido materializados o solo se consideren alertas, así como de la infraestructura que la soporta.

PRIMER REGISTRO

1.	Código del banco	9(04)
2.	Identificación del archivo	X(03)
3.	Período	F(06)
4.	*Filler*	X(151)
	Largo del registro	164 bytes

1. CÓDIGO DE LA IFI.
   Corresponde a la identificación de la institución financiera, según la codificación dada por esta Superintendencia.

2. IDENTIFICACIÓN DEL ARCHIVO.
   Corresponde a la identificación del archivo. Debe ser "I1X".

3. PERIODO.
   Corresponde al mes (aaaamm) al que se refiere la información.

Estructura de los registros

1.	Código de identificación único del incidente	X(30)
2.	Materialización del incidente	9(01)
3.	Fecha del evento	F(08)
4.	Hora del evento	9(06)
5.	Fecha del reporte	F(08)
6.	Hora del reporte	9(06)
7.	Fecha de la mitigación	F(08)
8.	Hora de la mitigación	9(06)
9.	Tipo de vulnerabilidad	9(02)
10.	Tipo de amenaza	9(02)
11.	Tipo de activos de información involucrados	9(02)
12.	Tipo de canales, productos o servicios involucrados	9(02)
13.	Número de clientes directamente afectados	R(09)
14.	Nombre del proveedor involucrado	X(30)
15.	RUT del proveedor involucrado	R(09)VX(01)
16.	Costos de las pérdidas asociadas al incidente	9(14)
17.	Costos de mitigación y reparación	9(14)
18.	Porcentaje de recuperación luego de la mitigación	9(03)
19.	Estado del incidente	9(01)
20.	Nivel de criticidad	9(01)
21.	*Filler*	9(01)
	Largo del registro....	164 bytes

Definición de términos

1. CODIGO DE IDENTIFICACIÓN ÚNICO DEL INCIDENTE
   Corresponde al código que identifica unívocamente el incidente reportado. Se utilizará el código asignado por la Superintendencia, en caso que se trate de un incidente de ciberseguridad comunicado según lo dispuesto en el numeral 1.1 del Capítulo 20-8 de la Recopilación Actualizada de Normas.

2. MATERIALIZACIÓN DEL INCIDENTE
   Se debe indicar si el incidente fue materializado o solo se trató de una amenaza, utilizando los siguientes códigos:

Código	
1	Materializado.
2	No materializado.

   Se entenderá por incidente el evento que afecte negativamente a la institución. En la base de incidentes deben reportarse tanto los eventos materializados como los no materializados, entendiéndose por estos últimos aquellos que la institución logró detectar en una fase temprana y no produjeron daños efectivos.

3. FECHA DEL EVENTO
   Corresponde indicar la fecha (aaaammdd) cuando se produjo el incidente.

4. HORA DEL EVENTO
   Corresponde indicar la hora (hhmmss) cuando se produjo el incidente (formato de 24 hrs).

5. FECHA DEL REPORTE
   Corresponde indicar la fecha (aaaammdd) en que el incidente fue detectado.

6. HORA DEL REPORTE
   Corresponde indicar la hora (hhmmss) en que el incidente fue detectado (formato de 24 hrs).

7. FECHA DE LA MITIGACIÓN
   Corresponde indicar la fecha (aaaammdd) en que el incidente fue mitigado.

   Si el incidente no ha sido mitigado a la fecha del reporte, completar el campo con nueves (99999999).

8. HORA DE LA MITIGACIÓN
   Corresponde indicar la hora (hhmmss) en que el incidente fue mitigado. Formato de 24 hrs.

   Si el incidente no ha sido mitigado a la fecha del reporte, completar el campo con nueves (9).

9. TIPO DE VULNERABILIDAD
   En el caso de que el incidente se hubiese materializado, corresponde determinar la causa principal que mejor describe el incidente, señalando el tipo de vulnerabilidad que permitió la materialización del incidente, de acuerdo a la clasificación presentada a continuación:

Código	Tipo de vulnerabilidad
01	Ausencia de las políticas establecidas para el control del riesgo de *Ciberseguridad*.
02	Inadecuada definición, instalación o mantención de la estructura física que soporta los activos de información lógicos.
03	Inadecuada definición o control de los accesos físicos.
04	Inadecuada definición o control de los accesos lógicos.
05	Inadecuada definición de los servicios provistos por agentes externos.
06	Inadecuada definición o control de la arquitectura tecnológica.
07	Prácticas inadecuadas de los usuarios internos de la organización.
08	Acceso físico de personal interno no autorizado.
09	Acceso físico de personal externo no autorizado.

10. TIPO DE AMENAZA
Corresponde especificar el tipo de amenazas que mejor describe el incidente, de acuerdo a los siguientes códigos:

Código	Tipo de amenaza
01	Ataques físicos como robo o hurto, secuestros, daños o pérdidas de activos de información tecnológicos de dispositivos, entre otros.
02	Destrucción voluntaria de activos de información o de la estructura física que lo soporta.
03	Interrupciones del servicio, tales como el servicio de red, energía o falta de algún recurso.
04	Actividades ilegales no físicas, como el robo de identidad, virus, certificados, maliciosos, malware, denegación de servicio, ingeniería social, etc.
05	Desastres naturales o medioambientales.
06	Amenazas legales.
07	Prácticas inadecuadas de los usuarios externos de la organización.

11. TIPO DE ACTIVOS DE INFORMACIÓN INVOLUCRADOS
Se debe especificar el tipo de activos afectados o potencialmente en riesgo. En caso de existir más de un tipo de activos afectados, completar nuevos registros.

Código	Tipo de activos
01	Información personal innominada de sus clientes, distintos de claves de seguridad.
02	Información nominada de productos o servicios de sus clientes, sin incluir claves de seguridad.
03	Información nominada de productos o servicios de sus clientes, incluyendo claves de seguridad.
04	Softwares
05	Base de datos de reclamos de los clientes.
06	Correos electrónicos y mensajería, incluyendo sus servidores.
07	Información asociada a proveedores.
08	Estaciones de trabajo o dispositivos móviles de sus empleados.
09	Servidores.
10	API´S.
11	Información asociada a gestión interna del banco.

12. TIPO DE CANALES, PRODUCTOS O SERVICIOS INVOLUCRADOS
Corresponde indicar el tipo de canales, productos o servicios prestados por la institución que fueron afectados por el incidente, ya sea en su disponibilidad o funcionamiento. En caso de existir varios canales, productos o servicios involucrados, completar tantos registros como se hayan detectado, utilizando el mismo número de incidente.

Código	Tipos de canales, productos o servicios involucrados
01	Cajeros automáticos sin considerar transferencia y giro de fondos.
02	Cajeros automáticos incluyendo el servicio de transferencia y giro de fondos.
03	Aplicaciones móviles sin considerar transferencia de fondos.
04	Aplicaciones móviles incluyendo el servicio de transferencia de fondos.
05	Página web de la institución sin considerar transferencia de fondos.
06	Página web de la institución incluyendo el servicio de transferencia de fondos.
07	Corresponsalías sin considerar transferencia y giro de fondos.
08	Corresponsalías incluyendo el servicio de transferencia y giro de fondos.
09	Sistema de pago con tarjetas u otros instrumentos similares, incluyendo POS u otros dispositivos físicos de pago.
10	Sistema de pago de bajo valor, a partir de mecanismos lógicos, no físicos, distintos de los individualizados en códigos anteriores.
11	Sucursales sin considerar transferencia y giro de fondos.
12	Sucursales incluyendo el servicio de transferencia y giro de fondos.
13	Ejecución, entrega y gestión de procesos asociados a productos de crédito a la banca minorista, distintos de los procesos individualizados en los códigos anteriores.
14	Ejecución, entrega y gestión de procesos asociados a productos de depósitos a la banca minorista, distintos de los procesos individualizados en los códigos anteriores.
15	Operaciones de tesorería, compra y venta de valores, divisas y materias primas por cuenta de clientes.
16	Operaciones de tesorería, compra y venta de valores, divisas y materias primas por cuenta propia.
17	Sistemas de pago, compensación y liquidación de alto valor.
18	Servicios de agencia, custodia, agencia a empresas, fideicomisos.
19	Administración de activos.
20	Banca comercial, cuando se trata de consideraciones distintas de las individualizadas en los códigos anteriores.

13. NÚMERO DE CLIENTES AFECTADOS
Corresponde informar el número de clientes afectados directamente por el incidente. En caso de incidentes no materializados, corresponde informar el número de clientes expuestos a la amenaza. En caso de no existir, completar el campo con nueves.

14. RUT DEL PROVEEDOR INVOLUCRADO
Corresponde indicar el RUT del proveedor involucrado directamente en la causa del incidente. Si existiese más de un proveedor, completar otro registro indicando el mismo número de incidente. De no existir, completar el campo con nueves.

15. NOMBRE DEL PROVEEDOR INVOLUCRADO
Corresponde indicar el nombre del proveedor involucrado directamente en la causa del incidente. Si existiese más de un proveedor, completar otro registro indicando el mismo número de incidente. De no existir, completar el campo con nueves.

16. COSTOS DE INCIDENTES
Corresponde informar los costos expresados en pesos chilenos a la fecha del reporte asociado al incidente, entendidos como el valor presente de las pérdidas reales.

En caso de no existir información, completar el campo con nueves. Posteriormente se debe informar cuando se disponga de nueva información, utilizando el mismo número de incidente.

17. COSTOS DE MITIGACIÓN Y REPARACIÓN
Corresponde informar los costos expresados en pesos chilenos a la fecha del reporte, asociados a los actos de mitigación, recuperación, puesta en marcha y reparación de los daños causados por el incidente.

En caso de no existir información, completar el campo con nueves. Posteriormente se debe informar cuando se disponga de nueva información, utilizando el mismo número de incidente.

18. PORCENTAJE DE RECUPERACIÓN LUEGO DE LA MITIGACIÓN
Corresponde informar el porcentaje de montos recuperados luego de los actos de mitigación.

De no existir o no corresponder, completar el campo con nueves. Si posteriormente se dispone de información, se reporta utilizando el mismo número de incidente.

19. ESTADO DEL INCIDENTE
Se debe indicar, para cada evento, si los planes de acción para su corrección definitiva se encuentran implementados.

Código	Estado del incidente
1	Sin plan de acción.
2	Con planes, pero sin implementación.
3	En proceso de implementación.
4	Planes de acción implementados.

20. NIVEL DE CRITICIDAD
Se debe indicar para cada incidente el nivel de criticidad, entendido como el impacto en términos de ciberseguridad. La criticidad, será definida por la propia institución de acuerdo a sus políticas de gestión de riesgos.

Código	Nivel de criticidad
1	Baja.
2	Media.
3	Alta.

Carátula de cuadratura

El archivo I1X debe entregarse con una carátula de cuadratura cuyo modelo se especifica a continuación:

MODELO

Institución _____ Código: _____

Información correspondiente al mes de: _____ Archivo I1X

Número de registros informados	