| | | |
|---|---|---|
| **CODIGO** | **:** | I12 |
| **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 o complementaria de incidentes reportados en periodos anteriores. Se entenderá por incidente de Ciberseguridad todo evento que ponga en riesgo o afecte negativamente los activos de información de la institución, así como de la infraestructura que la soporta. Consideraremos alertas a aquellos eventos registrados pero no materializados.*

*El objetivo de este archivo es contar con una base consolidada de los eventos en materia de Ciberseguridad y dar seguimiento a los mismos.*

**PRIMER REGISTRO**

1. Código del banco ..... 9(04)
2. Identificación del archivo..... X(03)
3. Período..... F(06)
4. *Filler*.....X(185)

Largo del registro..... 198 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 "I12".

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

**Registros siguientes**

Los registros siguientes contendrán información sobre incidentes y alertas, a la fecha que se refiere la información, lo que se informará en el primer campo de cada registro con los siguientes códigos:

| Código | Tipo de registro |
|---|---|
| 1 | Incidentes |
| 2 | Alertas |

**Registro que contiene el detalle de los incidentes**

*En este registro se deben informar todos los incidentes materializados.*

1. Tipo de registro ..... 9(01)
2. Número interno de identificación del incidente ..... X(30)
3. Número de identificación del incidente otorgado por la SBIF ..... X(30)
4. Fecha del incidente ..... F(08)
5. Hora del incidente ..... 9(06)
6. Fecha del reporte ..... F(08)

| | | |
|---|---|---|
| 7. | Hora del reporte | 9(06) |
| 8. | Fecha de la mitigación | F(08) |
| 9. | Hora de la mitigación | 9(06) |
| 10. | Tipo de vulnerabilidad | 9(02) |
| 11. | Tipo de amenaza | 9(02) |
| 12. | Tipo de activos de información involucrados | 9(02) |
| 13. | Tipo de canales, productos o servicios involucrados | 9(02) |
| 14. | Número de clientes directamente afectados | 9(14) |
| 15. | Nombre del proveedor involucrado | X(30) |
| 16. | RUT del proveedor involucrado | R(09)VX(01) |
| 17. | Costos de las pérdidas asociadas al incidente | 9(14) |
| 18. | Costos de mitigación y reparación | 9(14) |
| 19. | Porcentaje de recuperación luego de la mitigación | 9(03) |
| 20. | Estado del incidente | 9(01) |
| 21. | Nivel de criticidad | 9(01) |

Largo del registro ..... 198 bytes

**Definición de términos**

1. TIPO DE REGISTRO
   Corresponde al código que identifica el tipo de registro. Debe ser "1".

2. NÚMERO INTERNO DE IDENTIFICACIÓN DEL INCIDENTE
   Corresponde al código que identifica unívocamente el incidente reportado, asignado por el banco dentro de su registro interno. Este código servirá para futuras actualizaciones o información complementaria sobre el incidente, enviada en archivos futuros.

3. NÚMERO DE IDENTIFICACIÓN DEL INCIDENTE OTORGADO POR LA SBIF
   Corresponde al código que la SBIF le otorgó al incidente, en el caso que este haya sido informado por el sistema de reporte de incidentes operacionales (RIO). En caso contrario completar con ceros.

4. FECHA DEL INCIDENTE
   Corresponde indicar la fecha (AAAAMMDD) cuando se produjo el incidente.

5. HORA DEL INCIDENTE
   Corresponde indicar la hora (HHMMSS) cuando se produjo el incidente (formato de 24 hrs).

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

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

8. FECHA DE LA MITIGACIÓN
   Corresponde indicar la fecha (AAAAMMDD) en que el incidente fue mitigado, total o parcialmente; entendiendo por mitigación cualquier medida que contrarreste el impacto del incidente. Si no se ha iniciado el proceso de mitigación a la fecha del envío del archivo, completar el campo con 19000101.

9. HORA DE LA MITIGACIÓN
   Corresponde indicar la hora (HHMMSS) en que el incidente fue mitigado (formato de 24 hrs). Si no se ha iniciado el proceso de mitigación a la fecha del envío del archivo, completar el campo con nueves.

   Para los campos 10, 11, 12 y 13 siguientes, en el caso que se identifique más de una categoría principal del incidente, se deben informar cada una en un nuevo registro repitiendo los campos anteriores.

10. TIPO DE VULNERABILIDAD
    Corresponde informar la causa principal que mejor describe el incidente a la fecha del envío del archivo, señalando el tipo de vulnerabilidad que permitió su materialización, de acuerdo a los códigos de clasificación de la Tabla 95 "Tipo de vulnerabilidad".

11. TIPO DE AMENAZA
    Corresponde especificar el tipo de amenazas o vulnerabilidades que mejor describe el origen del incidente, dado el análisis a la fecha del envío del archivo, de acuerdo a los códigos de la Tabla 96 "Tipo de amenazas".

12. TIPO DE ACTIVOS DE INFORMACIÓN INVOLUCRADOS
    Se debe especificar el tipo de activos de información afectados o puestos en riesgo, de acuerdo a los códigos de la Tabla 97 "Tipos de activos de información".

13. 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, de acuerdo a los códigos de la Tabla 98 "Tipo de canales, productos o servicios".

14. NÚMERO DE CLIENTES DIRECTAMENTE AFECTADOS
    Corresponde informar el número de clientes afectados directamente por el incidente. En caso de no existir, completar el campo con ceros.

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. Si no corresponde informar, dejar el campo en blanco.

16. 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. Si no corresponde informar, completar el campo con ceros.

17. 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 tener información, completar el campo con ceros. Posteriormente, cuando ella se obtenga, se debe informar en el archivo del mes en que se obtuvo utilizando el mismo número de incidente.

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

En caso de no tener información, completar el campo con ceros. Posteriormente, cuando ella se obtenga, se debe informar en el archivo del mes en que se obtuvo utilizando el mismo número de incidente.

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

De no tener o no corresponder, completar el campo con ceros. Posteriormente, cuando ella se obtenga, se debe informar en el archivo del mes en que se obtuvo utilizando el mismo número de incidente.

20. ESTADO DEL INCIDENTE
Se debe indicar, para cada evento, si los planes de acción para su corrección definitiva se encuentran implementados, considerando lo siguiente:

| 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. |
| 5 | Totalmente mitigado. |

21. 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, la que deberá se consistente con definiciones reportadas en sus políticas internas, considerando lo siguiente:

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

**Registro que contiene el detalle de las alertas**

*En este registro se deben informar todas las alertas o eventos no materializados, detectados y/o interceptados por la institución.*

1. Tipo de registro ..... 9(01)
2. Número de alertas ..... 9(14)
3. Origen de datos ..... 9(02)
4. Tipo de alertas ..... 9(02)
5. Plataforma involucrada ..... 9(02)
6. Naturaleza de la amenaza ..... 9(02)
7. Acciones realizadas ..... 9(02)
8. Filler ..... X(173)

Largo del registro ..... 198 bytes

**Definición de términos**

1. TIPO DE REGISTRO
   Corresponde al código que identifica el tipo de registro. Debe ser "2".

2. NUMERO DE ALERTAS
   Corresponde a informar el número total de alertas, agrupadas de acuerdo a los campos siguientes.

3. ORIGEN DE LOS DATOS
   Corresponde informar el origen primario de la amenaza detectada, según lo siguiente:

| Código | Origen de datos |
|---|---|
| 01 | IPS perimetral |
| 02 | IPS Interno |
| 03 | Anti spam Email Gateway |
| 04 | Antivirus |
| 05 | Web Application Firewall (WAF) |
| 06 | Content Delivery Network (CDN) |

4. TIPO DE ALERTAS
   Corresponde informar el tipo de alerta que más se identifique con la causa principal de la amenaza, de acuerdo a los códigos de la Tabla 99 "Tipo de alertas".

5. PLATAFORMA INVOLUCRADA
   Corresponde informar la plataforma informática que fue afectada por la alerta en cuestión, de acuerdo a los códigos de la Tabla 100 "Tipo de plataforma informática".

6. NATURALEZA DE LA AMENAZA
   Corresponde informar cuál es la naturaleza de la amenaza detectada, de acuerdo a los códigos de la Tabla 101 "Naturaleza de la amenaza".

7. ACCIONES REALIZADAS
   Corresponde reportar la acción realizada para evitar la alerta detectada, de acuerdo a los códigos de la Tabla 102 "Tipo de acción realizada".

## Carátula de cuadratura

El archivo I12 debe entregarse con una carátula de cuadratura cuyo modelo se especifica a continuación:

MODELO

Institución _____ Código: _____

Información correspondiente al mes de: _____ Archivo I12

| | |
|---|---|
| Número de registros informados | |
| Número de registros con el código 1 en el campo 1 | |
| Número de registros con el código 2 en el campo 1 | |

## Tabla 95: Tipo de vulnerabilidad

| 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 | Inadecuada implementación o desarrollo de software. |
| 08 | Prácticas inadecuadas de los usuarios internos de la organización. |
| 09 | Acceso físico de personal interno no autorizado. |
| 10 | Acceso físico de personal externo no autorizado. |

## Tabla 96: Tipo de amenazas

| Código | Tipo de amenaza |
|---|---|
| 01 | Ataques físicos como robo o hurto, secuestros, daños o pérdidas de activos de información tecnológicos, daños o pérdidas 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, entre otros. |
| 05 | Desastres naturales o medioambientales. |
| 06 | Problemas contractuales, huelgas. |
| 07 | Prácticas inadecuadas de los usuarios externos de la institución. |
| 08 | Errores involuntarios de usuarios internos. |
| 09 | Prácticas inadecuadas de usuarios internos de la institución |

## Tabla 97: Tipo de activos de información

| Código | Tipo de activos de información |
|---|---|
| 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. |

## Tabla 98: Tipo de canales, productos o servicios

| Código | Tipos de canales, productos o servicios |
|---|---|
| 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. |

## Tabla 99: Tipo de alertas

| Código | Tipo de alertas |
|---|---|
| 01 | Malware |
| 02 | Daño o pérdida de activo de Información |
| 03 | Ejecución de Crontab |
| 04 | Estado Respuesta HTTP Ilegal |
| 07 | Firma de Ataque Detectada |
| 08 | Fuga de Información |
| 09 | Inyección Xpath |
| 10 | Inyección de Código Java |
| 11 | Largo Ilegal Método Post |
| 12 | Largo Ilegal URL |
| 13 | Largo Query Ilegal |
| 14 | Largo de Respuesta Ilegal |
| 15 | Método Ilegal (Delete) |
| 16 | Método Ilegal Ejecutado |
| 17 | Parámetro Ilegal en XML |
| 19 | Suplantación de identidad |
| 20 | Técnicas de Evasión |
| 21 | Tipo Archivo Ilegal |

## Tabla 100: Tipo de plataforma informática

| Código | Tipo de plataforma informática |
|---|---|
| 01 | Acceso a Internet |
| 02 | Red Interna |
| 03 | Correo |
| 04 | Estaciones de trabajo |
| 05 | Homebanking |
| 06 | Sitio Web Seguros |
| 07 | Servidores |
| 08 | Servidores y Estaciones de trabajo |

**Tabla 101: Naturaleza de la amenaza**

| Código | Tipo de naturaleza de la amenaza |
|---|---|
| 01 | Actividad sospechosa en la red |
| 02 | Correo Malicioso |
| 03 | Trojan |
| 04 | Malware |
| 05 | Virus no categorizado |
| 06 | Phishing |
| 07 | CriptoMalware |
| 08 | User-Agent Widgitoolbar |
| 09 | Man in the middle |
| 10 | Suplantación de identidad |
| 99 | Otro |

**Tabla 102: Tipo de acción realizada**

| Código | Tipo de acción realizada |
|---|---|
| 01 | Bloqueo de correo malicioso. |
| 02 | Bloqueo de firmas. |
| 03 | Revisión completa de antivirus. |
| 04 | Desconexión de la red y revisión completa de antivirus. |
| 05 | Desconexión de la red y se reinstala el antivirus. |
| 06 | Desconexión y revisión completa de antivirus. |
| 07 | Notificación y cierre de infraestructura. |
| 08 | Se realiza bloqueo del remitente y otros componentes identificados en el correo como la IP donde direcciona el link. |
| 09 | Se solicitan acciones al proveedor. |

## SISTEMA INSTITUCIONES

| Código | NOMBRE | Periodicidad | Plazo (días hábiles) |
|---|---|---|---|
| I01 | Accionistas | Trimestral | 6 |
| I02 | Grupos Relacionados | Trimestral | 3 |
| I03 | Directores, Apoderados Generales y Personas Relacionadas con ellos | Trimestral | 3 |
| I05 | Gravámenes sobre Acciones | Trimestral | 6 |
| I06 | Oficinas, personal, horarios de atención y cajeros automáticos | Mensual | 6 |
| I07 | Presidentes, Directores, Gerentes y Ejecutivos Principales | (1) | 3 |
| I08 | Antecedentes del gobierno corporativo del banco | Semestral | 9 |
| I09 | Antecedentes generales de filiales y sociedades de apoyo al giro del banco | Semestral | 9 |
| I10 | Antecedentes de directores y gerentes de filiales y sociedades de apoyo al giro del banco | Semestral | 9 |
| I11 | Parque de cajeros automáticos y tiempos de indisponibilidad o *Downtime* | Mensual | 9 |
| I12 | Incidentes de Ciberseguridad | Mensual | 10 |

(1): Debe remitirse cada vez que ocurra un cambio en los datos del último archivo enviado.

## SISTEMA ESTADÍSTICO

| Código | NOMBRE | Periodicidad | Plazo (días hábiles) |
|---|---|---|---|
| E01 | Remate de garantías en Créditos para la Vivienda | Semestral | 7 |
| E02 | Bienes Recibidos o Adjudicados en Pago | Trimestral | 7 |
| E03 | Venta de Bienes Recibidos o Adjudicados en Pago | Trimestral | 7 |
| E04 | Reclamos de Usuarios | Mensual | 7 |
| E05 | Cierre de productos | Mensual | 7 |