GOBIERNO DE CHILE
JUNTA NACIONAL DE AUXILIO
ESCOLAR Y BECAS

APRUEBA PROCEDIMIENTO DE GESTIÓN DE INCIDENTES QUE INDICA, EN EL MARCO DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN DE LA JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS.

RESOLUCIÓN EXENTA N° 3168

SANTIAGO, 30-11-2017

VISTO:

Lo dispuesto en la Ley N° 15.720 que crea la Junta Nacional de Auxilio Escolar y Becas; en la Ley N° 19.880, que establece Bases de los Procedimientos Administrativos que rigen las Actas de los Órganos de la Administración del Estado; en el Decreto Supremo del Ministerio de Educación N° 5.311 de 1968, que aprueba el Reglamento General de JUNAEB; en el Decreto Ley del Ministerio de Educación N° 180 de 1973, que declara receso del consejo de JNAEB cuyas facultades otorga a su Secretario General; en el Decreto Supremo del Ministerio Secretaría General de Gobierno N°83 del 2005, que aprueba Norma Técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos; Decreto Supremo del ministerio de Secretaría General de Gobierno N° 77 del 2004, que aprueba Norma Técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la Administración del Estado y entre estos los ciudadanos del Ministerio Secretaría General de la Presidencia; en el Decreto exento del Ministerio de Educación N° 1106 de noviembre de 2016 que nombra a don Jaime Tohá Lavanderos como Secretario General (S) de la Junta Nacional de Auxilio Escolar y Becas; y la resolución N° 1.600 de 2008 de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón.

CONSIDERANDO:

1. Que en virtud del Decreto Exento del Ministerio de Hacienda N° 194 de 17 de mayo de 2017, que modifica el Decreto Exento 290 de agosto de 2016, se aprueba el Programa Marco de los Programas de Mejoramiento de la Gestión (PMG) para el año 2017; el cual consta de dos áreas prioritarias y tres sistemas de gestión con sus respectivos objetivos, debiendo los servicios formular compromisos en uno o más sistemas de gestión, dependiendo del grado de desarrollo alcanzado a la fecha de la formulación.

2. Que, en lo que respecta a la Junta Nacional de Auxilio Escolar y Becas, uno de los Programas de Mejoramiento de Gestión dice relación con el Sistema de Seguridad de la Información, correspondiente al área de Calidad de Servicio y que

DIRECCIÓN

tiene por objetivo de gestión "*Gestionar los riesgos de seguridad de la información de los activos que soportan los procesos de provisión de bienes y servicios, mediante la aplicación de controles basados en la Norma NCH-ISO 27001 Of2013 del Instituto Nacional de Normalización, sobre Sistemas de Seguridad de la Información*".

3. Que, en este sentido, la referida la Norma NCHI-ISO 27001 Of2013; dispone en el punto 4.4 denominado "*Sistema de Seguridad de la Información" que "la organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, según los requerimientos de esta norma*"

RESUELVO:

APRUEBASE el siguiente documento relativo al Sistema de Seguridad de la Información de la Junta Nacional de Auxilio Escolar y Becas, cuyo texto se adjunta a la presente resolución y se entiende incorporado, de acuerdo al siguiente nombre:

1. A.16.01.01 – Responsabilidades y Procedimientos.
2. A.16.01.02 - Informes de Eventos en la seguridad.
3. A.16.01.03 - Reporte de las debilidades en la seguridad.
4. A.16.01.04 - Evaluación y decisión sobre los eventos de seguridad de la Información.
5. A.16.01.05 - Respuesta ante incidentes de seguridad de la Información.

ARTÍCULO 2°: **PUBLÍQUESE** la presente resolución una vez tramitada, en la sección Actos y Resoluciones ubicado en el mini sitio "Gobierno Transparente", en el portal web de JUNAEB, a objeto de dar cumplimiento con lo previsto tanto en el artículo 7° de la ley N°20.285, sobre Acceso a la Información Pública, como en el artículo 51° de su Reglamento.

Junta Nacional de Auxilio Escolar y Becas
SECRETARIO GENERAL
DIRECCIÓN

JAIME TOHÁ LAVANDEROS
SECRETARIO GENERAL (S)
JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS

MBG/RFV/FFR/jhs
DISTRIBUCIÓN:
1. Departamentos de Dirección Nacional y Direcciones Regionales
2. Oficina de Partes

DIRECCIÓN

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

Autorizado Firma Jefe del Informática	Autorizado Encargado de Seguridad de la Información
Elaborado por: Departamento de informática	Revisado por: Departamento de Planificación

INDICE

DIRECCIÓN

1 OBJETIVO

Establecer las actividades necesarias en Junaeb, para la detección oportuna y tratamiento de debilidades o eventos que comprometan la seguridad de los activos de información de la institución, a través de canales y puntos de contacto definidos.

2 ALCANCE

El presente procedimiento es aplicable por los siguientes centros de responsabilidad del nivel central (Dirección Nacional)[1], ya que son las encargadas de monitorear los incidentes, amenazas y debilidades asociados a la seguridad de la información que les compete:

- Depto. de Informática.
- Depto. de Administración y Finanzas.
- Depto. de Gestión de Personas.

Incidentes de Seguridad que afecten a los activos de información del tipo: base de datos, documento, equipo, expediente, formulario, infraestructura física, persona, sistema de información software en cuanto.

- Confidencialidad: acceso no autorizado a la información.
- Integridad: Modificación no autorizada, destrucción o perdida de información.
- Disponibilidad, inaccesibilidad a la información.

El procedimiento es aplicable a todos los funcionarios planta, contrata, reemplazos y suplencia, personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para Junaeb.

Abarcando los objetivos dispuestos en la norma 27001:2013 en sus controles:

A.16.01.01 – Responsabilidades y Procedimientos.

A.16.01.02 – Informe de Eventos en la seguridad.

A.16.01.03 - Reporte de las debilidades en la seguridad.

A.16.01.04 - Evaluación y decisión sobre los eventos de seguridad de la información.

A.16.01.05 - Respuesta ante incidentes de seguridad de la información.

3 DEFINICIONES

- **Gestión de incidentes[2]:** Manejo o administración de los incidentes.
- **Evento de Seguridad de la Información**: Corresponde a una ocurrencia identificada que puede ser relevante para la seguridad de la información. Una falla en las medidas de seguridad.
- **Incidente[3]**: Cualquier evento o una serie de eventos o una situación que comprometa de manera importante la disponibilidad, integridad y/o confidencialidad de la información. En general, es una violación de una política, estándar o procedimiento de seguridad que no permita el correcto funcionamiento de los servicios y operación de JUNAEB, así como cualquier evento que ponga en riesgo los activos de información de la institución.
- **Diferencia entre "evento" e "incidente"[4]:** Un evento no puede tener implicaciones negativas. El término evento puede ser utilizado como una expresión neutral. Los incidentes, por el contrario, pueden tener una connotación negativa.
- **Puntos de contacto**: Son los mecanismos y formas de comunicación que tendrá a cargo cada departamento, que indica el cómo proceder y con quien proceder al momento de existir un incidente de seguridad de la información, "Contacto con Autoridades" para recibir avisos de incidentes por

[1] Comprende las diferentes direcciones que abarque la Dirección Nacional de JUNAEB
[2] Según la norma ISO/IEC 27000:2014
[3] Según la norma ISO/IEC 27000:2014
[4] http://www.pmg-ssi.com/2016/09/iso-27001-diferencia-entre-evento-e-incidente/

DIRECCIÓN

cualquier funcionario planta, contrata, reemplazos y suplencia; personal a honorarios y contratista que presten servicios en la Dirección Nacional de JUNAEB.

- **Depto. de los ámbitos de aplicación**: Son los responsables de los puntos de detección de incidentes, cuya función es emitir un reporte de evento e incidentes de seguridad de la información en los tiempos, metodología y formatos establecidos.
- **CISO:** Encargado de Seguridad de la Información.
- **Comité de Seguridad TI:** Comité liderado por el Jefe del Departamento de Informática junto a miembros de las unidades de Sistemas e Infraestructura, Desarrollo y Mantención de Sistemas, Unidad de Control de Gestión Interna y Procesos.
- **Comité de Seguridad De la Información:** Comité liderado por el CISO y con participación activa del Jefe del Departamento de Informática, Jefe del Departamento de Administración y Finanzas, Jefe del Departamento de Gestión de Personas, Jefe del Servicio, además de integrantes que se propongas como otros Jefes de centros de responsabilidad.
- **Amenaza:** Es un evento que puede causar un incidente de seguridad en una organización produciendo pérdidas o daños potenciales en sus activos.
- **Evento do Seguridad de la Información**: Corresponde a una ocurrencia Identificada que puede ser relevante para la seguridad de la información.
- **Debilidades en la seguridad de la información:** Debilidad de un activo o de un grupo de activos que puede ser explotada por una o más amenazas que pueden poner en riesgo la seguridad de la información.
- **Incidente de seguridad de la información:** Cualquier evento o situación que comprometa de manera importante la disponibilidad, integridad y/o confidencialidad de la información. En general, es una violación de una política, estándar o procedimiento de seguridad que no permita el correcto funcionamiento de los servicios.

4 DESARROLLO DEL PROCEDIMIENTO

4.1 ROLES Y RESPONSABILIDADES

Rol	Responsabilidad
Funcionario	Informar cualquier evento o debilidad que pueda afectar la Seguridad de la Información
Encargado de Seguridad de la Información	Es responsable de la aplicación de este procedimiento, gestionar los eventos, debilidades e incidentes de seguridad de la información
Jefaturas de Departamento de la Dirección Nacional	Responsable de manejar los problemas relacionados a los incidentes de seguridad de la información dentro de su centro de responsabilidad, implementando los procedimientos establecidos, además deberá recolectar evidencia para documentar el incidente.
Comité de Seguridad de la Información:	Es responsable de garantizar que las personas responsables de administrar los incidentes de seguridad de la información, comprendan las prioridades de la organización para manejar dichas materias. Asimismo, responsables de solicitar al Encargado de la Seguridad de la Información mejoras en políticas, procedimientos y planes de contingencia o implementación de nuevos controles adicionales para fortalecer las acciones preventivas ante la posibilidad de un incidente, este comité es liderado por el CISO (CISO, Jefe Departamento de Informática, Jefes de áreas programáticas, Jefe del Servicio, entre otras jefaturas).
Mesa de Ayuda	Punto de contacto para eventos o incidente Tecnológico, encargado de derivar incidente al comité de Seguridad TI

DIRECCIÓN

Comité de Seguridad TI	Analizar los eventos o incidentes de seguridad de la información y discriminar si efectivamente se trata de un evento o incidente de seguridad de la información Informática o no.

4.2 NOTIFICACIÓN DEL EVENTO

Todo funcionario planta, contrata, reemplazos y suplencia; personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios en la Dirección Nacional de JUNAEB, ante la sospecha o indicio de fallas u otro comportamiento anómalo que configure un incidente de Seguridad de la Información, es responsable de informar a su jefatura directa o notificarlo a través de los canales o puntos de contacto, que éste disponga.

Es primordial que el funcionario notifique a la brevedad para que pueda dar inicio al procedimiento de Gestión de Incidentes de Seguridad de la Información, detallado en el control A.16.01.01 "Responsabilidades y procedimientos", respecto del tratamiento de incidentes en el Sistema de Seguridad de la Información.

4.2.1 TIPO DE INCIDENTE

Tipo	Descripción	Ejemplos
Informático	Todos aquellos incidentes que afecten las tecnologías de la información	• Denegación de servicios computacionales • Fallas en sistemas informáticos • Código malicioso • Acceso no autorizado a sistemas informáticos • Infraestructura TI
No Informático	Todos aquellos incidentes no contemplados en el punto anterior	• Violaciones de confidencialidad, integridad y disponibilidad (documento) • Filtración de información reservada • Incidentes provocados por la naturaleza • Acceso físico no autorizado

4.2.2 TIEMPO DE RESPUESTA A INCIDENTE

Variables	Descripción	Rango de Tiempo
Bajo	Tiempo máximo de demora que puede aceptar el proceso de resolución del incidente	Desde 241 min o mas
Medio		Desde 61 min a 240 min
Alto		Menor o igual a 60 min

DIRECCIÓN

4.2.3 CATEGORÍAS DE IMPACTO DE INCIDENTE

Categoría	Valor	Descripción
Catastrófico	5	Puede generar efectos en los activos de información que se traduce en un impacto monetario para la organización, lo que impactara catastróficamente el presupuesto y existirá un compromiso mayor sobre la imagen de la organización. Su materialización daña el proceso y cumplimiento de los objetivos impidiendo el cumplimiento de estos.
Mayores	4	Su materialización puede generar pérdidas financieras, que impactaran el presupuesto, compromiso de la imagen pública y del gobierno, lo que impedirá parcial o totalmente el cumplimiento de los objetivos
Moderados	3	Su materialización puede generar pérdidas financieras, lo que tendrá un impacto moderado sobre el presupuesto, comprometiendo moderadamente la imagen pública de la institución y el gobierno, su materialización causaría un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo el desarrollo en forma normal de este
Menores	2	Su materialización puede generar pérdidas financieras, las que tendrán un impacto menor en el presupuesto, compromete de forma menor la imagen pública de la institución y del gobierno. Su materialización causara un bajo daño en el desarrollo del proceso y no afectara el cumplimiento de los objetivos
Insignificantes	1	Su materialización no generara pérdidas financieras, y no compromete de ninguna forma la imagen pública de la institución y del gobierno, su materialización puede tener un pequeño o nulo efecto en el desarrollo del proceso y que no afectaría el cumplimiento de los objetivos

DIRECCIÓN

4.2.4 CATEGORÍAS DE PROBABILIDAD DE INCIDENTE

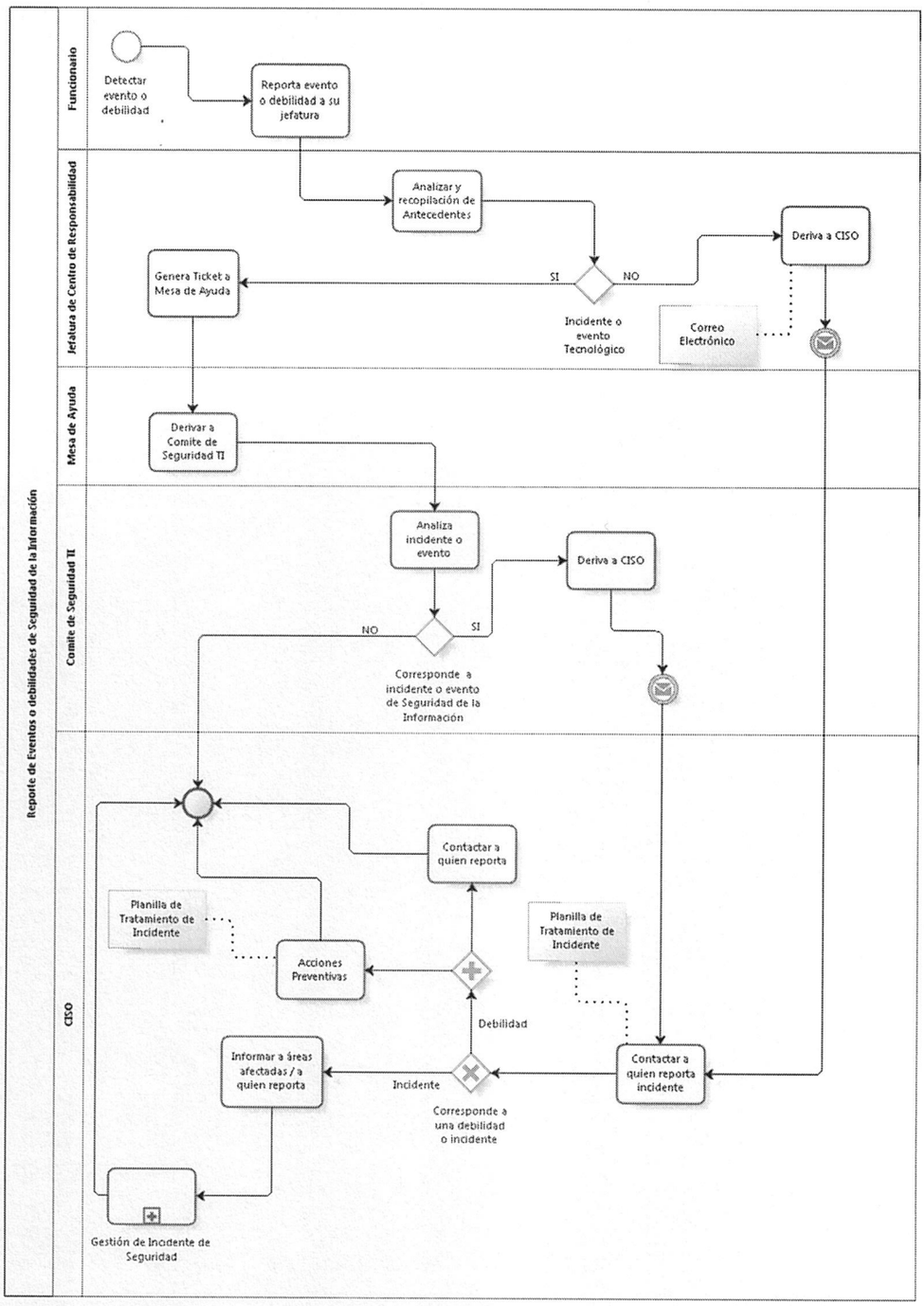
Categoría	Valor	Descripción
Casi Certeza	5	Probabilidad de ocurrencia muy alta, entre 90% y 100% de materialización
Probable	4	Probabilidad de ocurrencia alta, entre 66% y 89% de materialización
Moderado	3	Probabilidad de ocurrencia media, entre 31% y 65% de materialización
Improbable	2	Probabilidad de ocurrencia baja, entre 11% y 30% de materialización
Muy Improbable	1	Probabilidad de ocurrencia muy baja, entre 1% y 10% de materialización

4.2.5 TABLA DE PONDERACIÓN DE RIESGO

Nivel de Probabilidad (P)	Nivel de Impacto (I)	Severidad del Riesgo (S) S = (P*I)
Casi Certeza (5)	Catastróficas (5)	Extremo (25)
Casi Certeza (5)	Mayores (4)	Extremo (20)
Casi Certeza (5)	Moderadas (3)	Extremo (15)
Casi Certeza (5)	Menores (2)	Alto (10)
Casi Certeza (5)	Insignificantes (1)	Alto (5)
Probable (4)	Catastróficas (5)	Extremo (20)
Probable (4)	Mayores (4)	Extremo (16)
Probable (4)	Moderadas (3)	Alto (12)
Probable (4)	Menores (2)	Alto (8)
Probable (4)	Insignificantes (1)	Moderado (4)
Moderado (3)	Catastróficas (5)	Extremo (15)
Moderado (3)	Mayores (4)	Extremo (12)
Moderado (3)	Moderadas (3)	Alto (9)
Moderado (3)	Menores (2)	Moderado (6)
Moderado (3)	Insignificantes (1)	Bajo (3)
Improbable (2)	Catastróficas (5)	Extremo (10)
Improbable (2)	Mayores (4)	Alto (8)
Improbable (2)	Moderadas (3)	Moderado (6)
Improbable (2)	Menores (2)	Bajo (4)
Improbable (2)	Insignificantes (1)	Bajo (2)
Muy Improbable (1)	Catastróficas (5)	Alto (5)
Muy Improbable (1)	Mayores (4)	Bajo (4)
Muy Improbable (1)	Moderadas (3)	Moderado (3)
Muy Improbable (1)	Menores (2)	Bajo (2)
Muy Improbable (1)	Insignificantes (1)	Bajo (1)

DIRECCIÓN

4.3 REPORTE DE EVENTOS Y DEBILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN



4.3.1 NOTIFICACIÓN DE EVENTO INFORMÁTICO.

a) Todo funcionario que sostenga la sospecha de fallas o anomalías e inclusive fugas de información en los sistemas informáticos de Junaeb, el cual pueda ser catalogado como un Incidente de Seguridad de la Información deberá informar a la jefatura de su centro de responsabilidad.
b) La jefatura del Centro de Responsabilidad debe recopilar la información a través del formulario de registro de incidente Anexo N°1 y generar un ticket a la mesa de ayuda siempre y cuando el análisis realizado de como conclusión que se está en presencia de un evento o Incidente de Seguridad de la Información.
c) La mesa de ayuda derivara dicha información al Comité de Seguridad TI del Departamento de Informática.
d) El comité de seguridad TI, del Departamento de Informática deberá analizar los antecedentes proporcionados por el funcionario denunciante y ver si procede o no como un caso de Incidente de Seguridad de la Información, este comité podrá requerir mayor información del denunciante.
e) Si lo reportado corresponde a un Incidente de Seguridad de la Información, el comité de seguridad TI del Departamento de Informática clasificara, categorizara y generara las tareas y acciones de priorización de los trabajos requeridos para solucionar la problemática, lo que quedara plasmado en el formulario de valoración de incidentes, Anexo N°2, el Comité de Seguridad TI remitirá esta información a la Jefatura del Departamento de Informática.
f) El Jefe del Departamento de Informática deberá remitir dicha información, Anexo N°1 y Anexo N°2 al CISO de la organización.
g) El CISO es responsable de activar el plan o procedimiento de gestión de incidentes de seguridad de la información, contactando a la persona que reporto el evento o incidente.
h) El CISO revisa y puede re categorizar el evento modificando el formulario de valoración de incidentes Anexo N°2, categoriza el evento según la matriz de riesgo y acciona los procesos de acciones preventivas y la gestión del incidente de seguridad.
i) El CISO es encargado de generar el formulario de resultado de gestión del incidente Anexo N°3 e informar a las áreas involucradas y a quien reporte el incidente.
j) El CISO es encargado de incorporar la información en la Planilla de tratamiento de incidente la información que contengan los anexos N°1, N°2 y N°3.

4.3.2 NOTIFICACIÓN DE EVENTO DE ÁMBITO NO INFORMÁTICO.

Cabe señalar que estos casos son aquellos en los cuales se está ante un delito fragante de fuga de información, pérdida de esta o mal uso por parte de funcionarios o personas externas que tengan acceso a documentación, activos de la organización que puedan provocar perdida del activo y seguridad de la información.

a) Todo funcionario que sostenga la sospecha de fallas o anomalías e inclusive fugas de información en el ámbito de su trabajo diario en Junaeb, sospecha que pueda ser catalogado como un Incidente de Seguridad de la Información deberá informar a la jefatura de su centro de responsabilidad, entregando los datos necesarios de la potencial falla de Seguridad de la Información.
b) El Jefe del centro de responsabilidad analizara los antecedentes, verificando si procede a un incidente de Seguridad de la Información o no. Clasificara, categorizara y generara las tareas y acciones de priorización de los trabajos requeridos para solucionar la problemática, dentro de su ámbito, lo que quedara plasmado a través del formulario de registro de incidente Anexo N°1, la cual será generada por el funcionario denunciante y el jefe del departamento donde se encuentra el incidente.
c) Si lo reportado por el funcionario corresponde a un incidente de Seguridad de la Información, el Jefe del Departamento deberá remitir información al CISO de la organización, a través de los medios destinados para ello (correo electrónico, memorando, etc.).
d) El CISO es responsable de activar el plan o procedimiento de gestión de incidentes de seguridad de la información, contactando a la persona que reporto el evento o incidente.
e) El CISO categoriza el evento según la matriz de riesgo y acciona los procesos de acciones preventivas y la gestión del incidente de seguridad.
f) El CISO es encargado de generar el formulario de resultado de gestión del incidente Anexo N°3 e informar a las áreas involucradas y a quien reporte el incidente.

DIRECCIÓN

g) El CISO es encargado de incorporar la información en la Planilla de tratamiento de incidente la información que contengan los anexos N°1, N°2 y N°3.

Hecha la recolección de información el CISO debe analizar los antecedentes, el resultado de dicho análisis puede ser uno de los siguientes:

a) El evento no corresponde a una amenaza: Se cierra el registro de eventos, informando a la persona que reporto
b) El evento corresponde a una debilidad: Se gestiona la actividad de mitigación (con los dueños de los activos comprometidos, el área o unidad de competencia y/o comité de Seguridad), dejando registro en la planilla de tratamiento de incidentes.
c) El evento ocurrió y debe ser gestionado como incidente: Se activa el proceso de Gestión de incidentes de Seguridad de la Información.

4.3.3 CANALES ALTERNATIVOS

En la ocasión que el punto de contacto o canal no se encuentre operativo o que exista alguna falla técnica u operativa para informar el hecho establecido, la persona deberá evaluar otros canales para advertir y notificar sobre lo observado:

- Correo electrónico.
- Llamado telefónico.
- Mensaje de texto.

4.4 GESTIÓN DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Una vez que el incidente es declarado como tal por el CISO, debe ser ejecutado el Proceso de Gestión de Incidente de Seguridad (Punto 4.3.1), el cual consta de los siguientes pasos.

4.4.1 ESCALAMIENTO

El CISO en conjunto con la jefatura del área correspondiente, determina si el tipo de tratamiento que el incidente debe tener es urgente, deberá proceder con la mayor celeridad posible. Si la urgencia lo amerita, se deberá informar al Jefe del Departamento de Informática o al Jefe del Servicio. Para esto se debe basar en la recopilación de información que contiene la Planilla de Tratamiento de Incidentes (Anexo N°4):

- Tipo de Incidente
- Nivel de criticidad
- Alcance del Incidente
- Que origino el incidente
- Cómo ocurrió (o está ocurriendo) el incidente

Cada vez que se registra un incidente de Seguridad de la Información, éste se reenviara a los responsables de ejecutar las acciones definidas en el tratamiento del incidente de Seguridad de la Información para su rápida solución y respuesta al mismo, según los plazos definidos para cada acción (Punto 4.2. Tiempo de respuesta a Incidente). En el caso de no poder ser resuelto se realizara un escalado interno. Para cada tipo de incidente se avisara a la persona correspondiente. El criterio principal del escalado es el de transferencia a una persona de soporte más elevado, que tiene:

- Mayor conocimiento o experiencia.
- Recursos para solucionar cuestiones más complejas o difíciles
- Mayor potestad o cargo para tomar decisiones

DIRECCIÓN

En general dependiendo del tipo de incidente los responsables de ejecutar la respuesta inmediata serán:

Tipo de Activo involucrado en el incidente	Jefatura responsable de la respuesta
Base de Datos	Departamento de Informática
Infraestructura TIC	
Sistema Informático	
Software Inventariado	
Documento	Departamento donde se desarrolla el proceso
Expediente	
Medios de almacenamiento personal asignado	
Adulteración de claves	
Infraestructura Física	Administración y Finanzas
Otros equipos	
Persona	Departamento de Personas

4.4.2 RESPUESTA INMEDIATA

En esta etapa el CISO debe entregar lineamientos para la respuesta ante un incidente, para que la jefatura designada para la respuesta inmediata del Incidente sea responsable del desarrollo de las acciones inmediatas:

Acción Inmediata	Descripción
Contener el daño y minimizar el riesgo	Evitar que se propaguen los daños o efectos del incidente, coordinado las actividades necesarias para su disminución, probabilidad y consecuencia
Reclasificar el incidente si fuera necesario	Reclasificar según 4.2.1, 4.2.2, 4.2.3, 4.2.4 y 4.2.5
Protección de evidencias	Resguardar las evidencias recopiladas durante la gestión del mismo.
Notificación a los organismos externos	Cuando sea necesario notificar a organismos externos como por ejemplo (carabineros, PDI, Bomberos, etc.), esto debe ser canalizado a través del área Jurídica de la organización.
Recuperación de los sistemas	Contactar al administrador del o los sistemas a fin de gestionar la recuperación de estos.
Compilación y organización de la documentación del incidente	Recopilar todos los antecedentes relacionados con el incidente

4.4.3 PROCESO DISCIPLINARIO

Si el incidente es de mayor gravedad o se prevé el involucramiento de algún delito, el responsable de la respuesta inmediata, asesorándose por el integrante de la División jurídica designado para las materias de seguridad de Información, informara al Jefe superior del servicio y, de precisarse, a carabineros, bomberos, ambulancia, Ministerio Publico, PDI, etc., según lo requerido.
En el caso que existan eventuales responsabilidades administrativas, y dependiendo de la gravedad del incidente el Responsable de la respuesta inmediata solicitará a quien corresponda la instrucción de un procedimiento disciplinario o anotación de demerito en los términos establecido en el Estatuto Administrativo.
Cuando el incidente involucre a personal contratado a honorarios o terceros, se evaluará solicitar el término anticipado del contrato o, en caso que exista, la aplicación de la sanción que establezca el propio contrato, Política General de Seguridad de la Información u otras políticas ministeriales para el incidente detectado.

4.4.4 CONTINUIDAD DEL NEGOCIO

En el caso que el incidente no pueda ser controlado y ponga en riesgo las operaciones, entrega de productos y entrega de beneficios de Junaeb, el Comité de Seguridad de la Información más los dueños del proceso, evaluaran la activación de los procesos de continuidad de negocio.

4.4.5 RECOLECCIÓN DE EVIDENCIA

La recolección de la evidencia es responsabilidad del CISO, ésta debe ser clara y suficiente. Para ello se deberá:

Documentos en papel: El original se guarda de manera segura con un registro del individuo que encontró el documento. Dónde y cuándo fue encontrado el documento, y quién fue testigo del descubrimiento. En cualquier investigación se debe asegurar que los originales no son alterados;

Información sobre medios computacional es: Las imágenes o copias espejo (dependiendo de los requisitos aplicables) de cualquier medio removible, información en discos duros o en memorias, deben ser retenidas para asegurar su disponibilidad. El registro de todas las acciones durante el proceso de copiado se debería guardar y el proceso se debería efectuar ante testigos. Los medios originales y el registro (si esto no es posible, por lo menos una imagen espejo o copia) se deben guardar de manera segura e intactos (so utilizan mecanismos de protección e incluso encriptación para que nadie adultere la evidencia).

Cualquier trabajo forense se debe realizar sólo sobre copias del material de evidencia. Se debe supervisar y registrar cuándo y dónde fue ejecutado el proceso de copiado, quién realizó las actividades de copiado y qué herramientas y programas se han utilizado.

Esta evidencia es entregada al Comité de Seguridad de la Información para la evaluación de procesos disciplinaros.

4.4.6 COMUNICACIÓN

- Una vez contenido el incidente, el CISO debe informar a los involucrados en el incidente.
- Una vez al mes el CISO debe Difundir la planilla de tratamiento de incidentes con el Comité de Seguridad de la Información y los jefes de los departamentos de Administración y Finanzas, Informática, Gestión de Personas y Secretario General. Esto se realizará a contar del mes de marzo de 2018 que es la fecha de entrada en vigencia del presente procedimiento, esto debido a que se debe realizar una capacitación a los funcionarios y trabajadores durante los meses de diciembre 2017 a febrero 2018 respecto de este procedimiento.

4.4.7 ANÁLISIS DE CAUSA Y CIERRE DEL INCIDENTE

En esta etapa el CISO debe:

- Realizar un análisis de las causas del incidente.
- Cuando el incidente no esté cerrado, seleccionar e implementar un plan de acción adecuado, además de definir el plazo para su implementación
- Registrar el cierre del incidente en la planilla de tratamientos de incidentes.
- Una vez cerrado el incidente generar el informe de incidentes de seguridad.

4.4.8 APRENDER DE LOS INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

A lo menos una vez al año el Encargado de seguridad de la Información, debe revisar los incidentes de la seguridad del periodo analizado.

- Posibles tendencias.
- Eficacia de los tratamientos implementados.
- Cuantificación de los tipos, volúmenes y costos de los incidentes de seguridad.
- Incidentes recurrentes o de alto impacto.
- Problemas subyacentes.
- Necesidades de mejorar o implementación de nuevos controles para limitar la frecuencia, daño y costo de futuras ocurrencias.

Con los antecedentes aportados por esta revisión, el CISO debe proponer al Comité de Seguridad de la Información medidas que sean necesarias para que no vuelvan a ocurrir, además de detectar y promover

DIRECCIÓN

los aprendizajes de cada uno de ellos.

5 DIFUSIÓN

El procedimiento de gestión de incidentes, se comunica y difunde a todo el personal de la institución, informando de su publicación en la intranet institucional, lo cual permite su libre consulta a todo el personal de JUNAEB. El acceso a la intranet institucional es a través de su login y password personal.

6. REVISIÓN

El Encargado de Seguridad de la Información, efectuará una revisión de este documento al menos una vez cada 3 años desde su entrada en vigencia. Sin perjuicio de lo anterior, el documento puede ser evaluado y/o actualizado en cualquier momento, dependiendo de la necesidad de la organización por seguridad de la información.

7 VIGENCIA

El encargado de Seguridad de la Información, efectuará una revisión de este documento al menos una vez cada 3 años desde su entrada en vigencia. Sin perjuicio de lo anterior, el documento puede ser evaluado y/o actualizado en cualquier momento, dependiendo de la necesidad de la organización por seguridad de la información.

8 REGISTROS

REGISTRO 1. FORMULARIO DE REGISTRO DE INCIDENTES

FORMATO REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			Versión: x.x Fecha: xx/xx/xxxx Responsable:
INFORMACIÓN GENERAL DEL REPORTE			
Fecha y hora del reporte:			
Nombre de quien reporta:			
Cargo:		Dependencia y Extensión:	
Sede:		E-mail	

INFORMACIÓN GENERAL DEL INCIDENTE	
Fecha y hora del incidente:	
Lugar o sede del incidente:	
No. de Solicitud:	
Descripción del	

RECURSO INFORMÁTICO AFECTADO
Nombre del Recurso:
Ubicación Física:
Información que contiene:
Fecha de la última copia de seguridad:

Fuente propia Departamento de informática

DIRECCIÓN

REGISTRO 2. FORMULARIO DE VALORACIÓN DE INCIDENTES

FORMATO VALORACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión: x.x. Fecha: xx/xx/xxxx Responsable:
INFORMACIÓN GENERAL DEL INCIDENTE	
Fecha y hora del reporte:	
No. de solicitud:	
Descripción del Incidente	

INFORMACIÓN DE VALORACIÓN DE INCIDENTE	
Fecha y hora de valoración:	
Nombre de quien valora:	
Valoración del incidente:	
Observaciones de la valoración:	

Fuente propia Departamento de informática

DIRECCIÓN

REGISTRO 3. FORMULARIO DE RESULTADO DE GESTIÓN DEL INCIDENTE

REPORTE DEL RESULTADO DE LA INVESTIGACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión: x.x Fecha: xx/xx/xxxx Responsable:
Objetivo:	
Alcance:	El resultado reflejado en este documento solo debe ser conocido por las personas autorizadas

INFORMACIÓN GENERAL DEL INCIDENTE	
Fecha y hora del reporte:	
No. de solicitud:	
Descripción del Incidente	

INFORMACIÓN DE VALORACIÓN DE INCIDENTE	
Fecha y hora de valoración:	
Nombre de quien valora:	
Valoración del incidente:	

INFORMACIÓN EQUIPO INVESTIGADOR		
NOMBRE	**CARGO**	**E-Mail**

CAUSAS

PASOS EJECUTADOS EN LA INVESTIGACIÓN

OPORTUNIDADES DE MEJORA

No.	DESCRIPCIÓN	RESPOSABLE	FECHA DE FINALIZACIÓN

CONCLUSIONES

ANEXOS

Fuente propia Departamento de informática

DIRECCIÓN

REGISTRO 4. PLANILLA DE TRATAMIENTO DE INCIDENTES

Estado	N°	Origen	Fecha Reporte	Hora Reporte	Identificación de quien reporta	Activos / Sistemas Afectados	Corresponde a Incidente o Debilidad	Tipo de Incidente (NI o I) NI = No Informático	Nivel de criticidad	Descripción del Incidente

Fuente propia Departamento de informática

Responsable de la Acción	Acción Inmediata	Fecha de Acción Inmediata	Hora de Acción Inmediata	Se Activa Continuidad del negocio (S/N)	Registro de Evidencias	Acciones Correctivas / Preventivas	Costo Asociado	Respuesta Cierre	Fecha Cierre

Fuente propia Departamento de informática

Donde:

Estado	Estado inicial (Abierto, Acciones Inmediatas, Acciones	Responsable de	Responsable de la acción inmediata
N°	Numero de evento o incidente	Acción	Descripción de las acciones inmediatas realizadas para
Origen	Origen del evento o Incidente	Fecha de Acción	Registro de la fecha en que se realizo la acción inmediata
Fecha Reporte	Fecha en que es reportado evento o Incidente	Hora de Acción	Registro de la hora en que se realizo la acción inmediata
Hora Reporte	Hora en que es reportado evento o Incidente	Se Activa Continuidad	Indicar si se activa la continuidad del negocio
Identificación de quien reporta	Datos de la persona que reporta (nombre, cargo, centro de responsabilidad y datos de contacto)	Registro de Evidencias	Identificación de los registros y evidencias que respaldan el proceso disciplinario
Activos / Sistemas Afectados	Descripción de los activos o sistemas afectados (N° de inventario, serie, marca, tipo, etc.)	Análisis de Causa	Registrar las causas de raíz que produjeron el incidente
Corresponde a Incidente o Debilidad	Indicar si corresponde a un Incidente o Debilidad	Acciones Correctivas / Preventivas	Acciones correctivas o preventivas realizadas para eliminar las causas de raíz del incidente
Tipo de Incidente (NI o I) NI = No Informático	Indicar el tipo de incidente (NI= No Informático, I= Informático)	Costo Asociado	Costo asociado al incidente
Nivel de criticidad	Registrar el nivel de criticidad según la urgencia, criticidad	Respuesta	Resumen de las actividades de cierre del incidente y
Descripción del Incidente	Descripción del Incidente	Fecha Cierre	Fecha de cierre

Fuente propia Departamento de informática

9 CONTROL DE CAMBIOS

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES				
Nº Revisión	**Fecha Aprobación**	**Motivo de la revisión**	**Páginas Modificadas**	**Autor**
00	15/11/2017	Elaboración inicial	No aplica	Departamento de Informática

DIRECCIÓN