GOBIERNO DE CHILE
JUNTA NACIONAL DE AUXILIO
ESCOLAR Y BECAS

JUNAEB
DN
11 DIC 2017
OFICINA
DE
PARTES

APRUEBA POLÍTICA DE INVENTARIOS Y PROCEDIMIENTO DE INVENTARIO DE SEGURIDAD DE LA INFORMACIÓN, AMBAS DEL DEPARTAMENTO DE GESTIÓN, CONTROL DE GESTIÓN Y ESTUDIOS, QUE ESTABLECEN OBJETIVOS, DIRECTRICES, CONCEPTOS Y DEBERES QUE SEÑALAN.

RESOLUCION EXENTA Nº 3.006

SANTIAGO, 08 de octubre del 2017

VISTOS:

Lo dispuesto en el artículo 7° de la Constitución Política de la República; en el DFL N° 1/19.653, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado; en la ley N° 19.880, que Establece las Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado, en la ley N° 20.981 de presupuestos del sector público para el año 2017, en la Ley N° 15.720, que crea la Junta Nacional de Auxilio Escolar y Becas; en el Decreto Supremo N° 5.311 de 1968 del Ministerio de Educación, que fija Reglamento General de la Junta Nacional de Auxilio Escolar y Becas; en el Decreto Ley N° 180, de 1973, que declara en receso al Consejo de JUNAEB cuyas facultades otorga a su Secretario General, en el Decreto Exento N° 1106 de 11 de noviembre de 2016 del Ministerio de Educación, en la Resolución N° 1.600 de 2008 de Contraloría General de la República, que fija normas de exención del trámite de Toma de Razón;

DIRECCIÓN

CONSIDERANDO:

1.- Que, la Junta Nacional de Auxilio Escolar y Becas, es una corporación autónoma de derecho público que tiene como misión la aplicación de medidas coordinadas de asistencia social y económica a los escolares, conducentes a hacer efectiva la igualdad de oportunidades ante la educación, de conformidad a lo establecido en el artículo 1° de la ley N° 15.720;

2.- Que, para el cumplimiento de sus objetivos institucionales, el Departamento de Planificación, Control y Gestión de Estudios de la Dirección Nacional de JUNAEB, requirió confeccionar tanto una Política de Inventarios como un Procedimiento de inventario de Seguridad de la Información que cumplieran con las condiciones adecuadas para su funcionamiento, en relación al resguardo de la seguridad de los funcionarios, seguridad de la información, mejora en la calidad de los procesos y una mayor integración entre los distintos equipos de la institución.

3.- Que, las entidades regidas por el Decreto N°83 del año 2004, del Ministerio Secretaria General de la Presidencia, entre los cuales se encuentra comprendida la Junta Nacional de Auxilio Escolar y Becas "JUNAEB", deben adoptar Políticas de seguridad permanentes que incluyan planes de contingencia frente a incidentes de toda índole que pudieran poner en riesgo la continuidad operacional de los sistemas de información institucionales;

4.- Que, la necesidad de que la institución gestione adecuadamente la Seguridad de la Información, tiene como objetivo principal, mejorar los niveles de protección de los activos de información relevantes que dan sustento a los procesos de provisión y soportes.

5.- Que, la norma técnica aprobada mediante decreto N°83 del 2004, del Ministerio Secretaría General de la Presidencia, establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los órganos de Administración del Estado.

6.- Que, las exigencias y recomendaciones previstas en dicha norma, tienen por finalidad; a) garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de los documentos electrónicos ;b) facilitar la comunicación electrónica con y entre los órganos de la Administración del Estado, la ciudadanía y el sector público en general; c) salvaguardar el uso de documentos electrónicos de manera segura, confiable y con pleno respeto a la normativa vigente sobre confidencialidad de la información intercambiada.

7.- Que, los activos asociados a la información y a las instalaciones de procesamiento de la información deben ser; a) identificados; b) inventariados -el inventario de activos debe ser exacto, actualizado, consistente y alineado con otros inventarios-, c) mantenidos o custodiados por un determinado espacio de tiempo.

8.- Que, en el proceso de identificación de los activos estos deben ser clasificados en cuanto a su **estado** en el ciclo de vida de la información – ya sea creación, transformación, almacenamiento, transporte, eliminación y/o la destrucción-; y en cuanto a su **relevancia**, la que dependerá de la confidencialidad, integridad, disponibilidad y criticidad entre otros factores a considerar. En consecuencia:

RESUELVO:

ARTÍCULO PRIMERO.– APRUÉBASE, Política de Inventarios y Procedimiento de Inventario de Seguridad de la Información, ambos textos del Departamento de Planificación, Control de Gestión y Estudios, los que establecen sus objetivos, directrices, conceptos, deberes y medidas, aplicables y obligatorios para todos los funcionarios institucionales y, cuyos textos se exponen a continuación:

DIRECCIÓN

POLITICA DE INVENTARIOS

JUNAEB

DIRECCIÓN

1. OBJETIVO GENERAL

El objetivo del presente documento es entregar directrices generales para JUNAEB de los siguientes controles del sistema de la seguridad de la información:

- A 08.01.01 "Inventarios de Activos"
- A 08.01.02 "Propiedad de Activos"
- A 08.01.03 "Uso Aceptable de los Activos"
- A 08.01.04 "Devolución de Activos"

2. ALCANCE

La presente Política aplica a todo personal contratado en calidad jurídica de planta, contrata y honorario de la Dirección Nacional de JUNAEB que administran y manejan activos de información, mediante inventario, producto de sus contratos o convenios, de acuerdo a las responsabilidades inherentes a sus cargos.

3. MARCO JURIDICO

- Ley N° 20.285 de 2008, Sobre Acceso a la Información Pública.
- Ley N°20.730 de 2014, que Regula el Lobby y las Gestiones que representen intereses particulares ante las autoridades y funcionario/as.
- Ley N° 18.834 de 2005, sobre Estatuto Administrativo.
- Ley N° 19.880 de 2004, que Establece Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado.
- Decreto N° 250 del 2004 del Ministerio de Hacienda, que Aprueba Reglamento de la Ley N°19.886 de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios.
- Decreto Supremo Nº 83 del 2004, que Aprueba la Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
- Ley N° 19.886 de 2003, Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios.
- Ley N° 19.628 de 1999, sobre Protección de la Vida Privada.
- Ley N° 18.575 de 1986, Orgánica Constitucional de Bases Generales de la Administración del Estado.

4. ROLES Y RESPONSABILIDADES

Roles	Responsabilidades
Comité Seguridad de la Información	• Proponer mejoras y/o actualización de la Política. • Informar a la Dirección en caso de ocurrencia de incumplimientos a esta Política que afecten a la Institución.
Encargado/a Seguridad de la Información	• Verificar y monitorear la ejecución de la Política
Jefaturas de departamentos, unidades y funcionarios	• Conocer y cumplir con esta Política. • Alertar los incumplimientos a las directrices emanadas de esta Política. • Implementar medidas preventivas y/o correctivas que mitiguen o eliminen posibles riesgos.

5. POLÍTICA

5.1 Directrices generales para inventarios de productos y bienes

Cualquier tipo de inventario de la Dirección Nacional JUNAEB debe considerar – como mínimo- los siguientes puntos:

a) Mantener los inventarios mediante una administración y control eficiente, describiendo su metodología en un procedimiento pertinente a cargo del departamento responsable.
b) Realizar y/o actualizar el inventario a lo menos una vez al año.
c) Mantener un nivel adecuado de inventarios, para asegurar la continuidad de procesos y tareas de los departamentos, unidades y áreas de JUNAEB, Dirección Nacional.
d) Satisfacer rápidamente la demanda, mediante monitoreo de las necesidades en conjunto y a las solicitudes directas que realicen de su necesidad
e) Establecer bodegas o lugares de almacenaje limpios y ordenados (según leyes y normativas correspondientes), las cuales deben ser restringidas a solo personal autorizado.
f) Se exceptúan los puntos b, c, d, y e para *el Inventario De Activos De Seguridad De La Información*

5.2 Inventario de activos de seguridad de la información[1]

Se denomina *activo de información* a todo aquello que las entidades u organismos consideran importante o de alta validez para la misma, por contener o procesar información, como lo pueden ser bases de datos, contraseñas, números de cuentas, etc. de manera que un "activo" de información es aquel elemento que contiene o manipula información.

Como *inventario de seguridad de la información*, JUNAEB entenderá un catastro (o listado) de los principales *activos de información* que sean significativos, agrupando aquellos que, por ser similares, tiene sentido hacerlo. La finalidad de este inventario de activos de seguridad no es para la administración común de un inventario, sino que busca establecer la necesidad de protección o resguardo de éste, para prevenir riesgos en términos de divulgación, accesibilidad y confidencialidad (por ejemplo: pérdida de información, deterioro del activo, etc.)

El levantamiento y actualización de este listado, se realizará en base al procedimiento de inventario de seguridad de la información.

5.3 Propiedad de los activos[2] de información

Cada uno de los activos que se identifican en el catastro de activo de información[3], cuentan con un responsable, que es su propietario administrativo (ya que el dueño legal es JUNAEB, derecho de propiedad intelectual). Esta persona se deberá mantener la seguridad del activo y su administración durante el ciclo de vida del activo.

El propietario administrativo debe decidir quién accederá y quién no a la información mientras es elaborada o procesada, si estima necesario podrá aplicar alguna medida de seguridad adicional y es responsable de responder por los daños o pérdida de información e integridad[4]. Respecto de esto último, el propietario administrativo debe asegurarse del manejo adecuado del activo cuando se decide derivar a bodegas, eliminarlo o destruirlo[5].

5.4 Usuarios Externos:

Los usuarios externos que usan o que tengan acceso a los activos de información, instalaciones y/o recursos de procesamiento de la información de JUNAEB, deben tomar conciencia de los requisitos

[1] Control A 08.01.01 norma ISO27.001
[2] Control A 08.01.02 norma ISO 27.001
[3] sinónimo de Inventario de Activos de Información
[4] Distorsiones o modificaciones sin autorización
5 Se debe destruir o eliminar el activo según procedimiento de expurgo y normativas respectivas para instituciones publicas

DIRECCIÓN

de seguridad que se establecen para ellos y que JUNAEB los acuerda, declara y difunde en los respectivos contratos, anexos, convenios, y/o descargo de responsabilidad (disclaimer).

Además, son responsables de cualquier recurso de procesamiento de la información y cualquier uso desarrollado en el transcurso de su servicio, o posterior a él, según indica la Ley N° 19.628.

5.5 Uso aceptable de los activos[6] de información

- Los funcionarios de JUNAEB independiente de la calidad jurídica de contratación, deberán usar los recursos de la institución en forma responsable.
- Todos los funcionarios de JUNAEB independiente de la calidad jurídica de contratación, deben tomar las medidas necesarias para prevenir el acceso no autorizado a la información y se obligan, a guardar, respetar y hacer respetar el carácter de confidencial de toda la documentación, listados, archivos, sistemas, procesos, información y datos recibidos en razón de su trabajo. Como también extremar cuidados al copiar o de cualquier manera reproducir, comunicar, revelar, sea en forma total o parcial los archivos y demás Información que hubieran recibido por dichos motivos.
- Toda la información que contenga datos personales de Estudiantes (postulantes y beneficiarios de programas JUNAEB) se considera confidencial y reservado, la transferencia de dichos datos deberá realizarse en el marco del procedimiento de trasmisión de base de datos de carácter personal.

5.6 Manipulación de los activos de información

- Los Activos de Información Confidenciales o Reservados, deben ser manipulados con extremos cuidados y en base a la Ley N° 20.285 y Ley N° 19.628.
- De esta forma, ante una consulta, JUNAEB no está facultada para revelar los datos personales y sensibles de los que tome conocimiento. Es decir, se debe proteger la información (o activo de información) que contenga los datos personales y sensibles sobre: estudiantes beneficiarios, proveedores, contratistas, funcionarios, etc.
- Sin embargo, se considera "Público" toda información que no identifica a una persona en particular.
- Para que una información pase de "reservada" a "pública" y ésta pueda ser difundida o divulgada a un tercero o externo, debe ser tratada, borrando (o tachando o engreciendo, etc.) los datos sensibles y personales que puedan identificar al titular.
- También es información pública los resultados (o la información resultante) que se entregue en forma aglomerada, es decir, con carácter estadístico.
- Por último, es publica la información que se difunde en Banner de Gobierno Transparente y según lo solicite la Ley N° 20.285

5.7 Uso general de activos digitales

- El uso de Internet debe ser primordialmente para actividades relacionadas con las funciones laborales.
- Los usuarios autorizados son responsables de la seguridad de sus password y sus cuentas. Las cuentas son personales e intransferibles, según lo señalado en el procedimiento de inicio de sesión seguro y el sistema de gestión de contraseñas.
- Todos los funcionarios de JUNAEB, deben tener extrema precaución al abrir archivos adjuntos que se reciban de anónimos, los que pueden contener código malicioso.
- Sólo personal autorizado (Departamento de Informática) podrán monitorear estaciones de trabajo y tráfico de la red.
- Todos los trabajadores de JUNAEB independiente de la calidad jurídica de contratación, deberán respaldar información crítica, almacenándolas en un lugar seguro, definido por el Departamento de Informática.

5.8 Uso general de activos en papel

- Realizar acorde a la Política de protección de los registros en papel, quien debe tratar los activos de información que allí se contengan según lo estipula la Ley N° 20.285.

[6] Control A 08.01.03 norma ISO 27.001

DIRECCIÓN

5.9 Uso de no aceptado

Los funcionarios, independiente de la calidad jurídica de contratación, deben asumir estas restricciones durante el curso de las responsabilidades de su trabajo[7].

- La instalación o distribución de software, deberá estar en el marco de lo declarado en el procedimiento de instalación del software en sistemas operacionales.
- En general cualquier otra actividad que sea contraria a la ley, la moral y las buenas costumbres, que afecten la confidencialidad de la información, que afecte derechos de terceros, y también aquellas actividades que no guarden relación con las labores encomendadas dentro del ámbito de su trabajo.

5.10 Almacenamiento de los activos

- Los activos de información de carácter informáticos (discos duros, pc, laptop, etc.) son inventariados y mantenidos en bodegas por el Departamento de Informática.
- Una vez asignados; su cuidado y la información contenida en su interior es responsabilidad del funcionario al cual es asignado el equipo.
- Sin embargo, en caso de ser un "respaldo "o estar en "desuso", éste es de responsabilidad del Depto. de Informática.

5.11 Devolución de los activos

Se realizará en el marco de lo señalado en el procedimiento de Devolución de activos.

5.12 Destrucción de los activos

- Activos papel original con información confidencial deben ser expurgados (triturados o incinerados), de acuerdo al "Procedimiento de Expurgo".
- Copias de papel, de la JUNAEB Dirección Nacional deben ser depositados en las cajas de Fundación San José quien destruye los papeles, mediante tratamiento de reciclaje para pañales. Si no son depositados en estas cajas, deben ser destruidos (tachados, ilegibles y/o cortados) para asegurarse que la información no se divulgue.
- Otros Activos con información confidencial (discos duros, tarjetas TNE, cd, etc.) deben ser expurgados, según indiquen los procedimientos e instructivos de trabajo correspondientes.

5.13 Acciones disciplinarias

Infracciones a la Seguridad de la Información podrán ser sancionadas en conformidad a lo dispuesto en la Ley N° 18.834, sobre Estatuto Administrativo. Por su parte, el artículo 4 de la Ley 19.223, dispone que: "El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio". Y en el inciso primero del artículo 23 de la Ley 19.628 señala que: "La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin prejuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal"

6. REVISIÓN

El presente documento estará sujeto a revisión a lo menos una vez cada 3 años. No obstante, podrá ser actualizado en cualquier momento, dependiendo las necesidades de la institución.

7. DIFUSIÓN

La presente Política, una vez aprobada, estará publicada en la intranet Institucional para conocimiento y consulta de todo el personal de la JUNAEB independiente de la calidad jurídica de contratación, su accedo se realiza mediante login y password de usuario.

[7] La siguiente lista si bien no es exhaustiva, permite proveer de un marco regulatorio de las actividades que caen en la categoría de no aceptables

DIRECCIÓN

8. VIGENCIA

Esta Política entrará en vigencia una vez que sea aprobada y difundida por la Institución a través de la publicación en la intranet, y estará sujeta a las revisiones, de acuerdo al punto 6 mencionado anteriormente.
Todos los funcionarios de la JUNAEB, independiente de la calidad jurídica de contratación, tienen la responsabilidad de conocer la presente Política y cumplir lo que en ella se indica.

9. CONTROL DE CAMBIOS

Nº Revisión	Cambio	Fecha	Aprobado por:
00	Creación de la Política de Inventario	08/11/17	Director Nacional

PROCEDIMIENTO DE INVENTARIO DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

El objetivo del presente documento es describir la metodología con la cual se levanta o actualiza el Inventario de Seguridad de la Información de JUNAEB.

2. AMBITO DE APLICACIÓN

El procedimiento será aplicado en el nivel central por el Departamento de Planificación, Control de Gestión y Estudios, abarcando los procesos de provisión de bienes y servicios de la Institución, indicados en el alcance del PMG de Seguridad de la Información vigente, que es informado a los servicios revisores pertinentes[8] cuando éstos lo soliciten o cuando se estime conveniente en caso de cambio en el alcance del PMG.

3. RESPONSABILIDADES

Roles	Responsabilidades
Encargado de Seguridad de la Información	– Informar el inventario de seguridad de la información a los servicios que miden cumplimiento de PMG SSI, aplicando el presente documento.
Jefe de Deptos. y Unidad de la Dirección Nacional	– Colaborar con el levantamiento de inventario de seguridad de la información, proporcionando información fidedigna y actualizada según requerimiento del DEPLACGE. – Informar las alertas al personal a cargo. – Reportar al sistema de Gestión de Incidentes y poner en inicio el proceso de respuesta, planes de contingencia o planes de recuperación, etc.
Profesionales de la Unidad de Planificación, DEPLACGE	– Apoyar las gestiones del encargado de seguridad de la información en el levantamiento de sus activos e información asociada.

4. DEFINICIONES

Inventario de seguridad de la información: Se entenderá como inventario de seguridad de la información a un catastro (o listado) de los principales activos de información que sean significativos, agrupando aquellos que, por ser similares, tiene sentido hacerlo. La finalidad de este inventario de activos de seguridad no es para la administración común de un inventario, sino que busca establecer la necesidad de protección o resguardo de éste, para prevenir riesgos en términos de divulgación, accesibilidad y confidencialidad (por ejemplo: pérdida de información, deterioro del activo, etc.).

Activo de información: Se denomina activo de información a todo aquello que las entidades u organismos consideran importante o de alta validez para la misma, por contener o procesar información, como lo pueden ser bases de datos, contraseñas, números de cuentas, etc. de manera que un "activo" de información es aquel elemento que contiene o manipula información.

Integridad: Los activos de información se encuentran completos, actualizados y son veraces, sin modificaciones inapropiadas o corruptas.

[8] Servicios que miden cumplimiento de PMG SSI

Confidencialidad: Los activos de información se encuentran protegidos de personas/usuarios no autorizados.

Disponibilidad: Los usuarios autorizados pueden acceder a los activos de información cuando lo requieran, para utilizarlos apropiadamente al desempeñar sus funciones.

PMG: Programa de Mejoramiento a la Gestión.

SSI: Sistema de Seguridad de la Información.

DEPLACGE: Departamento de Planificación, Control de Gestión y Estudios.

5. DESCRIPCIÓN DE ACTIVIDADES

El DEPLACGE, levantará el Inventario de Seguridad cada 3 años o –en su defecto- su actualización- con el fin de identificar los activos asociados al PMG de Seguridad de la Información; coordinando a los diferentes departamentos y/o unidades de JUNAEB que se encuentren dentro de su alcance. Para ello, se utiliza el instrumento "Hoja de Inventario" Excel, entregado a los Servicios Públicos en el año 2015 por DIPRES,[9] (ver punto 6)

La completitud de la hoja de Excel se llenará en base a lo siguiente:

5.1 Hoja "Inventario".

Esta hoja del libro Excel, tiene por objetivo recoger el conjunto de los activos de información asociados a los procesos de provisión de bienes y servicios de la institución, cuyos productos estratégicos se encuentran en la Ficha A1, donde se deben considerar todos los activos de información de los procesos.

El inventario organiza los atributos de los activos en las tres secciones que se describen a continuación:

1) Descripción de procesos;

Esta sección contiene 3 campos que permite caracterizar el o los procesos del alcance en los que el activo participa	
Proceso	Corresponde al nombre del proceso de negocio (de provisión de productos/servicios estratégicos) al cual pertenecen los activos de información a incluir en el inventario. Estos procesos deben ser consistentes con los mencionados en el Oficio de alcance que se entrega a los servicios que miden cumplimiento de PMG SSI.
Subproceso	Son aquellos subprocesos en los que puede estar dividido el proceso transversal mencionado en la columna anterior, dependiendo de la complejidad del mismo.
Etapa relevante	Detalle de las fases más importantes que se deben desarrollar en cada subproceso para dar origen a los productos.

2) Identificación de los activos de información;

Esta sección contiene 12 campos que permite caracterizar la naturaleza de cada activo y sus condiciones de preservación y manejo, que servirán de insumo para el posterior análisis.	
Nombre Activo	En este campo debe incluirse todos los activos de información identificados para la etapa, independiente de su medio de soporte y sus características. Esta columna se encuentra destacada con azul, pues es una de las que dan consistencia entre esta hoja y la siguiente. Es importante señalar que, se debe evitar repetir el mismo activo en diferentes líneas.

[9] Se modificó hoja "Análisis de Riesgo" eliminando columna llamada "*producto esperado*". Además se excluyó hojas "Plan General" y "Implementación" por considerarse no pertinente a este procedimiento.

DIRECCIÓN

Identificador o código	En este campo se debe incluir el código dado por la institución al activo (nuevo o preexistente). Este atributo debe permitir identificar en forma única al activo.
Tipo	Este atributo permite establecer la naturaleza del activo, donde se deberá seleccionar (lista desplegable) la clasificación del activo, según los siguientes valores: – "Base de Datos": Es la información sistematizada y organizada. – "Documento": Corresponde a un escrito que refleja el resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella, pudiendo ser físico o electrónico – "Equipo": Objetos o dispositivos que realizan o apoyan la realización de un proceso y contienen información. A este tipo no le aplica los siguientes atributos: Soporte y Persona Autorizada para Copiar. – "Expediente": Conjunto de documentos y formularios dispuestos en estricto orden de ocurrencia, de ingreso o egreso. Este puede ser físico o electrónico, en cuyo caso la definición está dada por el DS 81: "Documento electrónico compuesto por una serie ordenada de actos y documentos representados en formato electrónico, dispuestos en estricto orden de ocurrencia, de ingreso o egreso en aquél, y que corresponde a un procedimiento administrativo o asunto determinado". – "Formulario": Corresponde a documentos utilizados para recoger información, pudiendo ser físico o electrónico. – "Infraestructura Física": Estructura que permite almacenar y/o custodiar activos de información del proceso, tales como: datacenter, oficinas de partes, bodegas, caja fuerte, etc. A este tipo no le aplica los siguientes atributos: Soporte, Persona Autorizada para Copiar, Medio de Almacenamiento, Tiempo de Retención, Disposición y Criterio de Búsqueda. – "Persona": personal de la institución que participa en un proceso de provisión. A este tipo no le aplica los siguientes atributos: Soporte, Persona Autorizada para Manipular, Persona Autorizada para Copiar, Medio de Almacenamiento, Tiempo de Retención, Disposición y Criterio de Búsqueda. – "Sistema": Programa computacional desarrollado a medida, por la institución o por un externo, cuyo objetivo es apoyar un proceso de negocio. – "Software": Programa computacional licenciado, producido por una empresa externa que lo distribuye o comercializa.
Ubicación	Corresponde al lugar físico o lógico donde se encuentra el activo mientras es utilizado en el proceso, esta descripción debe ser lo suficientemente detallada como para determinar a partir de esta información las condiciones de seguridad física en las que se encuentra el activo.
Responsable/ dueño	Corresponde al rol o cargo de la persona autorizada para tomar decisiones respecto del activo. Esto no implica necesariamente derecho de propiedad sobre el activo.
Soporte	Corresponde al medio en el cual se encuentra el activo, este puede ser en papel o digital. Esta característica no aplica a los activos de tipo "Persona", "Infraestructura física" ni "Equipo".
Persona Autorizada para Manipular	Corresponde al rol o cargo de la(s) persona(s) autorizada(s) para usar el activo de información, ya sea modificándolo, actualizándolo, trasladándolo o limpiándolo.
Persona autorizada para copiar (opcional)	Corresponde al rol o cargo de la(s) persona(s) autorizada para copiar el activo (aplicable al activo de información en papel y copias en medios magnéticos). Este campo es opcional (se puede omitir), y sirve cuando se quiere lograr una caracterización más en profundidad.
Medio de almacenamiento (opcional)	Descripción de la forma de guardar el activo durante el tiempo de retención. Este campo es opcional (se puede omitir), y sirve cuando se quiere lograr una caracterización más en profundidad.

Tiempo de retención (opcional)	Corresponde al tiempo en el cual el activo de información debe ser mantenido por la Institución en el medio de almacenamiento. Este campo es opcional (se puede omitir), y sirve cuando se quiere lograr una caracterización más en profundidad.
Disposición (opcional)	Corresponde al destino que se le da al activo de información una vez transcurrido el tiempo de retención. Este campo es opcional (se puede omitir), y sirve cuando se quiere lograr una caracterización más en profundidad.
Criterio de Búsqueda (opcional)	Forma en la cual se debiera buscar el activo de información. Corresponde al criterio de ordenamiento o indexación definido por la institución para el activo, que permite un acceso rápido y eficiente. Este campo es opcional (se puede omitir), y sirve cuando se quiere lograr una caracterización más en profundidad.

3) **Análisis de criticidad**;

El atributo de criticidad, está compuesta por cuatro campos que permitirá establecer una priorización de los activos del inventario, en función de los requerimientos de confidencialidad, integridad y disponibilidad, cuyos valores consideran la caracterización previamente realizada para cada activo.

Confidencialidad

Necesidad de permitir el acceso al activo solo a las personas debidamente autorizadas de acuerdo a lo definido por la institución. El acceso no autorizado tiene impacto para la institución o terceros. Para establecer este atributo, se debe considerar las leyes N°20.285, y N°19.628, así como también, la etapa del proceso en la cual se realiza el análisis del activo. En este campo, se debe clasificar en uno de los siguientes grados:

Grado	Definición
Pública	El activo no tiene restricciones de acceso
Reservada	Activo de información cuyo acceso no autorizado tiene impacto para la institución o terceros.

Integridad

Necesidad de preservar la configuración y contenido de un activo de Información. Su modificación no deseada tiene consecuencias que generan distintos niveles de impacto para la institución o terceros. El valor de este atributo está directamente relacionado con la magnitud de dicho impacto. En este campo, se debe clasificar en uno de los siguientes grados:

Grado	Definición
Baja	Activo de Información cuya modificación no deseada tiene consecuencias con impacto leve para la institución o terceros.
Media	Activo de Información cuya modificación no deseada tiene consecuencias con impacto significativo para la institución o terceros.
Alta	Activo de Información cuya modificación no deseada tiene consecuencias con impacto grave para la institución o terceros

Disponibilidad

Necesidad de preservar el tiempo de acceso al activo bajo un umbral predefinido por la institución. Sobrepasar dicho umbral implica indisponibilidad del activo la que genera distintos niveles de impacto para la institución o terceros. El valor de este atributo está directamente relacionado con la magnitud de dicho impacto. Los impactos para la institución o terceros pueden ser cuantificables (monto monetario o entrega de servicio) y no cuantificables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.). En este campo, se debe clasificar en uno de los siguientes grados:

	<table><tr><th>Grado</th><th>Definición</th></tr><tr><td>Baja</td><td>Activo de Información cuya inaccesibilidad, tiene impacto leve para la institución o terceros.</td></tr><tr><td>Media</td><td>Activo de Información cuya inaccesibilidad, tiene impacto significativo para la institución o terceros.</td></tr><tr><td>Alta</td><td>Activo de Información cuya inaccesibilidad, tiene impacto grave para la institución o terceros.</td></tr></table>
Criticidad	Esta columna se encuentra destacada con azul pues es una de las que dan consistencia entre esta hoja y la siguiente. Esta columna es calculada automáticamente en la planilla de instrumentos, en función de la tríada Confidencialidad-Integridad-Disponibilidad y puede tomar los siguientes valores: <table><tr><th>Grado</th><th>Definición</th></tr><tr><td>Baja</td><td>Ninguno de los valores asignados a la triada supera el valor "público" o "bajo".</td></tr><tr><td>Media</td><td>Alguno de los valores asignados a la triada es "medio".</td></tr><tr><td>Alta</td><td>Alguno de los valores asignados a la triada es "Reservado" o "Alto"</td></tr></table>

5.2 Hoja "ANÁLISIS DE RIESGOS".

Esta hoja del libro Excel, tiene por objetivo identificar los riesgos potenciales que amenazan los activos inventariados en la institución. Éstos pueden ser identificados ya sea por haberse materializado y haber afectado la seguridad de los activos, independiente de que exista registro de dicho incidente o porque el activo se encuentra en una situación de vulnerabilidad.

El análisis de riesgos, se distribuye en tres secciones que se describen a continuación:

1) Caracterización del activo:

Inicialmente, esta hoja debe estar pre-cargada con los activos identificados en la hoja – "Inventario" (de los cuales se detalla el proceso al que pertenece, el nombre del activo de información, su confidencialidad, integridad, disponibilidad y criticidad).

En esta sección, existen 6 campos (Proceso; Activo; Confidencialidad; Integridad; Disponibilidad; Criticidad), donde la información que se encuentra fue declarada en el Inventario de Activos, dicha información permite dar continuidad al análisis de riesgos.

2) Identificación y caracterización de los riesgos:

Dependiendo de la criticidad declarada en el inventario, en este análisis es posible identificar los riesgos asociados a un activo. Para registrar cada uno de ellos, se debe insertar en la hoja Excel las filas que se requieran. A su vez, para que cada riesgo se asocie a un control de la norma ISO 27.001 anexo A, que permitan su mitigación.	
Amenaza	Evento generado a partir de un agente externo o interno de la institución, que tenga el potencial de generar algún grado de daño (ya sea en relación a la Confidencialidad, Integridad o Disponibilidad) en uno o más activos de información institucional.
Vulnerabilidad	Se refiere a alguna "Condición de debilidad o fragilidad que se encuentra presente en el activo identificado". Usualmente se traduce en una debilidad o ausencia de control, que posibilita la ocurrencia de eventos no deseados y que pueden afectar a uno o más activos de información.
Descripción del Riesgo	Descripción de la consecuencia que existiría para el proceso, en el caso de que la Amenaza descrita afectase concretamente alguna vulnerabilidad del

	activo de información identificado.
Probabilidad de ocurrencia	Posibilidad de que el riesgo se materialice. Los valores posibles son: Casi Certeza; Probable; Moderado; Improbable; Muy Improbable.
Impacto	Corresponde a los efectos que tiene en la institución la materialización del riesgo. Los valores posibles son: Catastróficas; Mayores; Moderadas; Menores; Insignificantes.
Severidad	Corresponde al nivel de gravedad del riesgo, este será calculado por la planilla y corresponde a la probabilidad de ocurrencia por el impacto (Tabla 2). Los resultados posibles son: Extremo; Alto; Moderado; Bajo: ***Niveles de severidad del riesgo***

NIVEL PROBABILIDAD (P)	NIVEL IMPACTO (I)	SEVERIDAD DEL RIESGO S = (P x 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)	**ALTO (4)**
Muy improbable (1)	Moderadas (3)	**MODERADO (3)**
Muy improbable (1)	Menores (2)	**BAJO (2)**
Muy improbable (1)	**Insignificantes (1)**	**BAJO (1)**

Fuente: Guía Técnica Nº 53. CAIGG

3) Medidas de mitigación

Esta sección permite caracterizar cada uno de los controles seleccionados para mitigar los riesgos identificados	
Control para mitigar el riesgo	Corresponde a las medidas que propone la NCh-ISO 27001.Of2013, cuya implementación permitirá mitigar el riesgo identificado. Se debe agregar filas en caso de requerirse más de una
Cumplimiento	Corresponde a la declaración (afirmativa o negativa) respecto al cumplimiento del "Control para mitigar el riesgo" definido en la columna M.
Nombre del Archivo Evidencia	Nombre del archivo complementario que se presenta como medio de verificación de los controles que se declaren cumplidos, es decir, con un "SI" en la columna "Cumplimiento". En caso de incumplimiento, se deja vacío o indicar "no aplica".

DIRECCIÓN

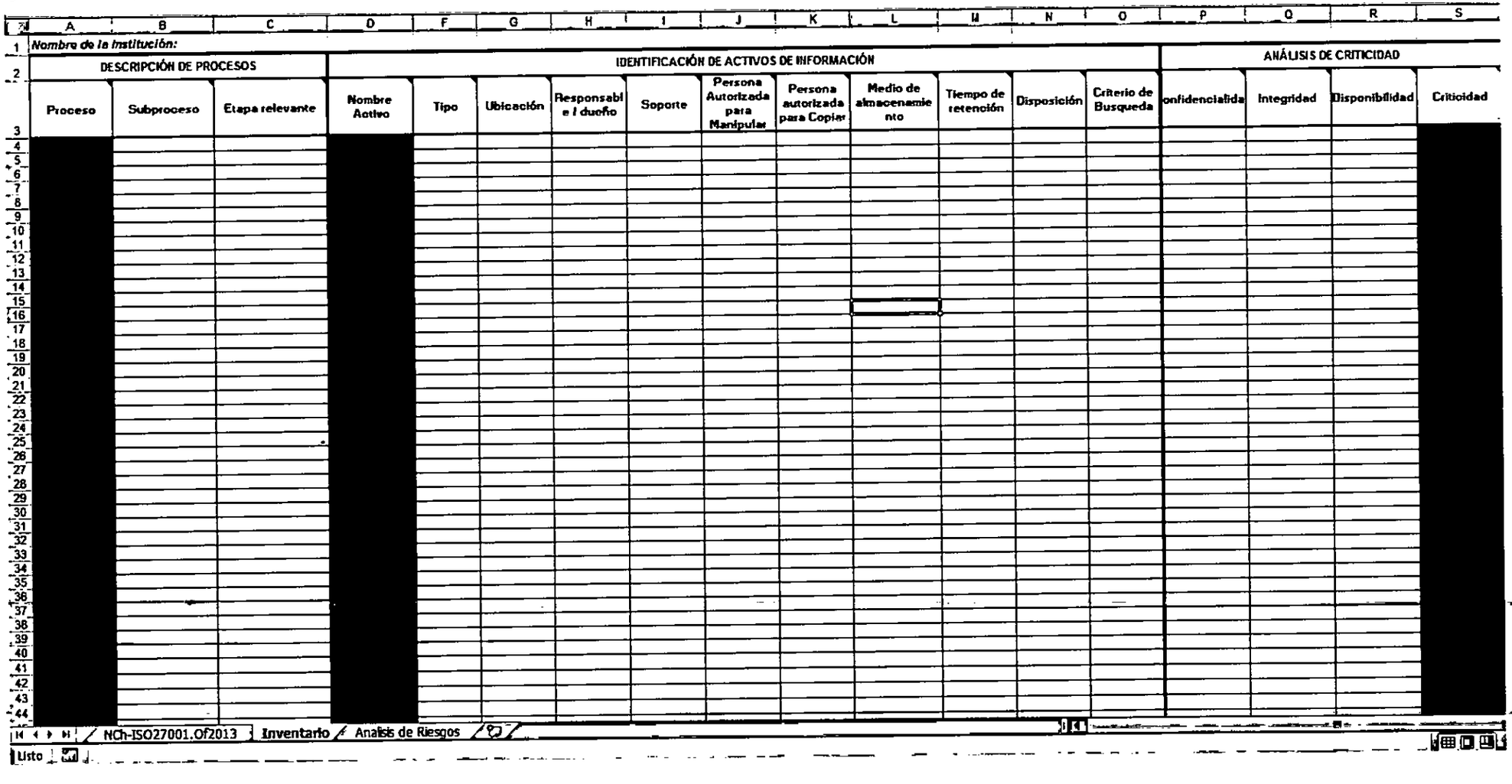
Finalmente, una vez construido el inventario, éste será publicado en la intranet de la institución para consulta y disposición de los diferentes departamentos y áreas de JUNAEB (de éste último, se excluirá la hoja de análisis de riesgo que sirve como información para el Encargado de Seguridad de la Información. Quien lo requiera, lo puede solicitar directamente vía mail).

No obstante a lo anterior, el Departamento de Auditoria Interna podrá auditar el presente procedimiento, según disponibilidad presupuestaria u otros aspectos a considerar.

DIRECCIÓN

5. REGISTROS

Hoja Inventario (Excel)

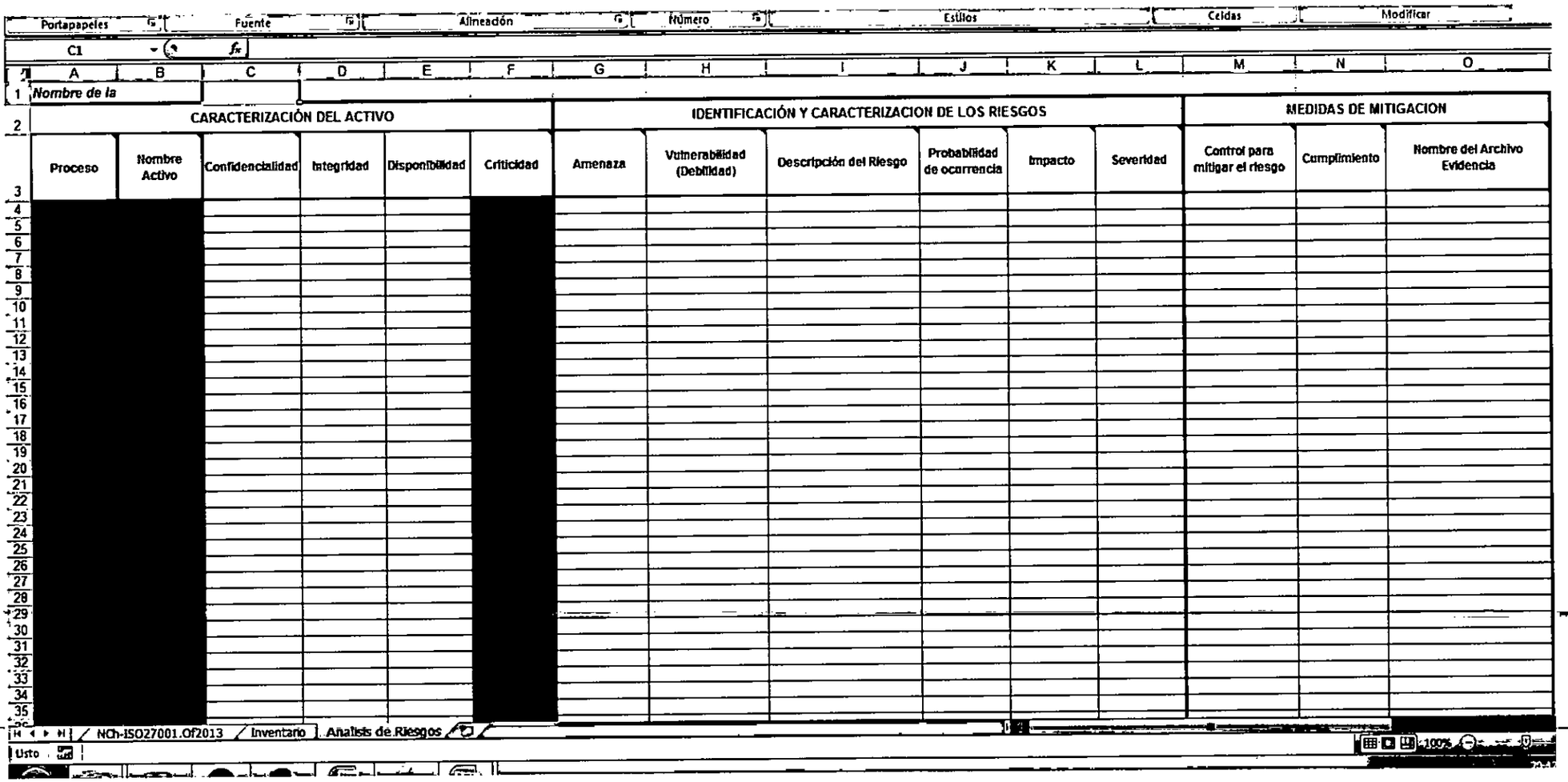


	A	B	C	D	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	*Nombre de la institución:*																	
2	DESCRIPCIÓN DE PROCESOS			IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN											ANÁLISIS DE CRITICIDAD			
3	Proceso	Subproceso	Etapa relevante	Nombre Activo	Tipo	Ubicación	Responsable / dueño	Soporte	Persona Autorizada para Manipular	Persona autorizada para Copiar	Medio de almacenamiento	Tiempo de retención	Disposición	Criterio de Busqueda	onfidencialida	Integridad	Disponibilidad	Criticidad
4	[redacted]			[redacted]														[redacted]
5																		
6																		
7																		
8																		
9																		
10																		
11																		
12																		
13																		
14																		
15																		
16																		
17																		
18																		
19																		
20																		
21																		
22																		
23																		
24																		
25																		
26																		
27																		
28																		
29																		
30																		
31																		
32																		
33																		
34																		
35																		
36																		
37																		
38																		
39																		
40																		
41																		
42																		
43																		
44																		

NCh-ISO27001.Of2013 | Inventario | Analisis de Riesgos

Listo

Hoja Análisis de Riesgo (Excel)



Nombre de la														
CARACTERIZACIÓN DEL ACTIVO						IDENTIFICACIÓN Y CARACTERIZACION DE LOS RIESGOS						MEDIDAS DE MITIGACION		
Proceso	Nombre Activo	Confidencialidad	Integridad	Disponibilidad	Criticidad	Amenaza	Vulnerabilidad (Debilidad)	Descripción del Riesgo	Probabilidad de ocurrencia	Impacto	Severidad	Control para mitigar el riesgo	Cumplimiento	Nombre del Archivo Evidencia
[redacted]	[redacted]				[redacted]									

NCh-ISO27001.Of2013 | Inventario | Analisis de Riesgos

6. **CONTROL DE CAMBIOS**

Nº Revisión	Cambio	Fecha	Aprobado por:
00	Creación del Procedimiento de Inventario de Activos	08/11/17	Director Nacional

ARTÍCULO SEGUNDO.- CÚMPLASE, con las obligaciones específicas establecidas en la Política de Inventarios, para los siguientes Departamentos, Unidades o Comités de la Dirección Nacional de JUNAEB; i) Comité Seguridad de la Información: a) Proponer mejoras y/o actualización de la Política; b) Informar a la Dirección en caso de ocurrencia de incumplimientos a ésta Política que afecten a la institución; ii) Encargado/a Seguridad de la Información: verificar y monitorear la ejecución de la Política ; iii) Jefaturas de departamentos, unidades y funcionarios: a) conocer y cumplir con esta Política; b) alertar los incumplimientos a las directrices emanadas de esta Política; c) Implementar medidas preventivas y/o correctivas que mitiguen o eliminen posibles riesgos.

ARTÍCULO TERCERO.- CÚMPLASE, con las obligaciones específicas establecidas en el Procedimiento de Inventario de Seguridad de la Información, para los siguientes Departamentos, Unidades o Comités de la Dirección Nacional de JUNAEB; i) Encargado/a de Seguridad de la Información: informar el inventario de seguridad de la Información a los servicios que miden cumplimiento PMG y SSI, aplicando el éste documento; ii) Jefes de Departamentos o Unidades: a) colaborar con el levantamiento de inventario de Seguridad de la Información proporcionando información fidedigna y actualizada según requerimiento del DEPLACGE, b) Informar las alertas al personal a cargo, c) reportar al Sistema de Gestión de Incidentes y poner en inicio el proceso de respuesta, planes de contingencia o planes de recuperación, etc; iii) Profesionales de la Unidad de Planificación, DEPLACGE: Apoyar las gestiones del encargado de Seguridad de la Información en el levantamiento de sus activos e información asociada.

ARTÍCULO CUARTO.- DIFÚNDASE, la Política de Inventarios así como el Procedimiento de Inventario de Seguridad de la Información, por medio de su publicación en la Intranet institucional permitiendo así su libre consulta para todos los funcionarios.

DIRECCIÓN

ARTÍCULO QUINTO.- PUBLÍQUESE la presente resolución una vez que se encuentre totalmente tramitada en la subsección "Actos con Efectos sobre Terceros" de la sección "Actos y Resoluciones", ubicado en el mini sitio "Gobierno Transparente" contenido en el portal web de JUNAEB a objeto de dar cumplimiento a lo previsto tanto en el artículo 7 de la ley N°20.285 sobre acceso a la información pública como con lo dispuesto en el artículo 51 de su reglamento.

Junta Nacional de Auxilio Escolar y Becas
SECRETARIO GENERAL

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

DIRECCIÓN

MBG/EGP/RFV/jon/sfa
DISTRIBUCIÓN:
1. Jefaturas de Departamentos JUNAEB
2. Directores Regionales JUNAEB
3. Departamento de Administración y Finanzas
4. Departamento Jurídico
5. Departamento de Planificación, Control de Gestión de Estudios
6. Archivo DEPLACGE

Minuta Jurídica N° 3628-17