

**CIRCULAR N°119 DE 12 DE ABRIL DE 2021,
QUE IMPARTE INSTRUCCIONES
RELATIVAS A LOS LINEAMIENTOS DE
CIBERSEGURIDAD QUE DEBEN
OBSERVAR LAS SOCIEDADES
OPERADORAS Y LAS SOCIEDADES
CONCESIONARIAS DE CASINOS DE
JUEGO¹**

VISTOS: Lo dispuesto en la Ley N°19.995, que establece las Bases Generales para la Autorización, Funcionamiento y Fiscalización de Casinos de Juego, en especial los artículos 4, 12, 36, 37 N°2, 4 y 42 N°7; en la Ley N°18.575, que contiene las Bases Generales de la Administración del Estado, en especial su artículo 5°; en los artículos 5°, 33 y 34 del Decreto Supremo N°287, de 2005, del Ministerio de Hacienda, que aprueba el Reglamento de Funcionamiento y Fiscalización de Casinos de Juego; Decreto Supremo N°533, de 2015, de Ministerio del Interior y Seguridad Pública, que crea el Comité Interministerial sobre ciberseguridad y modificaciones; el Decreto N°32, de 2017 y N°248, de 2020, ambos del Ministerio de Hacienda, que designa y renueva, respectivamente, a doña Vivien Alejandra Villagrán Acuña como Superintendente de Casinos de Juego (SCJ); el Instructivo Presidencial N°1, de 2017, que instruye la implementación de la Política Nacional sobre Ciberseguridad; Instructivo Presidencial N°8, de 2018, que imparte instrucciones urgentes en materia de Ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado; en la Ley N°19.233, que tipifica figuras penales relativas a la informática; en la Resolución N°725 de 2020 de la SCJ, que aprueba convenio de colaboración entre el Ministerio del Interior y Seguridad Pública y el Ministerio de Hacienda y las Superintendencias, de 4 de septiembre de 2019; la Resolución N°7, de 2019 de la Contraloría General de la República y sus modificaciones; así como en las demás disposiciones pertinentes; y

CONSIDERANDO:

1. Que, la masificación en el uso de las tecnologías de la información y de las comunicaciones, junto con servir al desarrollo del país, conlleva riesgos que pueden afectar los bienes y derechos de las personas, la seguridad pública, las infraestructuras críticas, el gobierno digital, los intereses esenciales y la seguridad exterior de Chile. Estos riesgos pueden provenir de diversas fuentes y se pueden manifestar mediante actividades tales como el espionaje, sabotaje, fraudes o ciberataques realizados por o desde otros países, por grupos organizados o por particulares, entre otros.

2. Que, a su vez, la Ciberseguridad es una disciplina cuyo objetivo es ayudar a gestionar el riesgo de las empresas a través de la instalación de un sistema de gestión de seguridad de la información que detecte, mitigue, monitoree y responda ante riesgos de seguridad de la información, buscando preservar no solo la disponibilidad y continuidad de un proceso productivo, sino que también la integridad y confidencialidad de todos los activos de información relevantes para los procesos de soporte, servicios productivos que son el núcleo y esencia de la empresa.

3. Que, el Comité Interministerial de Ciberseguridad, creado por Decreto Supremo N°533, de 2015, del Ministerio del Interior y Seguridad Pública, elaboró la Política Nacional de Ciberseguridad, aprobada y lanzada oficialmente el 27 de abril de 2017, la cual consigna, entre otros temas, que es necesario mejorar las instancias de comunicación, coordinación y colaboración entre instituciones, organizaciones y empresas, tanto del sector público como privado, nacionales e internacionales, con el propósito de fortalecer la confianza y entregar una respuesta común a los riesgos del ciberespacio.

¹ La presente versión corresponde a la Circular N°119, con todas sus modificaciones (Circulares N°130/2022 y N°132/2022). Los documentos anexos se encuentran disponibles para su descarga en la página web institucional de la Superintendencia, adjuntos a su circular.

4. Que, en dicho contexto y con el fin de mejorar las instancias de comunicación, coordinación y colaboración entre instituciones, es que el Ministerio del Interior y Seguridad Pública celebró un convenio de colaboración en materia de Ciberseguridad con la Superintendencia de Casinos de Juego el 4 de septiembre del año 2019, aprobado mediante Resolución N°725 de 2020 de la SCJ.

5. Que, el referido convenio tiene como fundamento la colaboración en materia de Ciberseguridad mediante el intercambio voluntario de información técnica, estadística, buenas prácticas, formación, desarrollo de proyectos y difusión en materia de Ciberseguridad. Todo ello con el fin de mejorar la colaboración y seguridad del ecosistema digital y el ciberespacio y apoyar el esfuerzo que cada empresa, así como el sector público, está realizando en materia de Ciberseguridad.

6. Que, actualmente los casinos de juego en su actividad comercial se encuentran sujetos a riesgos de ciberseguridad, tales como ocurrencias de incidentes asociados a contenido abusivo, interrupción de la red local o global (disponibilidad), código malicioso, recopilación de información, intentos de intrusión, intrusión, disponibilidad, información de seguridad de contenidos, fraude, vulnerabilidades del día cero, captura no autorizada de tráfico de datos en la infraestructura de red (confidencialidad) y medios de pago electrónicos; modificación o redireccionamiento del tráfico de datos en la infraestructura de red (integridad y/o confidencialidad); destrucción o alteración de otras infraestructuras o información digital, a través de las redes (integridad y/o disponibilidad), interceptación de cualquier forma de comunicación; iteración o interceptación no autorizada de dispositivos o máquinas de azar contempladas en la ley 19.995, entre otros.

7. En ese orden de ideas, no se puede desconocer el hecho de que la industria de casinos de juego opera sobre sistemas y plataformas tecnológicas y que muchos de ellos están conectados a través de redes internas o externas, formando parte de un ecosistema digital que es uno solo y que no admite divisiones. La interoperatividad y la digitalización demandan compartir millones de datos relevantes de forma automatizada que se procesa en sistemas de correlación y si bien la adopción de nuevas tecnologías, como podrían ser las nuevas formas de juego online o dispositivos IoT ("Internet of Things") de diversa índole, traen consigo nuevas oportunidades para la industria y sus usuarios, al mismo tiempo implican nuevos riesgos que deben ser abordados con una base de Ciberseguridad para operar de manera segura.

8. Que, por otra parte, conforme a lo dispuesto en el artículo 37 N°4 de la Ley N°19.995, corresponde a la Superintendencia de Casinos de Juego *"fiscalizar el desarrollo de los juegos, según las normas reglamentarias de los mismos, como también el correcto funcionamiento de las máquinas e implementos usados al efecto"*.

9. Que, debido a lo señalado y atendida la necesidad de fijar lineamientos con el objeto de prevenir la ocurrencia de daños en la materia y establecer y uniformar los mecanismos de notificación de incidentes de ciberseguridad, se dictan las siguientes instrucciones:

IMPÁRTASE LAS SIGUIENTES INSTRUCCIONES RELATIVAS A LOS LINEAMIENTOS DE CIBERSEGURIDAD QUE DEBEN OBSERVAR LAS SOCIEDADES OPERADORAS Y LAS SOCIEDADES CONCESIONARIAS DE CASINOS DE JUEGO

I. DISPOSICIONES GENERALES

1°. Objeto

A partir de las directrices establecidas por el Ministerio del Interior y Seguridad Pública en materia de ciberseguridad, la presente circular tiene por objeto establecer lineamientos mínimos a cumplir por las sociedades operadoras y las sociedades concesionarias de casinos de juego para la gestión de la Ciberseguridad.

Por una parte, se establecen medidas técnicas y de organización que buscan identificar tanto el análisis de impacto operacional como los riesgos y controles mitigantes, así como la gestión del ciclo de vida de un ciberincidente, considerando tanto la prevención, detección, análisis, notificación, contención, erradicación, respuesta, recuperación y documentación a su respecto.

Por otra parte, esta circular busca instruir sobre los reportes de ciberincidentes que las sociedades operadoras y las sociedades concesionarias de casinos de juego deben enviar a la Superintendencia con el objeto de establecer las acciones orientadas a mitigar sus efectos e impactos y contribuir a una oportuna normalización y estabilización de los servicios afectados.

2°. Definiciones

Para los efectos de la aplicación de esta circular, así como la gestión vinculada a ella, los términos que a continuación se señalan tendrán el significado que se indica:

- a. **Autenticación:** Proceso utilizado en los mecanismos de control de acceso con el objetivo de verificar la identidad de un usuario, dispositivo o sistema mediante la comprobación de credenciales de acceso.
- b. **Ciberespacio:** Dominio global y dinámico dentro del entorno de la información que corresponde al ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información, los datos (almacenados, procesados o transmitidos) que abarcan los dominios físico, virtual y cognitivo y las interacciones sociales que se verifican en su interior. Las infraestructuras tecnológicas corresponden a los equipos materiales empleados para la transmisión de las comunicaciones, tales como enlaces, enrutadores, conmutadores, estaciones, sistemas radiantes, nodos, conductores, entre otros. Los componentes lógicos de la información, en tanto, son los diferentes softwares que permiten el funcionamiento, administración y uso de la red.
- c. **Ciberincidente:** Todo evento que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y su infraestructura, que puedan afectar al normal funcionamiento de los mismos.
- d. **Ciberseguridad:** Conjunto de acciones posibles para la prevención, mitigación, investigación y manejo de las amenazas e incidentes sobre los activos de información, datos y servicios, así como para la reducción de los efectos de los mismos y del daño causado antes, durante y después de su ocurrencia.
- e. **Confidencialidad:** Principio de seguridad que requiere que los datos deberían únicamente ser accedidos por el personal autorizado a tal efecto.
- f. **Disponibilidad:** Capacidad de ser accesible y estar listo para su uso a demanda de una entidad autorizada.
- g. **Equipo de Respuesta ante Incidentes de Seguridad Informática, en adelante (CSIRT):** Centros conformados por especialistas multidisciplinarios capacitados para prevenir, detectar, gestionar y responder a incidentes informáticos, en forma rápida y efectiva, y que actúan según procedimientos y políticas predefinidas, coadyuvando asimismo a mitigar los efectos de ataques de ciberseguridad.

Para efectos de esta circular, corresponde al Departamento dependiente de la División de Redes y Seguridad Informática del Ministerio del Interior y Seguridad Pública creado mediante la resolución N°5.006, de 20 de agosto de 2019, del mencionado Ministerio. El

CSIRT podrá ser requerido, conforme a su disponibilidad, para gestionar incidentes por parte de las sociedades operadoras y concesionarias municipales.

- h. **Gestión de incidentes:** Procedimientos para la detección, análisis, manejo, contención y resolución de un incidente de ciberseguridad y responder ante ésta.
- i. **Incidente:** Evento inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes, equipos y sistemas de información.
- j. **Vulnerabilidad o brecha informática:** Debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.
- k. **Integridad:** Principio de seguridad que certifica que los datos y elementos de configuración sólo son modificados por personal y actividades autorizadas. La Integridad considera todas las posibles causas de modificación, incluyendo fallos de software y hardware, eventos medioambientales e intervención humana.
- l. **Ciberataque:** Cualquier incidente cibernético, provocado deliberadamente y que afecte a un sistema informático.
- m. **Resiliencia:** Capacidad de los sistemas, equipos o redes para seguir operando pese a estar sometidos a un incidente o ciberataque, aunque sea en un estado degradado, debilitado o segmentado. Así como, incluye la capacidad de restaurar con presteza sus funciones esenciales después de un incidente o ataque de modo de recuperarse con presteza de una interrupción, por lo general con un efecto reconocible mínimo.
- n. **Riesgo de Ciberseguridad:** Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes, equipos y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una de las amenazas antes mencionadas que produzca un impacto en términos de operatividad, o de integridad, confidencialidad o disponibilidad de datos, especialmente aquellos personales y sensibles tratados por la sociedad operadora o concesionaria de casino de juego y/o de implementos de juego.

II. GESTIÓN DE LA CIBERSEGURIDAD

1. Medidas de gestión

Toda sociedad operadora y concesionaria municipal deberá implementar medidas técnicas y de organización para gestionar los riesgos de Ciberseguridad de las redes, equipos y sistemas que utiliza para la prestación de los servicios a sus clientes, indistintamente de si tal gestión estuviere o no externalizada, los cuales deberán constar en un protocolo.

Cada sociedad operadora y concesionaria municipal determinará y explicitará en dicho protocolo las medidas de gestión que busque garantizar la disponibilidad, integridad y confidencialidad que en definitiva adopte, de conformidad con los riesgos asociados y la tecnología disponible. Los protocolos en que consten las medidas de gestión deberán contener, a lo menos:

- a. las medidas de seguridad física y ciberseguridad de los sistemas e instalaciones;
- b. las medidas de resiliencia de la red, equipos y sistemas;
- c. las medidas de gestión del riesgo propio de la actividad;
- d. las medidas de gestión de incidentes;
- e. las medidas de gestión de la continuidad de los servicios;
- f. las medidas de monitoreo permanente de los sistemas;
- g. las actividades de supervisión, auditoría y prueba;
- h. las medidas de conocimiento de las alertas de ciberincidentes a nivel nacional e internacional;
- i. las medidas de seguridad en los componentes tecnológicos de los equipos para los servicios entregados, que garanticen adecuadamente la integridad, confidencialidad y

disponibilidad de las transmisiones e información, tales como dispositivos y máquinas de azar contemplados en la Ley N°19.995, medios de pago integrado, redes inalámbricas, entretots;

- j. calificación mínima exigida, los planes de capacitación y seguridad del personal que opera los componentes tecnológicos;
- k. mecanismo o procedimiento de recuperación de la información en caso de pérdida de ésta por manipulación, ciberincidentes u otras causas de su responsabilidad.

Asimismo, los protocolos y sistemas de seguridad asociados deberán ser revisados al menos una vez por año calendario y actualizados cada vez que corresponda, debiendo constar explícitamente en acta de sesión de Directorio o acta de reunión con la Alta Gerencia dicha revisión.

Para todo lo anterior, se deberá considerar cualquiera de los principios y estándares internacionalmente aceptados en materia de Ciberseguridad, tales como, y sin ser taxativos, International Organization for Standardization (ISO), las recomendaciones de la OCDE incluidas en el “*Digital Security Risk Management for Economic and Social Prosperity*” (2015) y “*Recommendation on Digital Security of Critical Activities*” (2019).

2. Medidas de prevención y mitigación

Las sociedades operadoras y las sociedades concesionarias de casinos de juego con el objeto de prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten la seguridad de las redes, equipos, soporte tecnológico interno o externalizado y sistemas utilizados para la prestación de los servicios, con el objeto de garantizar su continuidad operativa deberán diseñar, implementar, practicar y evaluar un plan de respuesta, cuyo contenido deberá constar del protocolo antes señalado, que otorgue adecuada cobertura a sus redes, equipos y sistemas en conformidad con estándares internacionales o nacionales, de amplia aplicación, tales como los mencionados en el párrafo anterior, y, a su vez, desde el punto de vista de los clientes, se deberá promover garantizar la integridad, disponibilidad y confidencialidad de la información asociada a sus datos personales y datos sensibles de acuerdo a la definición señalada en la Ley N°19.628 de protección de datos personales; además de la información de juego y datos bancarios

3. Análisis de riesgo y seguridad por diseño

Las sociedades operadoras y las concesionarias de casinos de juego, desde las etapas de concepción, planeamiento y diseño de sus sistemas y procesos y, en general, durante toda su gestión a partir del inicio de la operación, deberán aplicar criterios orientados a minimizar los riesgos de ciberincidentes y a facilitar una adecuada gestión de éstas durante su operación, mantención y optimización.

El diseño, instalación y operación de sistemas, equipos y procesos utilizados en la operación de los casinos, deberá considerar el desarrollo de procesos de análisis y gestión de riesgos, debidamente explicitados en el protocolo, que permitan por ejemplo, identificar las vulnerabilidades, amenazas y riesgos implícitos en el uso, procesamiento, almacenamiento y transmisión de la información; considerando la protección, detección, respuesta y recuperación ante incidentes de ciberseguridad que se presenten, contribuyendo a un ciberespacio seguro y resiliente.

Para la implementación de nuevas tecnologías, las sociedades operadoras y las sociedades concesionarias de casinos de juego, deberán adoptar las medidas tendientes a garantizar la operación y seguridad de las partes sensibles de sus sistemas, redes y equipos, así como también la obligación de resguardar la confidencialidad, disponibilidad e integridad de la información que se transmita y almacene por sus tecnologías, las que podrán ser acreditadas por cualquier medio para efectos de fiscalización por parte de la SCJ.

Con el objeto de garantizar la ciberseguridad en la implementación de nuevas tecnologías, las sociedades operadoras y las sociedades concesionarias de casinos de juego, deberán considerar un conjunto de medidas de mitigación de riesgos de Ciberseguridad. Lo anterior será validado y aprobado por el directorio o por la alta gerencia, si no cuenta con directorio,

de la sociedad operadora y concesionaria municipal, y notificando el acta o documento en que conste la aprobación vía Sistema de Autorizaciones y Notificaciones (SAYN) o a través de la plataforma informática establecida para este trámite, en la sección “Trámites” del sitio web institucional, o en la que la reemplace, a la Superintendencia durante los 30 días hábiles siguientes a su aprobación.

En el Anexo N°1 de la presente Circular se detallan el conjunto de materias mínimas para considerar en los análisis de riesgos de ciberseguridad.

4. Planes de gestión de riesgo

Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán contar con planes de gestión de riesgos de ciberseguridad, que deben estar documentados; y formulados con arreglo a principios, estándares y directrices que guarden la debida coherencia con las características de las redes, equipos y sistemas a los cuales se aplican. Dichos planes deberán formularse de forma que permitan anticipar consecuencias derivadas de amenazas tales como ciberataques y ciberincidentes no hostiles, en base a un análisis y evaluación de los riesgos a los cuales se exponen sus redes, equipos y sistemas, con el objetivo de evitar o reducir la ocurrencia de tales contingencias y mitigar sus eventuales efectos, indicando acciones inmediatas y medidas progresivas de mejoras, con sus respectivos indicadores, controles y documentación.

Al menos una vez al año calendario los planes de gestión de riesgo deberán ser revisados y en su caso actualizados y sometidos a conocimiento y aprobación del directorio o por la alta gerencia, si no cuenta con directorio, de la sociedad operadora o de la concesionaria municipal. La presentación que se haga deberá mencionar el estado de los riesgos de ciberseguridad e indicadores claves, con los incidentes y planes de acción de mejoras. Durante los 30 días corridos siguientes a su celebración se entregará a la Superintendencia una copia del acta de directorio o de la reunión de la alta gerencia, si la sociedad no cuenta con directorio, donde conste la realización de la revisión y aprobación, de la cual se podrá omitir la información no pertinente a ciberseguridad, y que será tratada con la debida reserva.

5. Documentación de planes de gestión

La documentación y demás antecedentes que den cuenta del detalle de los planes de gestión de riesgos deberán estar permanentemente disponibles en caso de fiscalizaciones a realizar por la Superintendencia. Asimismo, esta información podrá ser utilizada como antecedente, en el contexto de un simulacro voluntario de crisis gestionado por CSIRT en materias de ciberseguridad.

III. UNIDADES DE CIBERSEGURIDAD

1°. Unidades de ciberseguridad

Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán contar con una Unidad de Ciberseguridad, cuyo responsable será la contraparte técnica ante esta SCJ y deberá contar con las competencias suficientes para velar por la observancia de las obligaciones previstas en la presente circular, identificar los riesgos de afectación de los servicios por causa de ciberincidentes, verificar el cumplimiento eficaz de los respectivos planes de gestión, reportar los ciberincidentes y coordinar la gestión de ciberseguridad en general. Los roles y responsabilidades contempladas en esta Unidad deberán constar por escrito en el mismo Protocolo señalado en el numeral II.

La función de la Unidad de Ciberseguridad podrá ser realizada por un empleado/a dependiente de la sociedad operadora o por terceros. Tratándose de terceros, la función puede estar externalizada en un área del grupo económico controlador del cual forma parte integrante la sociedad operadora, pero fuera de la estructura organizacional de ésta última, o bien ser ejercida por terceros externos contratados especialmente para el desarrollo de las funciones establecidas en la presente circular.

La Unidad de Ciberseguridad deberá contar permanentemente con, a lo menos, un encargado/a titular de ciberseguridad en funciones y un suplente, quienes no requerirán de dedicación exclusiva.

Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán notificar a esta Superintendencia las identidades y medios de contacto del o la titular y suplente de la Unidad de Ciberseguridad, dentro de los 10 días hábiles siguientes a la entrada en vigencia de esta circular a través del SAYN o a través de la plataforma informática establecida para este trámite, en la sección "Trámites" del sitio web institucional, o en la que la reemplace. En el mismo plazo se deberá proceder ante modificaciones en dichos cargos. La designación podrá constar en acta de directorio o ser consideradas dentro de las funciones en el contrato individual de las personas que ostenten dichos cargos

Las competencias mínimas de la contraparte técnica ante esta SCJ están detalladas en Anexo N°2 de la presente Circular.

IV. REPORTE OBLIGATORIO DE CIBERINCIDENTES

1°. Obligación de reportar ciberincidentes

Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán reportar a la Superintendencia los ciberincidentes que detecte en sus redes, equipos y sistemas y que alcancen los Niveles de peligrosidad e impacto establecidos en esta circular, sin perjuicio de las instrucciones precisas que emita la Superintendencia respecto de tipos específicos de incidentes.

Como criterio de referencia para el reporte de un ciberincidente se utilizará el Nivel de peligrosidad que se le asigne conforme a la tabla número 1. Sin perjuicio de lo anterior, a lo largo del desarrollo, mitigación o resolución del ciberincidente, se categorizará con un Nivel de impacto que determinará la obligatoriedad de su reporte a la Superintendencia y/o al CSIRT. En caso de que un suceso pueda asociarse con dos o más tipos de incidentes con niveles de peligrosidad distintos, se le asignará el nivel de peligrosidad más alto de estos dos o más tipos.

a. Niveles de peligrosidad

El Nivel de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en las redes, equipos y sistemas de una entidad, así como para la calidad o continuidad de servicios prestados. Este indicador se fundamenta en las características intrínsecas de la tipología de amenaza. Sin ser taxativa la siguiente clasificación, forman parte de las redes, equipos y sistemas de información de los Casinos, los siguientes:

- i. Bases de datos de clientes asociados a, por ejemplo:
 - Clubes de fidelización.
 - Plataformas promocionales de juego.
- ii. Sistemas de administración operativa de los casinos de juego.
- iii. Red de CCTV.
- iv. Sistema de juego y comunicaciones:
 - Sistema de monitoreo y control (SMC)
 - Registro de eventos críticos de máquinas de azar (MDA)
 - Base de datos del SMC
- v. Registros asociados al Sistema de Prevención de Lavado de Activos y Financiamiento del Terrorismo.

vi. Registros asociados a juego responsable y autoexclusión voluntaria.

Conforme sus características, las amenazas serán clasificadas con los siguientes niveles depeligrosidad: Crítico, Muy Alto, Alto, Medio y Bajo. El nivel asignado se determinará según se indica en la tabla a continuación:

Tabla N°1: Niveles de Peligrosidad de ciberincidentes

| Nivel | Clasificación | Tipo de incidente |
|----------|---|---|
| Crítico | Otros | Amenaza Avanzada Persistente |
| Muy alto | Código dañino | Distribución de malware Configuración de malware |
| | Intrusión | Interceptación de datos sensibles (datos personales, bancarios, etc). Alteración o modificación de alguno de los elementos de las máquinas de azar |
| | Disponibilidad del servicio | |
| | | Interrupciones |
| Alto | Contenido abusivo | Pornografía infantil, contenido sexual o violento inadecuado |
| | Código Dañino | Sistema infectado Servidor C&C (Mando y Control) |
| | Intrusión | Compromiso de aplicaciones Compromiso de cuentas con privilegios |
| | Intento de Intrusión Disponibilidad del servicio Compromiso de la información Fraude | Ataque desconocido DoS (Denegación de servicio) DDoS (Denegación distribuida de servicio)Acceso no autorizado a información |
| | | Modificación no autorizada de información |
| | | Pérdida de datos Phishing |
| | | |
| Medio | Contenido abusivo | Discurso de odio |
| | Obtención de información | Ingeniería social Explotación de vulnerabilidades conocidas. |
| | Intrusión | Intento de acceso con vulneración de credenciales. Compromiso de cuentas sin privilegios. |
| | Disponibilidad del servicio | Mala configuración Uso no autorizado de recursos |
| | Fraude | Derechos de autor Suplantación |
| | Vulnerable | Criptografía débil Amplificador DDoS |
| | | Servicios con acceso potencial no deseado |

| Nivel | Clasificación | Tipo de incidente |
|-------|---|---|
| | | Revelación de información Sistema vulnerable |
| Bajo | Contenido abusivo Obtención de información Otros | Spam Escaneo de redes |
| | | Análisis de paquetes (sniffing) Otros |

b. Niveles de impacto

Los criterios empleados para la determinación del nivel de impacto asociado a un ciberincidente atienden los parámetros que se indican a continuación, sin un orden de prelación o importancia predeterminado:

- Tipología de la información o sistemas afectados.
- Grado de afectación a las instalaciones.
- Posible interrupción en la prestación del servicio normal.
- Tiempo y costos propios y ajenos hasta la recuperación del normalfuncionamiento de las instalaciones y equipos.
- Pérdidas económicas.
- Cantidad de unidades operativas o de negocio afectadas.
- Daños reputacionales asociados.

Los posibles niveles de impacto de un ciberincidente son Crítico, Muy Alto, Alto, Medio, Bajo o Sin Impacto. El nivel de impacto correspondiente se asignará usando como referencia la siguiente tabla:

Tabla N°2: Niveles de impacto de ciberincidentes

| Nivel | Descripción |
|----------|--|
| Crítico | Afecta a sistemas clasificados como confidenciales o que contengan datos calificados como sensibles de acuerdo con la ley vigente. |
| | Afecta a más del 90% de los sistemas de la organización. |
| | Interrupción en la prestación del servicio igual o superior a 24 horas. |
| | El ciberincidente requiere más de 504 horas corridas para su resolución. |
| | El ciberincidente afecta a más de un casino a nivel nacional. |
| Muy alto | Daños reputacionales muy elevados. |
| | Afecta la vida privada y/o la honra de la persona y su familia, y asimismo, la protección de sus datos personales. |
| | Afecta a un servicio o sistema esencial para la operación del casino de juego. |
| | Afecta a más del 75% de los sistemas del casino de juego |
| | Interrupción en la prestación del servicio igual o superior a 8 horas. |
| Alto | El ciberincidente precisa para resolverse de 240 horas corridas. |
| | El ciberincidente afecta a 2 o más casinos a nivel Nacional. |
| | Afecta a más del 50% de los sistemas del supervisado. |
| | Interrupción en la prestación del servicio igual o superior a 1 hora. |
| | El ciberincidente requiere de 120 horas corridas para su resolución. |
| Medio | El ciberincidente afecta a 1 casino a nivel Nacional. |
| | Daños reputacionales de difícil reparación, con eco mediático afectando a la reputación de terceros. |
| | Afecta a más del 20% de los sistemas del supervisado. |
| | Interrupción en la presentación del servicio igual o superior a 30 minutos. |
| | El ciberincidente requiere de 40 horas corridas para su resolución. |
| | Daños reputacionales apreciables, con eco mediático. |

| Nivel | Descripción |
|-------------|---|
| Bajo | Afecta a los sistemas del supervisado. Interrupción de la prestación de un servicio. |
| Sin impacto | Daños reputacionales puntuales, sin eco mediático. No hay ningún impacto apreciable. |

c. Ciberincidentes de reporte obligatorio

Los ciberincidentes se asociarán a los niveles de peligrosidad o de impacto que les correspondan de conformidad con lo dispuesto en el presente numeral, siendo obligatorio el reporte de todos aquellos ciberincidentes que alcancen un nivel de peligrosidad o impacto calificado como Crítico, Muy Alto o Alto y aquellos incidentes que interrumpan el normal desarrollo del juego.

Además, las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán notificar a la Superintendencia los incidentes de ciberseguridad que afecten a proveedores de máquinas de azar, que alcancen un nivel de peligrosidad o impacto calificado como Crítico, Muy Alto o Alto, tan pronto tengan conocimiento de ellos.

Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán reportar a la Superintendencia a través del SAYN, o a través de la plataforma informática establecida para este trámite, en la sección “Trámites” del sitio web institucional, o en la que la reemplace, en tiempo y forma todos los ciberincidentes que registren en sus redes, equipos y sistemas de información, como asimismo aquellos que afecten a proveedores de máquinas de azar y estén obligados a notificar por superar los umbrales de impacto o peligrosidad dispuesto en el presente numeral, además de los incidentes que interrumpan el normal desarrollo del juego. El formulario SAYN o de la plataforma informática correspondiente contemplará los campos requeridos. Sin perjuicio de lo anterior, la Superintendencia podrá establecer reglas de reportes especiales aplicables a tipos específicos de incidentes.

La obligación de reportar se entenderá formalmente cumplida con el envío del reporte a la Superintendencia a través de los mecanismos dispuestos para ello y es independiente a toda instrucción dictada por la SCJ relativa a la notificación de contingencias. Con todo, cualquier consulta adicional, generará una nueva obligación para la sociedad operadora de reportar, dentro del plazo señalado en el propio requerimiento.

La sociedad operadora o concesionaria municipal no debe omitir deliberadamente reportar un ciberincidente de reporte obligatorio.

2°. Contenido de los reportes

Se deberá reportar en tiempo y forma toda aquella información relativa al ciberincidente que sea exigible. Sin embargo, en el reporte inicial solamente deberá proporcionar la información que tenga en su conocimiento en ese momento, debiendo completarla en los reportes que envíe con posterioridad.

Los reportes de ciberincidentes deberán contener, a lo menos, los siguientes campos de información que se encontrarán disponibles en la plataforma SAYN o en la plataforma informática establecida para este trámite, en la sección “Trámites” del sitio web institucional, o en la que la reemplace.

- Resumen ejecutivo del ciberincidente.
- Identificación de la sociedad operadora o concesionaria municipal
- Encargado de ciberseguridad en funciones.
- Fecha y hora precisas de ocurrencia del ciberincidente.
- Fecha y hora precisas de detección del ciberincidente.
- Descripción detallada de lo sucedido.
- Recursos tecnológicos afectados.
- Origen o causa identificable del ciberincidente.

- i. Taxonomía, clasificación o tipo de ciberincidente.
- j. Nivel de peligrosidad
- k. Nivel de impacto
- l. Indicadores de compromiso: indicadores de compromiso de nivel IP, indicadores de compromiso de nivel de dominios y subdominios, indicadores de compromiso de correos, indicadores de compromiso a nivel MD5, entre otros similares.
- m. Plan de acción y medidas de resolución y mitigación.
- n. Afectados actuales y potenciales.
- o. Medios necesarios para la resolución calculados en horas de trabajo necesarias.
- p. Impacto económico estimado, si procede y es conocido.
- q. Cantidad de unidades operativas o de negocio afectadas, si se conociere.
- r. Daños reputacionales, aun cuando sean eventuales.
- s. Las bitácoras generadas de forma automática por los sistemas, si corresponde
- t. Antecedentes que se adjuntan, si procede.

3°. Oportunidad de los reportes

Los reportes consideran tres etapas: un reporte inicial, reportes intermedios y un reporte final.

El reporte inicial, obligatorio, es una comunicación consistente en poner en conocimiento y alertar de la existencia de un ciberincidente.

Los reportes intermedios actualizan los datos disponibles en ese momento con relación al ciberincidente comunicado. Se efectuarán tantos reportes intermedios como se consideren necesarios a partir de la hora en que se generó el reporte inicial inmediato. Con todo, deberá informarse, haya o no novedades, con la frecuencia indicada en la tabla N°3, salvo que se haya efectuado el reporte final del ciberincidente en ese mismo período.

El reporte final amplía y confirma los datos definitivos en relación con el ciberincidente reportado a partir del día en que se generó el reporte inicial inmediato.

Tabla N°3: Oportunidad de reportes obligatorios

| Nivel de peligrosidad o impacto | Reporte inicial | Reporte intermedio | Reporte final |
|---------------------------------|-----------------|-------------------------|------------------------|
| Crítico | 1 hora | 3/ 6/ 12/ 24/ 48 horas | Máximo 10 días hábiles |
| Muy alto | 1 hora | 6/ 12/ 24/ 48/ 72 horas | Máximo 15 días hábiles |
| Alto | 1 hora | 24/ 48/ 72 horas | Máximo 20 días hábiles |

Toda la información reportada deberá quedar registrada y disponible por parte de la sociedad operadora y concesionaria municipal.

4°. Tratamiento de los reportes

Los reportes de ciberincidentes serán tratados como documentación confidencial. En particular, en aquellos datos que pudiera exponer antecedentes técnicos propios de la sociedad operadora o concesionaria municipal, que pongan en riesgo la ciberseguridad del mismo, así como la información de clientes en conformidad a la legislación sobre protección de la vida privada.

V. INFORMACIÓN A TERCEROS E INTERCAMBIO DE INFORMACIÓN

En caso de reportar y/o alertar a terceros para prevenir, gestionar o resolver un

ciberincidente, la sociedad operadora o concesionaria municipal podrá solicitar, por intermedio de la Superintendencia, la asistencia del CSIRT, el que actuará conforme a su disponibilidad. En caso de requerir apoyo de Equipos de Respuesta en el extranjero, se deberá velar por la privacidad y el debido resguardo de los datos personales involucrados.

En el intercambio de información se estará a las indicaciones que figuren en los reportes respecto del alcance que puede tener la difusión de la información que contiene conforme el estándar *Traffic Light Protocol* TLP, descrito en Anexo N°3 de la presente circular. En caso de estimarse que es necesario difundir la información a terceros más allá del alcance de la designación TLP indicada por el autor del reporte, se requerirá autorización de la fuente original. En general, no se revelarán cualesquiera datos que pudieran exponer antecedentes técnicos propios del regulado, que pongan en riesgo la Ciberseguridad del mismo, así como cualquier información de sus clientes, conforme lo dispuesto en la ley sobre protección de la vida privada.

En caso de que se decida informar directamente al público o terceros, la publicación estará orientada a la entrega de información sobre los ciberincidentes, posibles causas, medidas de mitigación, recomendaciones de seguridad, alternativas de acciones a seguir, o sistemas afectados y cualquier otra información de importancia para la correcta y oportuna información del público en general, sin que esto signifique afectaciones a la reputación de los involucrados.

VI. RESOLUCIÓN DE CIBERINCIDENTES

1. Obligación de resolución de ciberincidentes

Una vez detectado un ciberincidente que afecte a una red, equipo o sistema utilizado para la prestación de servicios, la sociedad operadora o concesionaria municipal deberá efectuar de manera oportuna todas las gestiones que sean necesarias para su resolución y restaurar la normal provisión de los servicios afectados, con arreglo a su plan de gestión de riesgos y, en todos los casos, dando primera prioridad a aquellas medidas que permitan evitar o, en su defecto, minimizar el impacto a los clientes finales.

Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán proporcionar la información adicional que les sea requerida para analizar la naturaleza, causas y efectos de los incidentes notificados, así como para elaborar estadísticas y reunir los datos necesarios para elaborar informes de resultados. La información adicional proporcionada será tratada con reserva y no será usada para fin alguno que sea distinto de los autorizados.

Asimismo, sin perjuicio de las medidas inmediatas conducentes a la mitigación de los efectos y al restablecimiento de los servicios afectados por un ciberincidente, las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán subsanar, en la medida que sea técnicamente posible, según los respaldos fundados, las vulnerabilidades de sus sistemas, equipos y redes que hubieren permitido o facilitado ciberincidentes. Las medidas adoptadas deberán ser informadas a la Superintendencia en caso de ser solicitado por ésta.

En caso de que las sociedades operadoras y las sociedades concesionarias de casinos de juego detecten que sus redes, equipos y sistemas fueron utilizados como medio para la comisión de algún delito informático, deberá informarlo a la Superintendencia al momento del reporte. Junto a ello y de estimarlo necesario, deberán propender a formular las denuncias ante los órganos competentes y ejercer las acciones judiciales pertinentes.

Las sociedades operadoras y las sociedades concesionarias de casinos de juego serán responsables, por las pérdida o filtración de información que sea producto de su negligencia con respecto a la recepción, tenencia, manipulación, almacenamiento y entrega de la información que se trasmite o deposita en custodia en sus sistemas, para garantizar la certeza, confidencialidad, seguridad y no repudiación de la comunicación.

Asimismo, es recomendable que las sociedades operadoras y las sociedades concesionarias de casinos de juego realicen un proceso de investigación forense para los ciberincidentes relevantes, ciberataques y ciberdelitos, efectuados tanto por personal interno como también desde el exterior, considerando al menos las etapas de identificación, recopilación, adquisición, examen y análisis de evidencias digitales, junto con la generación de documentación e informes de la investigación forense, interpretación de evidencia digital y las conclusiones del trabajo realizado; además de cumplir los requerimientos necesarios para preservar y realizar adecuadamente la cadena de custodia de las evidencias digitales obtenidas y generadas. Este proceso de investigación forense podrá ser realizado por la Unidad de ciberseguridad o por personal externo con competencias comprobables.

Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán diseñar, implantar y mantener controles de protección y detección para facilitar el proceso de investigación forense, entre los que se encuentra gestionar el ciclo de vida completo de registros históricos (logs) en aspectos tales como: existencia, nivel de detalle, consistencia de su información, período de resguardo mínimo de seis meses durante los primeros 3 años de vigencia de la presente Circular (luego de ese período, el resguardo deberá ser mínimo por un año) y modo de resguardo, como también realizar periódicamente pruebas de trazabilidad para asegurar su calidad y que serán de utilidad al momento de ser requeridos para una investigación forense. Esto es aplicable para tanto para sistemas e infraestructura interna, servicios externalizados, y servicios o tecnologías contratadas”.

2. Resguardo de datos sensibles

Deberán omitirse en los reportes de ciberincidentes todo dato o información personal de carácter sensible, conforme a lo dispuesto en el artículo 2 letra g) de la Ley N°19.628 sobre Protección de la Vida Privada² o la que la reemplace, así como toda otra información a partir de la cual sea posible inferirlos. Asimismo, en los casos en que la autoridad competente instruya a la sociedad operadora o concesionaria municipal para que envíe a un tercero una copia de un reporte, deberá eliminar todos los datos personales o que permitan deducir la identidad de la persona aludida.

En todos los casos, deberán considerarse las regulaciones de utilización de la información del usuario y su metadata, ya sea para beneficio propio de la sociedad operadora o concesionaria municipal o de terceros, sin la expresa autorización del cliente, conforme lo establecido en el artículo 9° de la citada ley N°19.628 y conforme los principios transversales de derechos humanos reconocidos por la comunidad internacional.

VII. REPORTES NO OBLIGATORIOS

Las sociedades operadoras y las sociedades concesionarias de casinos de juego podrán reportar sobre ciberincidentes que no alcancen los umbrales de información obligatoria especificados en el título IV. En cualquier caso, todo reporte de ciberincidente le obligará a proseguir reportando el desarrollo de éste, si así correspondiere conforme la presente circular, y a gestionar su resolución.

VIII. SUPERVISIÓN DE SEGURIDAD

Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán someter a lo menos una vez al semestre sus redes, equipos y sistemas a pruebas de seguridad. Las pruebas podrán ser efectuadas por las sociedades operadoras y las sociedades concesionarias de casinos de juego en forma interna, o bien, con asistencia por parte de terceros externos especializados en dichos servicios.

² Art. 2 letra g) Ley N°19.628: Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

En todo caso, deberán efectuarse conforme estándares actualizados, sean nacionales o internacionales, o bien, conforme criterios ampliamente aceptados por la industria. Deberá dejarse constancia de las pruebas efectuadas, los estándares aplicados, los resultados obtenidos, las medidas adoptadas en consecuencia y las oportunidades de mejora detectadas.

Asimismo, se deberá informar a la SCJ mediante el SAYN o a través de la plataforma informática establecida para este trámite, en la sección “Trámites” del sitio web institucional, o en la que la reemplace, su ejecución a más tardar 15 días hábiles luego de realizadas.

Las pruebas de seguridad y simulacros de ciberseguridad deberán considerar, a lo menos, las siguientes actividades de control y documentación:

- Elaboración del conjunto de pruebas de seguridad a realizar, identificando la infraestructura física y lógica a utilizar.
- Descripción detallada de cada prueba o simulación, el procedimiento de ejecución y los medios de evidencia o verificación del cumplimiento satisfactorio de las pruebas.
- Descripción detallada de las actividades o medidas y procedimientos de restauración para la continuidad operacional y de servicio.
- Verificación de la consistencia y seguridad del almacenamiento de los logs o registros que evidencien los incidentes de ciberseguridad y otros datos tales como direcciones, puertos, aplicaciones, contenidos, datos transmitidos, mensajes de los sistemas sometidos a pruebas o simulación de ciberataque o incidente de ciberseguridad.
- Preparar un reporte con el resultado de las pruebas o simulaciones de seguridad, con medios de verificación apropiados.

IX. DISPOSICIONES FINALES

1. Fiscalización

La Superintendencia podrá fiscalizar en cualquier momento el cumplimiento de las obligaciones contenidas en esta circular.

2. Sanciones

Las infracciones a las disposiciones de la presente circular serán sancionadas de acuerdo con lo dispuesto en el artículo 46 de la Ley N°19.995.

3. Entrada en vigencia

La presente circular entrará en vigencia transcurrido seis meses contados desde su dictación.

FIRMADO POR VIVIEN VILLAGRÁN ACUÑA, SUPERINTENDENTA DE CASINOS DE JUEGO