



MEMORÁNDUM N°

58/2019

**DE:** JUAN BRAVO MIRANDA  
SECRETARIO EJECUTIVO (S)

**A:** JEFATURAS DE LAS DIVISIONES DE LA AGENCIA DE CALIDAD  
DE LA EDUCACIÓN

**C/C:** JEFATURA DEL DEPARTAMENTO DE AUDITORÍA  
JEFATURA DE LA UNIDAD DE PLANIFICACIÓN

**REF.:** Decreto Exento N° 324, de 2018, del Ministerio de Hacienda,  
que aprueba Programa Marco de los Programas de  
Mejoramiento de la Gestión de los servicios en el año 2019,  
para el pago del incremento del desempeño institucional del  
artículo 6° de la Ley N° 19.553.

**FECHA:** 14 ABR 2019

---

Como es de su conocimiento los Programas de Mejoramiento de la Gestión (PMG) en los servicios públicos tienen su origen en la Ley N° 19.553, de 1998, que concede una asignación de modernización y otros beneficios, y asocian el cumplimiento de objetivos de gestión a un incentivo monetario para los funcionarios públicos.

En dicho contexto, para el año 2019 se incluyó el objetivo de gestión eficaz, cuyo grado de cumplimiento se mide a través de indicadores de desempeño, siendo, uno de ellos, el relativo a controles de seguridad de la información.

Es debido a lo anterior, que se procedió, por una parte, a elaborar políticas y procedimientos concernientes al Sistema de Gestión de Seguridad de la Información, y, por la otra, a revisar y/o actualizar los ya vigentes en la Agencia, resultando, como producto de todo ello, primeras o nuevas versiones de los referidos instrumentos, cuya difusión resulta imprescindible de realizarse al interior de la Agencia.

Ahora bien, a la fecha del presente memorándum, el Comité de Seguridad de la Información de la Agencia ha aprobado, a través de acta de 03 de julio de 2019, las políticas de estructura funcional del Sistema de Gestión de Seguridad de la Información; la de seguridad para recursos humanos; la de control de acceso físico y lógico; y la de escritorio y pantallas limpias, las que serán aprobadas por las respectivas resoluciones exentas de este servicio.

En cuanto a los procedimientos aprobados mediante la antes citada acta del Comité de Seguridad de la Información, también se precisa de su consecuente propagación, por lo que, para su acabado conocimiento y puesta en práctica cuando corresponda, se pasan a insertar a continuación, a saber:

## **Tabla de Contenidos**

1. Procedimiento de eliminación o reutilización equipamiento (página 3)
2. Procedimiento de asignación y devolución de recursos (página 7)
3. Procedimiento de contacto con autoridades (página 14)
4. Procedimiento de respaldo de información (página 23)
5. Procedimiento de contacto con grupos de interés (página 31)
6. Procedimiento de elaboración/ actualización de inventario de activos (página 38)
7. Procedimiento de inicio de sesión seguro (página 45)
8. Procedimiento de mantención de equipos críticos (página 49)
9. Procedimiento de equipo de usuario desatendido (página 57)

## 1. PROCEDIMIENTO DE ELIMINACIÓN O REUTILIZACIÓN DE EQUIPAMIENTO.

| Procedimiento de Eliminación o Reutilización de Equipamiento<br>Control A.11.02.07 |   |  |   |
|--|---|--|---|
| Tabla de Contenidos  |   |  |   |
| 1  | Objetivo.....   |  | 3 |
| 2  | Alcance.....  |  | 3 |
| 3  | Normas y Referencias.....   |  | 3 |
| 4  | Términos y Definiciones. ....   |  | 4 |
| 5.   | Roles y Responsabilidades .....   |  | 4 |
| 6.   | Directrices Generales para la Entrega y Devolución de Recursos .....          |  | 4 |
| 7.   | Modo de Operación .....   |  | 4 |
| 7.1  | Flujo de Procedimiento .....  |  | 5 |
| 7.2  | Matriz del Proceso de Entrega de Activos en caso de Ingreso de Nuevo Personal |  | 5 |
| 7.7  | Matriz de Responsabilidades.....  |  | 6 |
| 8.   | Registro de Operación.....  |  | 6 |

| REVISIONES DEL PROCEDIMIENTO |          |                       |                                  |
|------------------------------|----------|-----------------------|----------------------------------|
| Nº Versión                   | Fecha    | Motivo de la revisión | Páginas elaboradas o modificadas |
| Cero (0)                     | 28-06-19 | Elaboración inicial   | Todas                            |

| ELABORADO POR   | VALIDACIÓN TÉCNICA       | APROBADO POR  | APROBADO POR    |
|---|--------------------------|---|-----------------|
| Sistema de Gestión de Seguridad de Información y Ciberseguridad | Patrick Soto<br>Jefe TIC | Andrea Soto Araya<br>Encargada de Seguridad de la Información | Comité de SGSIC |

### 1. Objetivo.

Este procedimiento tiene por finalidad tanto determinar el mecanismo de verificación del equipamiento por eliminar o reutilizar, para asegurar que estos no contengan información confidencial, como especificar los mecanismos de destrucción de información sensible, o que cuente con derechos de autor, de la Agencia de Calidad de la Educación

### 2. Alcance.

Todos los equipos institucionales inventariados, cuya adquisición haya significado la inversión de recursos para la Institución como, por ejemplo, computadores personales, teléfonos celulares, dispositivos portátiles y otros que se pongan a disposición del personal o de funcionarios(as) en particular, y que, por el término de la vida útil de este, deberá ser eliminado para destrucción o reutilización.

### 3. Normas y Referencias.

- Ley N° 19.223, sobre Figuras Penales relativas a la Informática.
- Ley N° 20.285, sobre Acceso a la Información Pública.
- DS N° 83/2005, del Ministerio Secretaría General de la Presidencia, Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información - Requisitos.

- Norma NCh-ISO 27002:2013, Código de Prácticas para la Gestión de la Seguridad de la Información.
- Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, vigente.
- Política de Uso de Celulares Corporativos de la Agencia de Calidad de la Educación, vigente.

#### 4. Términos y Definiciones.

|  |   |
|--|---|
| <b>Borrado Seguro (Wiping)</b>             | Proceso mediante el cual se sobrescribe varias veces cada segmento de la superficie del disco del equipo en cuestión con cadenas aleatorias de ceros y unos.      |
| <b>Distro Linux (System Rescue 6.0.2.)</b> | Proceso de borrado seguro, cuyo objetivo es específicamente el que la información que una vez fue contenida por el equipo no pueda ser recuperada posteriormente. |

#### 5. Roles y Responsabilidades.

- Unidad de Tecnologías de Información y Comunicación:** Es responsabilidad de la Unidad eliminar correctamente la información contenida en los equipos que serán eliminados, reutilizados o devueltos a los proveedores. Una vez se determine que la información que contiene un equipo será eliminada, la Unidad deberá comunicar de esto al Encargado(a) de Seguridad de la Información, mediante la utilización del "Registro de Eliminación de Información o Equipamiento". En caso de que un equipo deba ser formateado para su posterior reutilización, la Unidad deberá solicitar la autorización de la Jefatura de la División de Administración General.
- Encargado(a) de Seguridad de la Información:** Como rol líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), tiene la responsabilidad de monitorear el cumplimiento de este procedimiento. Adicionalmente debe ser notificado del acta de eliminación que entrega la Unidad TIC.
- Jefatura de División de Administración General:** Como supervisores de las acciones realizadas por la Unidad TIC, deberá autorizar el formateo de los equipos que serán reutilizados posteriormente por personal de la organización.

#### 6. Directrices Generales para la Entrega y Devolución de Recursos.

Teniendo en cuenta la importancia de la información manipulada dentro de la institución, particularmente en relación con la privacidad y confidencialidad de esta, es necesario tomar las precauciones pertinentes para la protegerla. En función de lo anterior la organización ha definido los siguientes tipos de eliminación de información para los diferentes escenarios presentados a continuación:

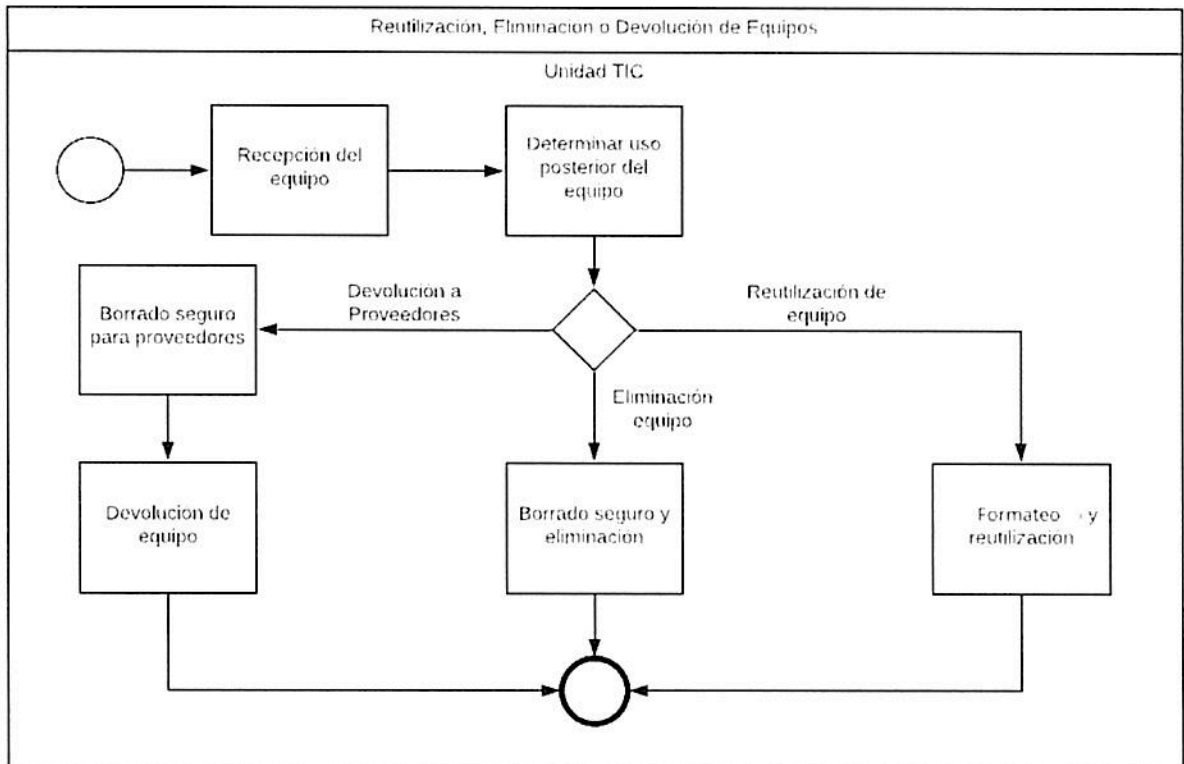
| <b>TIPO DE EVENTO</b>           | <b>FORMA DE ELIMINACIÓN DE INFORMACIÓN</b>  |
|---------------------------------|---|
| <b>Eliminación del Equipo</b>   | Borrado Seguro (Wiping)   |
| <b>Reutilización del Equipo</b> | Borrado Seguro (Wiping)<br>Actualización del ID del equipo en la CMDB, quedando con estado "Disponible" |
| <b>Devolución del Equipo</b>    | Borrado Seguro (Wiping)<br>Distro Linux, system rescue 6.0.2  |

Es importante detallar que una vez sea realizada cualquiera de estas formas de eliminación, deberá ser llenado el "Registro de Eliminación de Información o Equipamiento", el cual deberá ser visado por el Encargado(a) de Seguridad de la Información.

#### 7. Modo de Operación.

De acuerdo con los eventos descritos anteriormente, se establece un flujo comunicacional específico, en donde, de acuerdo con el tipo de evento, se definen las tareas pertinentes, así como los roles responsables de la realización de estas.

### 7.1 Flujo de Procedimiento.



### 7.2 Matriz del Proceso de Entrega de Activos en caso de Ingreso de Nuevo Personal.

| ID | ACTIVIDAD                           | DESCRIPCIÓN  | RESPONSABLE | ID ACTIVIDAD SIGUIENTE |
|----|-------------------------------------|--|-------------|------------------------|
| 1  | Recepción del equipo                | Una vez que el equipo ha cumplido su vida útil dentro de la organización y es necesario que este sea eliminado, debe ser entregado a Unidad TIC para asegurar que la información almacenada dentro de estos equipos sea correctamente eliminada.   | Unidad TIC  | 2                      |
| 2  | Determinar uso posterior del equipo | Con el objetivo de hacer un borrado seguro de la información contenida en el equipo, es necesario determinar correctamente el uso posterior que se le dará al equipo en cuestión, este puede ser: <ul style="list-style-type: none"> <li>- Equipo será devuelto a los proveedores (3)</li> <li>- Equipo será eliminado (4)</li> <li>- Equipo será reutilizado (5)</li> </ul> | Unidad TIC  | 3, 4, o 5              |
| 3  | Borrado seguro para proveedores     | Se deberá efectuar un borrado seguro (Wiping). Adicionalmente se deberá correr Distro Linux (System rescue 6.0.2) con el objetivo de que la información no pueda ser recuperada por los proveedores  | Unidad TIC  | 3A                     |
| 3A | Devolución de equipo                | Una vez se ha asegurado que la información que el equipo contenía no puede ser recuperada, se puede efectuar la devolución del equipo al proveedor.  | Unidad TIC  | FIN                    |

| ID | ACTIVIDAD                      | DESCRIPCIÓN  | RESPONSABLE | ID ACTIVIDAD SIGUIENTE |
|----|--------------------------------|--|-------------|------------------------|
| 4  | Borrado seguro y eliminación   | Se procederá a efectuar un borrado seguro sobre el equipo (Wiping), haciendo utilización también de Distro Linux (System rescue 6.0.2). Una vez este sea realizado, se procederá a eliminar el equipo según lo establecido en el Procedimiento de Eliminación de Medios.   | Unidad TIC  | FIN                    |
| 5  | Borrado seguro y reutilización | Se efectuará el borrado seguro del equipo. Posteriormente se deberá actualizar el ID del equipo en la CMDB, quedando este como "disponible". Cuando el equipo sea asignado para su reutilización, se deberá asignar el ID cambiado al trabajador a quien fue asignado el equipo.<br><br><b>Nota:</b> Es importante detallar que en caso de que un equipo deba ser reutilizado posteriormente, es la Jefatura de la División de Administración General quien debe autorizar el formateo del equipo en cuestión. | Unidad TIC  | FIN                    |

### 7.3 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

De esta forma, la matriz de responsabilidades para el proceso es:

| ID | ACTIVIDAD                           | UNIDAD TIC | ENCARGADA SI | JEFATURA DAG |
|----|-------------------------------------|------------|--------------|--------------|
| 1  | Recepción del equipo                | R/E        | I            | I            |
| 2  | Determinar uso posterior del equipo | R/E        | -            | -            |
| 3  | Borrado seguro para proveedores     | R/E        | A            | I            |
| 3A | Devolución de equipo                | R/E        | -            | -            |
| 4  | Borrado seguro y eliminación        | R/E        | A            | -            |
| 5  | Borrado seguro y reutilización      | R/E        | A            | A            |

### 8. Registro de Operación.

| REGISTRO                                    | ID | RESPONSABLE/DUEÑO DEL REGISTRO | TIEMPO RETENCIÓN      | SOPORTE | LUGAR |
|---|----|--------------------------------|-----------------------|---------|-------|
| Inventario de recursos tecnológicos en CMDB | -  | Analista de Soporte al Usuario | 4 años / Archivo UTIC | Digital | CMDB  |

## 2. PROCEDIMIENTO DE ASIGNACIÓN Y DEVOLUCIÓN DE RECURSOS.

| Procedimiento de Asignación y Devolución de Recursos<br>Control A.08.01.04 |  |
|--|--|
| Tabla de Contenidos  |  |
| 1  | Objetivo..... 7  |
| 2  | Alcance..... 7   |
| 3  | Normas y Referencias..... 7  |
| 4  | Términos y Definiciones..... 8   |
| 5.   | Roles y Responsabilidades..... 8   |
| 6.   | Directrices Generales para la Entrega y Devolución de Recursos..... 9                    |
| 7.   | Modo de Operación..... 9   |
| 7.1  | Flujo de Procedimiento..... 9  |
| 7.2  | Matriz del Proceso de Entrega de Activos en caso de Ingreso de Nuevo Personal..... 9     |
| 7.3  | Flujo de Procedimiento..... 11   |
| 7.4  | Matriz del Proceso de Recepción de Activos en caso de Desvinculación de Personal..... 11 |
| 7.5  | Flujo de Procedimiento..... 12   |
| 7.6  | Matriz del Proceso de Entrega de Activos en caso de Solicitud..... 12                    |
| 7.7  | Matriz de Responsabilidades..... 12  |
| 8.   | Registro de Operación..... 2   |

### REVISIONES DEL PROCEDIMIENTO

| Nº Versión | Fecha    | Motivo de la revisión | Páginas elaboradas o modificadas |
|------------|----------|-----------------------|----------------------------------|
| Uno (1)    | 28-06-19 | Elaboración inicial   | Todas                            |

| ELABORADO POR   | VALIDACIÓN TÉCNICA       | APROBADO POR  | APROBADO POR    |
|---|--------------------------|---|-----------------|
| Sistema de Gestión de Seguridad de Información y Ciberseguridad | Patrick Soto<br>Jefe TIC | Andrea Soto Araya<br>Encargada de Seguridad de la Información | Comité de SGSIC |

### 1. Objetivo.

El presente procedimiento tiene por objetivo establecer y definir las actividades a realizar para solicitar y controlar tanto la entrega como la devolución de los recursos tecnológicos pertenecientes a la Agencia de Calidad de la Educación, en adelante la Agencia. El procedimiento en cuestión está particularmente diseñado para dejar constancia de la entrega o recepción de los recursos cuando se produce un ingreso, una desvinculación o algún otro cambio en las funciones del personal de la Agencia.

### 2. Alcance.

Este procedimiento deberá ser aplicado sobre todos los recursos tecnológicos de propiedad de la Agencia que deban ser asignados a funcionarios(as) tanto internos de planta, contrata u honorarios, como externos, terceros y proveedores, que de forma directa o indirecta requieran de estos recursos para el cumplimiento de sus responsabilidades.

### 3. Normas y Referencias.

- Ley N° 20.529, Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su Fiscalización.

- DFL N° 29, del año 2004 que fija el Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo.
- Ley N° 19.880, Establece Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la administración del Estado.
- Ley N° 20.285, sobre acceso a la Información Pública.
- Decreto Supremo N° 83, Norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información - Requisitos.
- Norma NCh-ISO 27002:2013, Código de Prácticas para la Gestión de la Seguridad de la Información.
- Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, vigente.

#### 4. Términos y Definiciones.

|   |  |
|---|--|
| <b>Activo de Información</b>                  | La Información es un activo fundamental para el desarrollo, operativa, control y gestión de la Institución, se considera como la información propiamente tal, así como todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.  |
| <b>Acceso a la información</b>                | El acceso a la información es el derecho que tiene toda persona de buscar, recibir y difundir información en poder del Servicio, y que justifique el quehacer para el cual fue contratado.   |
| <b>Derechos de accesos</b>                    | Conjunto de permisos dados a un usuario, de acuerdo con sus funciones, para acceder a un determinado recurso.  |
| <b>Restringir el acceso</b>                   | Delimitar el acceso de los usuarios, servidores públicos a honorarios y terceras partes a determinados recursos.   |
| <b>Sistema de información</b>                 | Aplicaciones, servicios, activos de tecnología de información, u otros componentes para el manejo de la información.   |
| <b>Medios de procesamiento de información</b> | Los dispositivos internos y/o externos que tenga la capacidad de procesar información, almacenarla y que se encuentren disponibles para ser manipulados por el usuario. Como ejemplos de medios de procesamiento de información, podemos enumerar: <ul style="list-style-type: none"> <li>• Servidores de aplicaciones: de correo, de impresión, aplicaciones web.</li> <li>• Servidores de Almacenamientos.</li> <li>• Computadores personales.</li> <li>• Discos duros externos</li> <li>• Pendrives.</li> <li>• Teléfonos móviles.</li> </ul> |
| <b>Usuario(a)</b>                             | Persona que utiliza un activo de información, tales como: computador personal, notebook, tablet, disco duro, teléfonos de la Agencia en virtud de su empleo, sin importar la naturaleza jurídica de este o del estatuto que lo rija.   |

#### 5. Roles y Responsabilidades.

- d) **Analista Departamento de Gestión y Desarrollo de las Personas:** Como miembro del Departamento de Gestión y Desarrollo de Personas, colabora de forma directa con los procesos de vinculación y desvinculación de la organización. En función de lo anterior, es también responsable de dar inicio al proceso de entrega/devolución de recursos de la Agencia, mediante el llenado tanto del formulario de vinculación, indicando los recursos que deberán ser asignados al trabajador que se incorpora a la organización, como del de desvinculación.
- e) **Encargado(a) de Seguridad de la Información:** Como rol líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), tiene la responsabilidad de monitorear el cumplimiento de este procedimiento, así como de atender cualquier complicación asociada a la entrega o recepción de recursos que son propiedad de la organización.
- f) **Analista de Soporte al Usuario:** Como rol a cargo del inventario de los recursos tecnológicos pertenecientes a la organización, es responsabilidad de éste verificar la



disponibilidad de los recursos solicitados, así como de hacer entrega de estos. Adicionalmente, debe de hacer recepción de los recursos que son devueltos por los trabajadores que han sido desvinculados de la organización. Dado lo anterior, este rol deberá también garantizar la constante mantención actualizada del inventario de recursos tecnológicos.

- g) **Jefatura Directa:** Como superior inmediato del usuario que recibe uno a varios recursos tecnológicos, es la labor de éste determinar correctamente los recursos que deberán ser facilitados al usuario en cuestión, con el objetivo de que este pueda realizar sus funciones correctamente. Adicionalmente, deberá aprobar o rechazar las solicitudes de recursos adicionales elevadas por los usuarios que se encuentren bajo su ámbito de gestión.
- h) **Usuario:** Hace referencia a todo colaborador, tanto interno como externo, a quien se le han asignado recursos para la realización de sus tareas.

**6. Directrices Generales para la Entrega y Devolución de Recursos.**

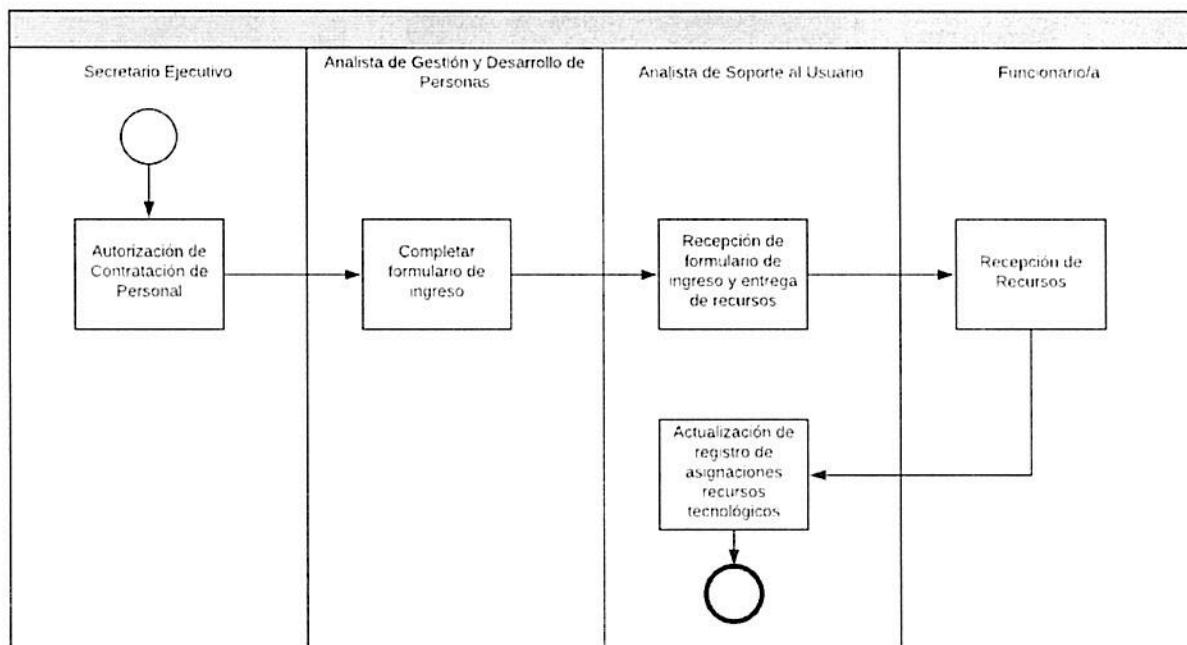
Teniendo en cuenta que todos los colaboradores y colaboradoras de la organización necesitan de recursos tecnológicos para la realización de sus tareas, es necesaria la existencia de instancias formales para hacer entrega/recepción de éstos, así como de mecanismos definidos para dejar constancia de estos movimientos. En este contexto, a continuación, se detallan los principales insumos utilizados por la organización con el objetivo de la realización ordenada del procedimiento en cuestión:

| TIPO DE EVENTO             | INSUMO                                       |
|----------------------------|--|
| Vinculación de Personal    | Anexo I: Formulario de Solicitud de Recursos |
| Desvinculación de Personal | Anexo II: Formulario de Entrega de Recursos  |

**7. Modo de Operación.**

De acuerdo con los eventos descritos anteriormente, se establece un flujo comunicacional específico, en donde, de acuerdo con el tipo de evento, se definen las tareas pertinentes, así como los roles responsables de la realización de estas.

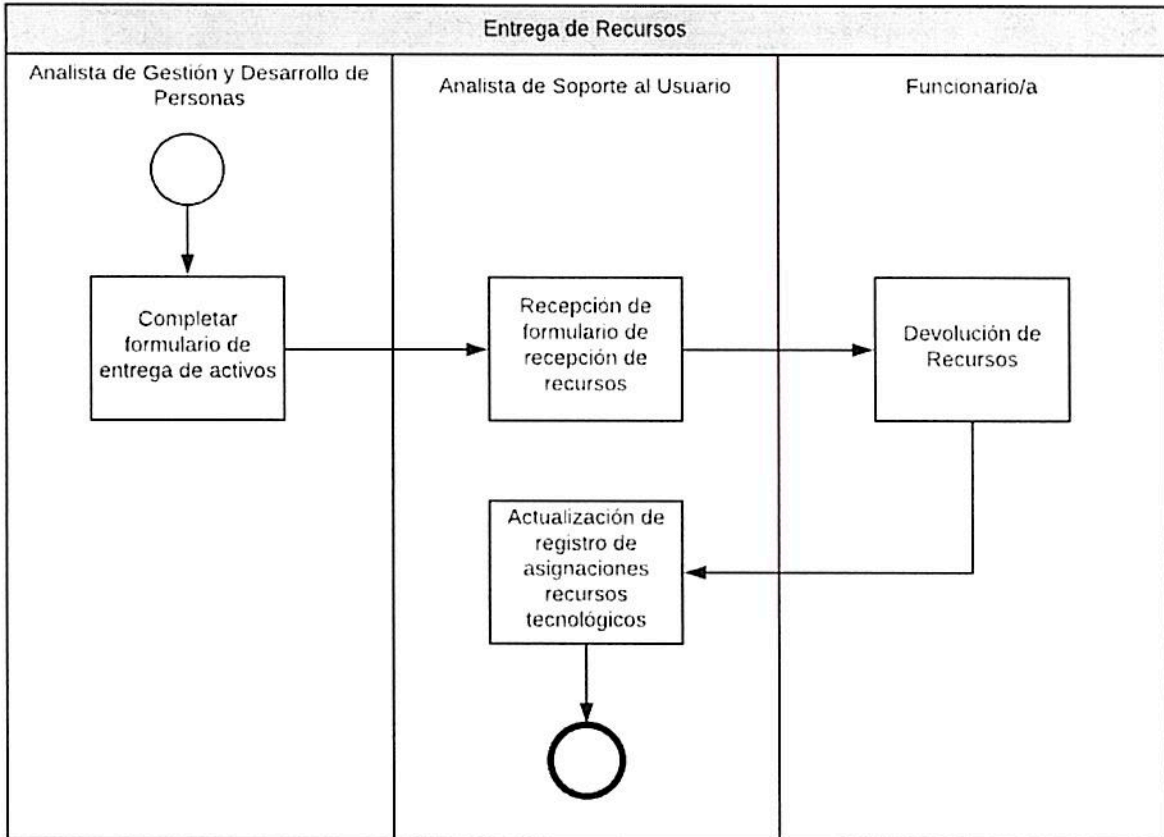
**7.1 Flujo de Procedimiento para Asignación de Recursos por Ingreso de Personal.**



**7.2 Matriz del Proceso de Entrega de Recursos en caso de Ingreso de Nuevo Personal.**

| <b>ID</b> | <b>ACTIVIDAD</b>  | <b>DESCRIPCIÓN</b>   | <b>RESPONSABLE</b>                        | <b>ID ACTIVIDAD SIGUIENTE</b> |
|-----------|---|--|---|-------------------------------|
| 1         | Autorización de contratación del personal                       | Una vez es autorizada la incorporación del personal a la organización por parte del Secretario Ejecutivo, se notifica de ésta al Departamento de Gestión y Desarrollo de las Personas, con la finalidad de hacer oficial la vinculación del personal en cuestión.  | Secretario Ejecutivo                      | 2                             |
| 2         | Completar formulario de ingreso                                 | En virtud de la autorización recibida, se procede a completar el formulario de ingreso dispuesto para solicitar recursos, en el cual se deberán especificar los recursos que serán asignados al rol que se incorpora, en función de las especificaciones entregadas en la descripción del cargo y por su Jefe Directo según corresponda. | Analista de Gestión y Desarrollo Personas | 3                             |
| 3         | Recepción de formulario de ingreso y entrega de recursos        | Se hace recepción del formulario de ingreso, en el cual se encuentran especificados los recursos que deberán ser entregados al rol que se incorpora a la organización.<br>El Analista de Soporte al Usuario deberá revisar la disponibilidad del material solicitado, y hacer entrega al trabajador de lo requerido.                     | Analista de Soporte al Usuario            | 4                             |
| 4         | Recepción de recursos   | El trabajador/a que se incorpora a la organización hace recepción de los recursos y revisa que estos correspondan a lo señalado en el formulario de ingreso. Adicionalmente, deberá firmar el acta de recepción.   | Colaborador(a) de nuevo ingreso           | 5                             |
| 5         | Actualización de Registro de Asignaciones Recursos Tecnológicos | Una vez realizada la recepción de el o los recursos tecnológicos, se debe actualizar el estado de éste/éstos en la CMDDB mediante su asignación al código del usuario.   | Analista de Soporte al Usuario            | FIN                           |

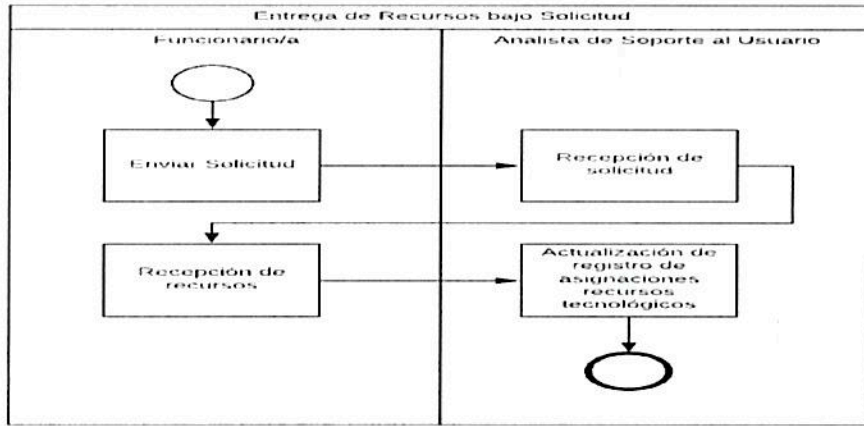
**7.3 Flujo de Procedimiento para Devolución de Recursos por Desvinculación.**



**7.4 Matriz del Proceso de Recepción de Recursos en caso de Desvinculación de Personal.**

| ID | ACTIVIDAD   | DESCRIPCIÓN   | RESPONSABLE                               | ID ACTIVIDAD SIGUIENTE |
|----|---|---|---|------------------------|
| 1  | Completar formulario de Entrega de Activos                      | Se procede a llenar el formulario de Entrega de Activos.  | Analista de Gestión y Desarrollo Personas | 2                      |
| 2  | Recepción de formularios de Entrega de Activos                  | Se hace recepción del formulario de Entrega de Activos. El Analista de Soporte al Usuario deberá revisar que el trabajador tenga recursos asignados, si es así, procede a realizar la recepción de estos. | Analista de Soporte al Usuario            | 3                      |
| 3  | Devolución de recursos  | El trabajador que ha dejado de formar parte de la organización procede a devolver los recursos que le han sido entregados y firma el acta de retiro de estos.   | Trabajador                                | 4                      |
| 4  | Actualización de Registro de Asignaciones Recursos Tecnológicos | Una vez realizada la recepción de el o los recursos tecnológicos, se debe actualizar el estado de éste/éstos en la CMDB como "disponible(s)".   | Analista de Soporte al Usuario            | FIN                    |

**7.5 Flujo de Procedimiento para Entrega de Recursos por Solicitud.**



**7.6 Matriz del Proceso de Entrega de Recursos en caso de Solicitud.**

| ID | ACTIVIDAD   | DESCRIPCIÓN  | RESPONSABLE                    | ID ACTIVIDAD SIGUIENTE |
|----|---|--|--------------------------------|------------------------|
| 1  | Elevar solicitud  | El trabajador en cuestión procede a elevar una solicitud a su Jefe Directo para la obtención de recursos esenciales para la realización de sus funciones.  | Trabajador                     | 2                      |
| 2  | Recepción de solicitud  | Se hace recepción de la solicitud aprobada por el Jefe Directo del trabajador, a continuación, se procede a verificar la disponibilidad del activo solicitado. En caso de tener stock del activo especificado, deberá ser facilitado al rol en cuestión. | Analista de Soporte al Usuario | 3                      |
| 3  | Recepción de recursos   | El trabajador hace recepción de los recursos y revisa que estos se encuentren en buen estado. Adicionalmente, deberá firmar el acta de recepción.  | Trabajador                     | 4                      |
| 4  | Actualización de Registro de Asignaciones Recursos Tecnológicos | Una vez realizada la recepción de el o los recursos tecnológicos, se debe actualizar el estado de éste/éstos en la CMDB como "disponible(s)".  | Analista de Soporte al Usuario | FIN                    |

**7.7 Matriz de Responsabilidades.**

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

De esta forma, la matriz de responsabilidades para el proceso de ingreso de nuevo personal es la siguiente:

| ID | ACTIVIDAD                    | TRABAJADOR | JEFATURA DIRECTA | ENCARGADA SI | ANALISTA SOPORTE USUARIO | ANALISTA GESTIÓN | SECRETARIO EJECUTIVO |
|----|------------------------------|------------|------------------|--------------|--------------------------|------------------|----------------------|
| 1  | Autorización de contratación | I          | I                | I            | -                        | -                | R/E                  |

|   |   |     |   |   |     |     |   |
|---|---|-----|---|---|-----|-----|---|
|   | del personal  |     |   |   |     |     |   |
| 2 | Completar formulario de ingreso                                 | C   | I | - | I   | R/E | - |
| 3 | Recepción de formulario de ingreso y entrega de recursos        | I   | I | - | R/A | -   | - |
| 4 | Recepción de recursos   | R/E | - | I | R/A | -   | - |
| 5 | Actualización de Registro de Asignaciones Recursos Tecnológicos | -   | - | - | R/E | -   | - |

De esta forma, la matriz de responsabilidades para e proceso de desvinculación es la siguiente:

| ID | ACTIVIDAD   | TRABAJADOR | JEFATURA DIRECTA | ENCARGADA SI | ANALISTA SOPORTE USUARIO | ANALISTA GESTIÓN |
|----|---|------------|------------------|--------------|--------------------------|------------------|
| 1  | Completar formulario de Entrega de Activos                      | C          | I                | -            | I                        | R/E              |
| 2  | Recepción de formularios de Entrega de Activos                  | I          | I                | -            | R/A                      | -                |
| 3  | Devolución de recursos  | R/E        | -                | I            | R/A                      | -                |
| 4  | Actualización de Registro de Asignaciones Recursos Tecnológicos | -          | -                | -            | R/E                      | -                |

De esta forma, la matriz de responsabilidades para e proceso de solicitud de recursos es la siguiente:

| ID | ACTIVIDAD   | TRABAJADOR | JEFATURA DIRECTA | ENCARGADA SI | ANALISTA SOPORTE USUARIO |
|----|---|------------|------------------|--------------|--------------------------|
| 1  | Elevar solicitud  | R/E        | A                | I            | -                        |
| 2  | Recepción de solicitud  | C          | I                | -            | R/E                      |
| 3  | Recepción de recursos   | E/A        | I                | -            | R                        |
| 4  | Actualización de Registro de Asignaciones Recursos Tecnológicos | -          | -                | -            | R/E                      |

### 8. Registro de Operación.

| REGISTRO                                     | ID | RESPONSABLE/DUEÑO DEL REGISTRO | TIEMPO RETENCIÓN      | SOPORTE | LUGAR |
|--|----|--------------------------------|-----------------------|---------|-------|
| Registro de asignaciones actualizado en CMDB | -  | Analista de Soporte al Usuario | 4 años / Archivo UTIC | Digital | CMDB  |

### **3. PROCEDIMIENTO DE CONTACTO CON AUTORIDADES.**

| <b>Procedimiento de Contacto con Autoridades<br/>Control A.06.01.03</b> |  |
|---|--|
| <b>Tabla de Contenidos</b>  |  |
| <b>1</b>  | <b>Objetivo..... 14</b>  |
| <b>2</b>  | <b>Alcance..... 14</b>   |
| <b>3</b>  | <b>Normas y Referencias..... 14</b>  |
| <b>4</b>  | <b>Términos y Definiciones. .... 15</b>  |
| <b>5.</b>   | <b>Roles y Responsabilidades ..... 15</b>  |
| <b>6.</b>   | <b>Eventos de Seguridad de la Información ..... 16</b>   |
| <b>6.1</b>  | <b>Asignación de Autoridades ante diferentes tipos de evento. .... 16</b>  |
| <b>7.</b>   | <b>Modo de Operación..... 17</b>   |
| <b>7.1</b>  | <b>Flujo de Procedimiento. .... 17</b>   |
| <b>7.2</b>  | <b>Matriz del Proceso de Contacto con Autoridades en caso de Eventos de Seguridad de la Información. .... 18</b> |
| <b>7.3</b>  | <b>Matriz de Responsabilidades..... 20</b>   |
| <b>8.</b>   | <b>Registro de Operación. .... 21</b>  |

#### **REVISIONES DEL PROCEDIMIENTO**

| <b>Nº<br/>Versión</b> | <b>Fecha</b> | <b>Motivo de la revisión</b> | <b>Páginas elaboradas o<br/>modificadas</b> |
|-----------------------|--------------|------------------------------|---|
| Uno (1)               | 28/05/2019   | Elaboración inicial          | Todas                                       |

| <b>ELABORADO POR</b>   | <b>VALIDACIÓN<br/>TÉCNICA</b>          | <b>REVISADO POR</b>   | <b>APROBADO POR</b>                          |
|--|--|---|--|
| <b>Sistema de Gestión de la Información y Ciberseguridad (SGSIC)</b> | <b>Patrik Soto<br/>Jefe Unidad TIC</b> | <b>Andrea Soto Araya<br/>Encargada de Seguridad de la Información</b> | <b>Comité de Seguridad de la Información</b> |

#### **1. Objetivo.**

El objetivo del presente documento es, definir un flujo comunicacional, oficial y estructurado, orientado a hacer frente a los diferentes tipos de eventos que pudiesen afectar la disponibilidad, integridad, confidencialidad, autenticidad y privacidad de los activos de información críticos de la Agencia, identificando aquellas autoridades tanto internas como externas que representan, según sus diferentes competencias, un apoyo para la gestión y solución de éstos.

#### **2. Alcance.**

Este procedimiento deberá ser aplicado por todos(as) los(as) funcionarios internos de planta, contrata y personal honorarios que tengan acceso de forma directa o indirecta a los activos de información de la Agencia.

#### **3. Normas y Referencias.**

- Política General de Seguridad de la Información de la Agencia, aprobada por Resolución Exenta N° 0589, de 16 de mayo de 2019, de la Agencia de Calidad de la Educación.
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información.

#### 4. Términos y Definiciones.

|  |   |
|--|---|
| <b>Amenaza</b>                               | Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o una organización.  |
| <b>Riesgo</b>                                | Las condiciones de debilidad en los activos que pueden ser afectadas por la existencia de una amenaza concreta, y las consecuencias que esto tiene. Es el efecto o materialización de la amenaza, el cual se puede clasificar respecto de su severidad, considerando su nivel de probabilidad y el impacto que generaría su ocurrencia.   |
| <b>Autoridad</b>                             | Facultad o derecho que posee un individuo o conjunto de individuos para actuar, mandar, o exigir una determinada acción a otros, en virtud del poder que emana de su posición dentro de la organización o institución. En el caso del sistema de seguridad de la información serán entendidas como autoridades, los responsables de los procesos de continuidad del negocio y recuperación ante desastres; y los servicios de emergencia, salud, bomberos y carabineros.  |
| <b>Evento de Seguridad de la Información</b> | Se refiere a la identificación y materialización de una amenaza o riesgo detectado el cual pudiera eventualmente comprometer la continuidad operacional de la Agencia.  |
| <b>Incidente de Seguridad</b>                | Se refiere a la Identificación y materialización de una amenaza o riesgo detectado que afecte la continuidad operacional que afecte activos de información relevantes para la Agencia.  |
| <b>Vulnerabilidad</b>                        | Debilidades propias de las características propias de cada activo, que los exponen a una amenaza o riesgo.  |
| <b>Evento de Seguridad</b>                   | Se refiere a la identificación y materialización de una amenaza o riesgo detectado, que afecte la continuidad operacional dañando activos relevantes de la Agencia  |
| <b>Plan de Contingencia</b>                  | Plan de Acción donde se señala explícitamente, el procedimiento a seguir, ante la ocurrencia de un incidente de seguridad de la información, que comprometa la continuidad operacional de la Agencia.   |
| <b>Activos de Información</b>                | Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta manera es que se distingue la información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.), los equipos, sistemas, infraestructura que soportan esta información y las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales. |
| <b>Contactos críticos</b>                    | Corresponden al nivel de contacto que se necesita ubicar con urgencia en caso de dificultades tecnológicas o incidentes.  |
| <b>Red de Seguridad</b>                      | Corresponden a números telefónicos públicos de servicios de emergencia, que no referencian la identificación de una persona.  |
| <b>Seguridad de la Información</b>           | Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de informar, no repudio y confidencialidad.   |

#### 5. Roles y Responsabilidades.

- i) **Funcionarios internos de la Agencia:** Todo colaborador o colaboradora interna de la Agencia de Calidad de la Educación, que de forma directa o indirecta detecte un evento o suceso que pueda perjudicar alguno de los objetivos específicos del SGSIC, establecidos en la Política General de Seguridad de Información, aprobada mediante resolución exenta número 0589, tiene la responsabilidad de informarlo, tanto a su jefatura directa, como a la Encargada(o) de Seguridad de la Información del servicio, según indica el flujo comunicacional de este procedimiento descrito en el punto 7 de este documento.
- j) **Encargada(o) de Seguridad de la Información:** Como Autoridad Interna líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), este rol tiene la responsabilidad de liderar el flujo comunicacional con las autoridades ante a la notificación

de un evento de seguridad de información, así como realizar el seguimiento de la misma, apoyando de forma constante en la toma de decisiones.

- k) **Jefatura de Unidad de Tecnologías de Información y Comunicación:** La jefatura de la Unidad TIC, como Autoridad Interna a cargo de velar por la mantención operativa de los servicios tecnológicos de la Agencia, será responsable de recibir, liderar y delegar las acciones necesarias para resolver los eventos de seguridad que estén dentro de su ámbito de responsabilidades, tanto con su equipo, como con los proveedores críticos que estén bajo su gestión.
- l) **Jefatura de División de Administración General:** La jefatura de la DAG, como Autoridad Interna a cargo de la administración general de la institución, será responsable de recibir, liderar y delegar las acciones necesarias para resolver los eventos de seguridad que estén dentro de su ámbito de responsabilidades, tanto a través de la Jefatura de Unidad de Administración General, como a través de los proveedores críticos asociados.

## 6. Eventos de Seguridad de la Información.

A continuación, se establecen de forma general, los tipos de eventos que pudiesen afectar el correcto funcionamiento de los procesos críticos de la Agencia. Éstos pueden ocasionar daños en los activos de información relevantes para la Agencia, por lo que, para cada uno de ellos, se deberá realizar una eficiente y coordinada gestión comunicacional que permita hacer frente éstos. Parte de esta gestión es el contacto apropiado con las autoridades relevantes y competentes que permitan la mitigación de los efectos de la ocurrencia del mismo.

- a) **Eventos de origen ambiental:** Corresponden a aquellos eventos que suceden sin intervención directa del ser humano. Afectan de forma directa recursos como instalaciones, hardware, redes comunicacionales, soportes de información y equipamiento auxiliar, generando así un impacto directo en la disponibilidad de los activos de información. Como ejemplos de este tipo de eventos, se tiene: desastres naturales.
- b) **Eventos de origen industrial:** Corresponden a aquellos eventos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estos eventos pueden darse de forma accidental o deliberada, y, al igual que los eventos de origen ambiental, afectan recursos como instalaciones, hardware, redes comunicacionales, soportes de información y equipamiento auxiliar, generando así un impacto directo en la disponibilidad de los activos de información. Como ejemplos de este tipo de eventos, se tiene: daños por agua, fuego y desastres industriales.
- c) **Eventos de origen tecnológico:** Corresponden a aquellos eventos que tienen su génesis en el incorrecto o no funcionamiento de los componentes tecnológicos que apalancan los procesos críticos de la Agencia, los cuales pueden ser generados tanto de forma intencional como no intencional por el ser humano. Éstos eventos pueden impactar de forma transversal tanto la disponibilidad, confidencialidad, integridad, autenticidad y privacidad de los activos de información del servicio. Como ejemplos de este tipo de eventos, se tiene: indisponibilidad o intermitencia de plataformas y software, fallas de configuración, vulnerabilidades técnicas, errores de usuarios y/o administradores, difusión de código malicioso, entre otros.
- d) **Eventos de origen en el proveedor:** Corresponden a aquellos eventos que tienen su origen en la indisponibilidad o corte de un servicio prestado por un proveedor. Al igual que en el punto anterior, éste tipo de eventos pueden generar un impacto transversal en la disponibilidad, confidencialidad, integridad, autenticidad y privacidad de los activos de información del servicio. Como ejemplos de este tipo de eventos, tenemos: corte de servicio de conexión a internet, indisponibilidad de servicio de correo electrónico y almacenamiento en la nube, corte de servicios básicos.

### 6.1 Asignación de Autoridades ante diferentes tipos de evento.

A continuación, se dan a conocer aquellos contactos críticos a los que se debe recurrir en caso de la ocurrencia de un evento de seguridad de la información según lo señalado en el punto anterior:

| TIPO DE EVENTO    | AUTORIDAD                                | INTERNA/EXTERNA | CONTACTO |
|-------------------|--|-----------------|----------|
| Origen Ambiental  | Jefe DAG / Unidad Administración General | Interna         | Anexo I  |
| Origen Industrial | Jefe DAG / Unidad                        | Interna         | Anexo I  |



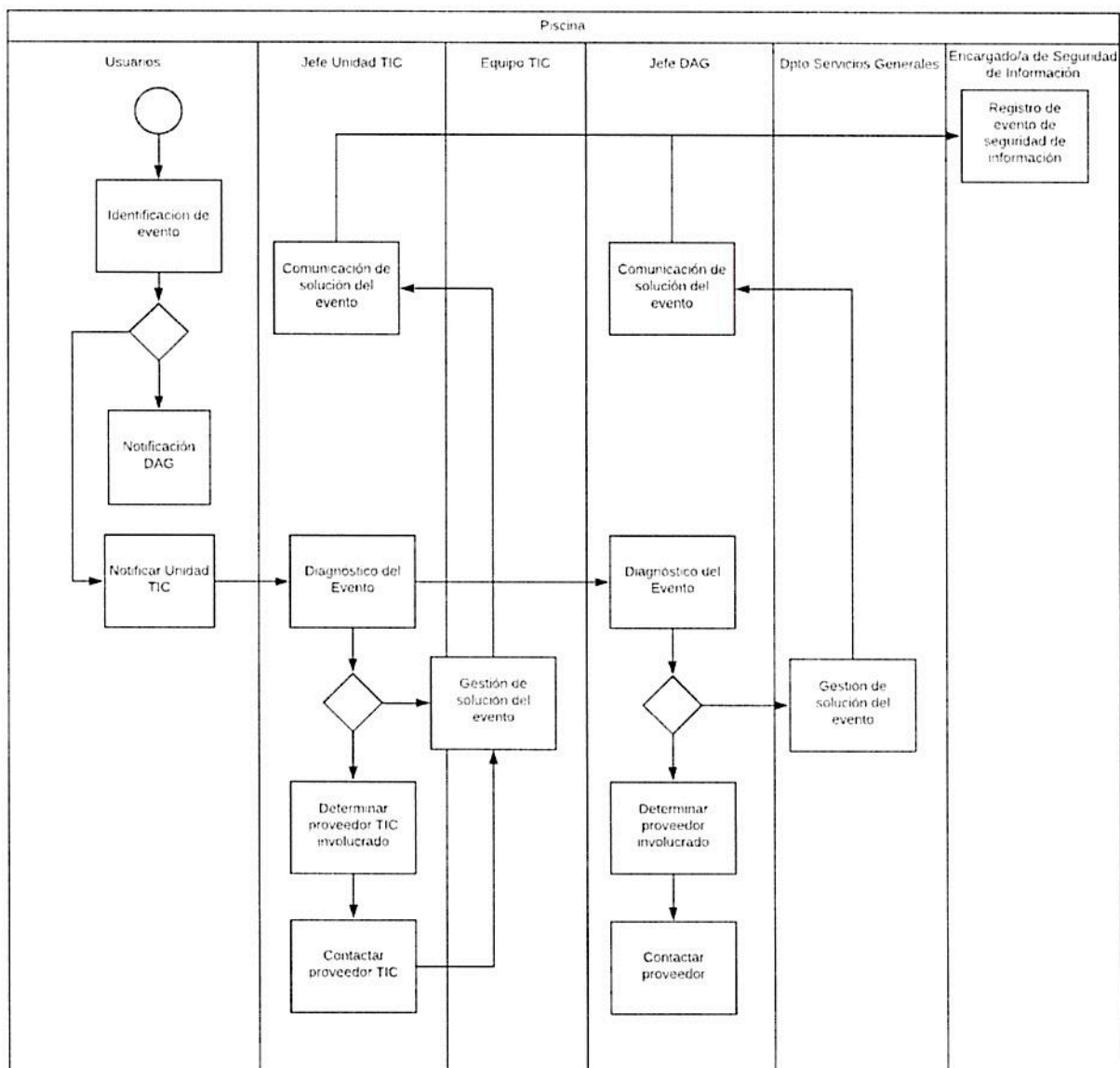
|                            |  |                          |                 |
|----------------------------|--|--------------------------|-----------------|
|                            | <b>Administración General</b>          |                          |                 |
| <b>Origen Tecnológico</b>  | <b>Jefe Unidad TIC</b>                 | <b>Interna</b>           | <b>Anexo I</b>  |
| <b>Origen en Proveedor</b> | <b>Jefe DAG/Unidad TIC y Proveedor</b> | <b>Interna y Externa</b> | <b>Anexo II</b> |

Para estos efectos, es responsabilidad de la División, Departamento o Unidad encargada de gestionar el incidente de seguridad recurrir al listado de contactos críticos de la Agencia. Este debe contener una lista amplia de contactos de emergencia, para atender cualquier situación imprevista.

### 7. Modo de Operación.

De acuerdo con los eventos descritos anteriormente, se establece un flujo comunicacional específico, en donde, de acuerdo al tipo de evento, se definen las autoridades pertinentes basado en su ámbito de responsabilidades. De esta forma, el flujo comunicacional es el siguiente:

#### 7.1 Flujo de Procedimiento.



**7.2 Matriz del Proceso de Contacto con Autoridades en caso de Eventos de Seguridad de la Información.**

| ID | ACTIVIDAD                          | DESCRIPCIÓN   | RESPONSABLE                     | ID ACTIVIDAD SIGUIENTE |
|----|------------------------------------|---|---------------------------------|------------------------|
| 1  | Comunicación preliminar del evento | <p>Se debe notificar de forma inmediata, sobre el evento de seguridad a:</p> <ul style="list-style-type: none"> <li>- Jefatura Directa</li> <li>- Encargada(o) de Seguridad de la Información</li> </ul> <p>Esta notificación debe hacerse mediante el medio de comunicación más eficiente que se encuentre disponible, o bajo la siguiente prioridad:</p> <ul style="list-style-type: none"> <li>- Sistema de Tickets</li> <li>- Anexo telefónico</li> <li>- Correo institucional</li> <li>- Celular personal</li> </ul>   | Funcionarios(as)                | 2                      |
| 2  | Determinación del tipo de evento   | <p>Según los tipos de evento descritos en el punto seis (6) de este documento, se pueden dar las siguientes posibilidades:</p> <ul style="list-style-type: none"> <li>- El evento es de origen tecnológico (3)</li> <li>- El evento es de origen natural y/o industrial (5)</li> </ul>  | Funcionario(a)                  | 3 o 5                  |
| 3  | Notificar a Unidad TIC             | <p>Se debe notificar del evento a:</p> <ul style="list-style-type: none"> <li>- Jefe de Unidad TIC</li> <li>- Soporte Interno TIC</li> </ul> <p>La notificación del evento debe indicar la mayor cantidad de antecedentes sobre el mismo y debe hacerse mediante el medio de comunicación más eficiente que se encuentre disponible, o bajo la siguiente prioridad:</p> <ul style="list-style-type: none"> <li>- Anexo telefónico</li> <li>- Correo institucional</li> <li>- Celular personal</li> </ul> <p><b>NOTA:</b> El detalle de contacto con el equipo TIC se encuentra en el documento de "Listado de Responsables por tipo de Evento de Seguridad", sección de contactos para soporte interno.</p> | Funcionario(a)                  | 4                      |
| 4  | Diagnóstico del evento             | <p>Al momento de diagnosticar el evento reportado, se pueden dar las siguientes alternativas:</p> <ul style="list-style-type: none"> <li>- El evento puede ser solucionado por el equipo TIC (4A)</li> <li>- El evento incluye a un proveedor TIC (4B)</li> </ul>   | Jefe de Unidad TIC              | 4A o 4B                |
| 4A | Solución de evento                 | <p>Se deben realizar las actividades necesarias para volver a la normalidad en el servicio tecnológico afectado.</p>  | Jefe de Unidad TIC / Equipo TIC | 7                      |

| ID | ACTIVIDAD                                | DESCRIPCIÓN  | RESPONSABLE                                 | ID ACTIVIDAD SIGUIENTE |
|----|--|--|---|------------------------|
| 4B | Determinar proveedor TIC involucrado     | <p>Se debe determinar el o los proveedores TIC involucrados en el evento para establecer contacto directo con la contraparte asignada. Se pueden dar las siguientes alternativas:</p> <ul style="list-style-type: none"> <li>- Entel</li> <li>- Microsoft</li> <li>- Google</li> <li>- AWS</li> </ul> <p><b>NOTA:</b> El detalle de los servicios asociados a cada proveedor están detallados en el documento de "Listado de Responsables por tipo de Evento de Seguridad", sección de proveedores TIC</p> | Jefe de Unidad TIC                          | 4C                     |
| 4C | Contactar proveedor TIC                  | <p>Se debe establecer contacto con la contraparte asignada con el proveedor para soporte técnico.</p> <p><b>NOTA:</b> El detalle de contacto asociado a cada proveedor se encuentra en el documento de "Listado de Responsables por tipo de Evento de Seguridad", sección de proveedores TIC</p>   | Jefe de Unidad TIC                          | 4a                     |
| 5  | Notificar a DAG                          | <p>Se debe notificar del evento a:</p> <ul style="list-style-type: none"> <li>- Jefe DAG</li> </ul> <p>La notificación del evento debe indicar la mayor cantidad de antecedentes sobre el mismo.</p> <p><b>NOTA:</b> El detalle de contacto para notificación de eventos se encuentra en el documento de "Listado de Responsables por tipo de Evento de Seguridad" de contactos de Administración General.</p>   | Funcionario(a)                              | 6                      |
| 6  | Diagnóstico del evento                   | <p>Al momento de diagnosticar el evento reportado, se pueden dar las siguientes alternativas:</p> <ul style="list-style-type: none"> <li>- El evento puede ser solucionado por alguna unidad DAG(6A)</li> <li>- El evento incluye a un proveedor General (6B)</li> </ul>   | Jefe DAG                                    | 6A o 6B                |
| 6A | Solución de evento                       | Se deben realizar las actividades necesarias para volver a la normalidad en el servicio tecnológico afectado.  | Jefe DAG / Unidad de Administración General | 7                      |
| 6B | Determinar proveedor General involucrado | Se debe determinar el o los proveedores Generales involucrados en el evento para establecer contacto directo con la contraparte asignada.  | Jefe DAG                                    | 6C                     |
| 6C | Contactar proveedor General              | <p>Se debe establecer contacto con la contraparte asignada por el proveedor.</p> <p><b>NOTA:</b> El detalle de contacto asociado a cada proveedor se encuentra en el documento de "Listado de Responsables por tipo de Evento de Seguridad" sección de proveedores TIC</p>   | Jefe DAG                                    | 6A                     |

| ID | ACTIVIDAD   | DESCRIPCIÓN   | RESPONSABLE                              | ID ACTIVIDAD SIGUIENTE |
|----|---|---|--|------------------------|
| 7  | Comunicación de solución de evento                | Se debe notificar la solución definitiva del evento a:<br>- Encargada de Seguridad de la Información<br>- Jefatura directa del funcionario(a) que alertó del evento<br>- Equipos participantes en las actividades de solución del evento<br><br>La comunicación se debe llevar a cabo mediante el correo electrónico corporativo. | Jefe Unidad TIC o Jefe DAG               | 8                      |
| 8  | Registro de evento de seguridad de la información | Se debe registrar el evento según lo establecido en el Procedimiento de Gestión de Incidentes de Seguridad de la Información.   | Encargada de Seguridad de la Información | FIN                    |

### 7.3 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

Se esta forma, la matriz de responsabilidades se estructura de la siguiente manera:

| ID | ACTIVIDAD   | FUNCI ONARIO | JEFATUR A DIRECTA | ENCARGAD A SI | JEFE TIC | JEFE DAG | EQUIP O TIC | UNIDA D ADMIN. GENER AL |
|----|---|--------------|-------------------|---------------|----------|----------|-------------|-------------------------|
| 1  | Comunicación preliminar del evento                | E/R          | I                 | I             | -        | -        | -           | -                       |
| 2  | Determinación del tipo de evento                  | R            | C                 | I             | -        | C        | -           | -                       |
| 3  | Notificar a Unidad TIC                            | R/E          | I                 | I             | I        | -        | I           | -                       |
| 4  | Diagnóstico del evento                            | -            | -                 | C/I           | R/A      | -        | E           | -                       |
| 4A | Solución de evento                                | -            | I                 | C/I           | R/A      | -        | E           | -                       |
| 4B | Determinar proveedor TIC involucrado              | -            | -                 | C/I           | R/A      | -        | E           | -                       |
| 4C | Contactar proveedor TIC                           | -            | -                 | C/I           | R/A      | -        | E           | -                       |
| 5  | Notificar a DAG                                   | R/E          | I                 | I             | -        | C        | -           | I                       |
| 6  | Diagnóstico del evento                            | -            | -                 | C/I           | -        | R/A      | -           | E                       |
| 6A | Solución de evento                                | -            | I                 | C/I           | -        | R/A      | -           | E                       |
| 6B | Determinar proveedor General involucrado          | -            | -                 | C/I           | -        | R/A      | -           | E                       |
| 6C | Contactar proveedor General                       | -            | -                 | C/I           | -        | R/A      | -           | E                       |
| 7  | Comunicación de solución de evento                | -            | I                 | I             | R/E      | R/E      | I           | I-                      |
| 8  | Registro de evento de seguridad de la información | C            | C                 | R/E           | C        | C        | C           | C                       |

**8. Registro de Operación.**

| REGISTRO  | ID | RESPONSABLE/DUEÑO DEL REGISTRO              | TIEMPO RETENCIÓN      | SOPORTE | LUGAR                       |
|---|----|---|-----------------------|---------|-----------------------------|
| Listado de responsables por tipo de evento de Seguridad | -  | Encargado(a) de Seguridad de la Información | 4 años / Archivo UTIC | Digital | PC Responsable del Registro |

**ANEXO I**

**Listado de Responsables por tipo de Eventos de Seguridad de la Agencia de Calidad de la Educación (ejemplo de formato)**

**1. Soporte Informático Agencia de Calidad de la Educación.**

| NOMBRE | ROL | CELULAR | ANEXO | CORREO ELECTRÓNICO |
|--------|-----|---------|-------|--------------------|
|        |     |         |       |                    |
|        |     |         |       |                    |

**2. Seguridad de la Información.**

| NOMBRE | ROL | CELULAR | ANEXO | CORREO ELECTRÓNICO |
|--------|-----|---------|-------|--------------------|
|        |     |         |       |                    |
|        |     |         |       |                    |

**3. Proveedores TIC.**

| PROVEEDOR | SERVICIO | NOMBRE | CELULAR/FONO | CORREO ELECTRÓNICO |
|-----------|----------|--------|--------------|--------------------|
|           |          |        |              |                    |
|           |          |        |              |                    |
|           |          |        |              |                    |
|           | -        |        |              |                    |
|           | -        |        |              |                    |
|           | -        |        |              |                    |

**4. Proveedores Generales (a través del Departamento de Administración General).**

| PROVEEDOR | SERVICIO | NOMBRE | CELULAR/FONO | CORREO ELECTRÓNICO |
|-----------|----------|--------|--------------|--------------------|
|           |          |        |              |                    |
|           |          |        |              |                    |
|           |          |        |              |                    |
|           |          |        |              |                    |

**5. Contactos de Servicios Básicos Genéricos.**

| <b>PROVEEDOR</b> | <b>CORREO ELECTRÓNICO</b> |
|------------------|---------------------------|
|                  |                           |
|                  |                           |
|                  |                           |
|                  |                           |

**Aprobado por:**

**Firma:**

**Fecha de Actualización:**

#### 4. PROCEDIMIENTO DE RESPALDO DE INFORMACIÓN.

| <b>Procedimiento de Respaldo de Información<br/>Control A.12.03.01</b> |   |
|--|---|
| <b>Tabla de Contenidos</b>   |   |
| <b>1</b>   | <b>Objetivo..... 23</b>   |
| <b>2</b>   | <b>Alcance..... 23</b>  |
| <b>3</b>   | <b>Normas y Referencias..... 23</b>   |
| <b>4</b>   | <b>Términos y Definiciones. .... 24</b>   |
| <b>5.</b>  | <b>Roles y Responsabilidades ..... 24</b>                                       |
| <b>6.</b>  | <b>Directrices Generales para Respaldo de Información ..... 24</b>              |
| <b>6.1</b>   | <b>Directrices Generales para Respaldo de Servidores..... 24</b>                |
| <b>6.2</b>   | <b>Directrices Generales para Respaldo de Estaciones de Trabajo ..... 25</b>    |
| <b>7.</b>  | <b>Modo de Operación ..... 25</b>   |
| <b>7.1</b>   | <b>Flujo de Procedimiento para Respaldo de Servidores ..... 25</b>              |
| <b>7.2</b>   | <b>Matriz del Procedimiento para Respaldo de Servidores ..... 26</b>            |
| <b>7.3</b>   | <b>Flujo de Procedimiento para Respaldo de Estaciones de Trabajo ..... 27</b>   |
| <b>7.4</b>   | <b>Matriz del Procedimiento para Respaldo de Estaciones de Trabajo ..... 28</b> |
| <b>7.5</b>   | <b>Matriz de Responsabilidades..... 29</b>                                      |
| <b>8.</b>  | <b>Registro de Operación. .... 30</b>   |

#### REVISIONES DEL PROCEDIMIENTO

| Nº Versión | Fecha      | Motivo de la revisión | Páginas elaboradas o modificadas |
|------------|------------|-----------------------|----------------------------------|
| Uno (1)    | 31/05/2019 | Elaboración inicial   | Todas                            |

| ELABORADO POR   | VALIDACIÓN TÉCNICA              | APROBADO POR  | APROBADO POR    |
|---|---------------------------------|---|-----------------|
| Sistema de Gestión de Seguridad de Información y Ciberseguridad (SGSIC) | Patrick Soto<br>Jefe Unidad TIC | Andrea Soto Araya<br>Encargada de Seguridad de la Información | Comité de SGSIC |

#### 1. Objetivo.

En función de los objetivos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), declarado en la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, en adelante la Agencia, el presente documento tiene por objetivo establecer las actividades necesarias para respaldar la información contenida tanto en servidores como en estaciones de trabajo críticas de la Agencia, de modo de mantener el cumplimiento con los objetivos del SGSIC mencionados anteriormente.

#### 2. Alcance.

Este procedimiento se debe aplicar a la totalidad de la información contenida en los servidores y estaciones de trabajo de la Agencia.

#### 3. Normas y Referencias.

- Política General de Seguridad de la Información de la Agencia de Calidad de la Educación
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información.

#### 4. Términos y Definiciones.

|  |   |
|--|---|
| <b>Copias de seguridad</b>               | Conjunto de archivos, carpetas y demás datos a los que se ha realizado copia de seguridad y se han almacenado en un archivo o en uno o varios medios (cintas, discos, DVD etc.).  |
| <b>Respaldo completo</b>                 | Es aquel que considera el respaldo de la totalidad de la información de interés para la Agencia. Incluye una copia de archivos de información de acuerdo a las extensiones de archivo que puedan contener información relevante para la Agencia, ofreciendo un respaldo por extensión de archivo sobre el perfil del usuario. |
| <b>Respaldo incremental</b>              | Copia los archivos creados o modificados desde la última copia de seguridad total (completa) o incremental.   |
| <b>Sistema de información</b>            | Aplicaciones, servicios, activos de tecnología de información, u otros componentes para el manejo de la información.  |
| <b>Usuario</b>                           | Persona que utiliza un activo de información, tales como: computador personal, notebook, Tablet, disco duro de la Agencia, ya sea que lo utilice en virtud de un empleo, sin importar la naturaleza jurídica de este o del estatuto que lo rija.  |
| <b>Periodo de retención del respaldo</b> | Es el tiempo indicado por el usuario o jefe directo que debe permanecer el respaldo activo.   |

#### 5. Roles y Responsabilidades.

- a) **Usuario:** Responsable de solicitar el respaldo de su equipo, así como de realizar los debidos respaldos en la nube mediante la utilización de las carpetas de Google.
- b) **Encargada(o) de Seguridad de la Información:** Como líder del SGSIC, este rol será el encargado de velar por el cumplimiento de este procedimiento.
- c) **Jefatura de Unidad de Tecnologías de Información y Comunicación:** Será responsable de garantizar la ejecución de este procedimiento, así como de entregar las directrices necesarias para su mejora continua en el tiempo.
- d) **Analista de Soporte al Usuario:** Será éste el rol encargada de coordinar, preparar y ejecutar los respaldos de información asociados a las estaciones de trabajo de los colaboradores y colaboradoras de la Agencia.
- e) **Supervisor de Plataforma:** Será éste el rol responsable de coordinar, preparar, ejecutar y validar los respaldos, ya sean manuales o automáticos de los servidores de la Agencia.

#### 6. Directrices Generales para Respaldo de Información

A continuación, se entregan las directrices generales asociadas al respaldo de la información tanto en servidores como en estaciones de trabajo de la Agencia de Calidad de la Educación.

##### 6.1 Directrices Generales para Respaldo de Servidores.

De forma general, el respaldo de información almacenada en servidores de la Agencia, se debe realizar de forma diaria, y según las definiciones establecidas en el procedimiento asociado. Así mismo, la Agencia de Calidad de la Educación declara que toda información compartida para el trabajo diario, así como los archivos de producción personal que sean fruto del trabajo realizado para la Agencia, mediante sus divisiones, departamentos y unidades, debe residir en servidores de archivos (carpetas compartidas) especialmente habilitados por la Unidad de Tecnologías de Información y Comunicación a cada una de éstas, como contenedores de información productiva de la Agencia. Estos servidores de archivo serán respaldados según los lineamientos establecidos para el respaldo de servidores del servicio.



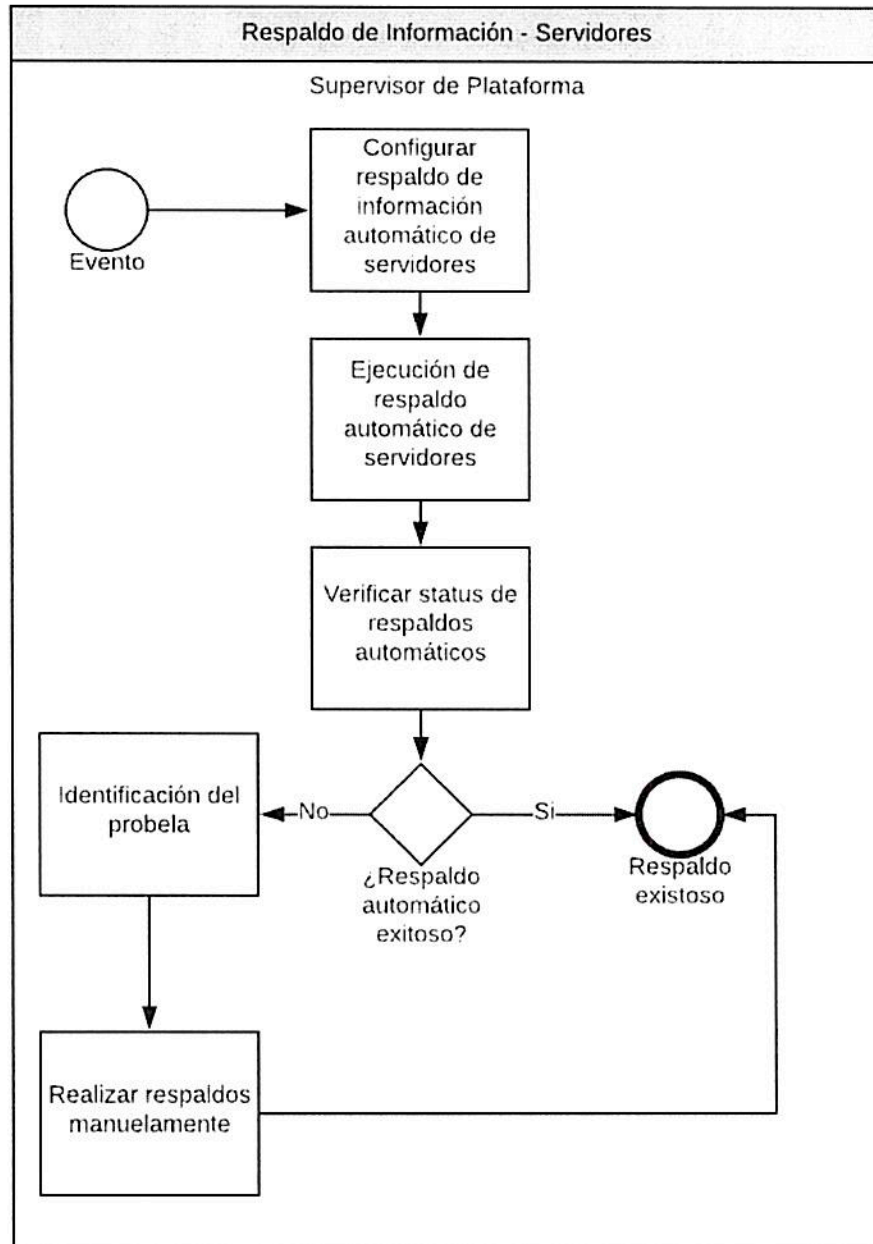
## 6.2 Directrices Generales para Respaldo de Estaciones de Trabajo.

Dado lo especificado en el punto anterior, en donde se declara que la información compartida para el trabajo diario, así como la información producida bajo este mismo contexto debe ser almacenada en las carpetas compartidas disponibilizadas por la Unidad de TIC, es que el procedimiento de respaldo de información para estaciones de trabajo responde a la necesidad o solicitud específica de realizar un respaldo completo e íntegro de la información contenida en los computadores de los colaboradores y colaboradoras de la Agencia.

## 7. Modo de Operación.

A continuación, se describen los flujos procedimentales para el respaldo de información contenida tanto en servidores como en estaciones de trabajo de la Agencia de Calidad de la Educación.

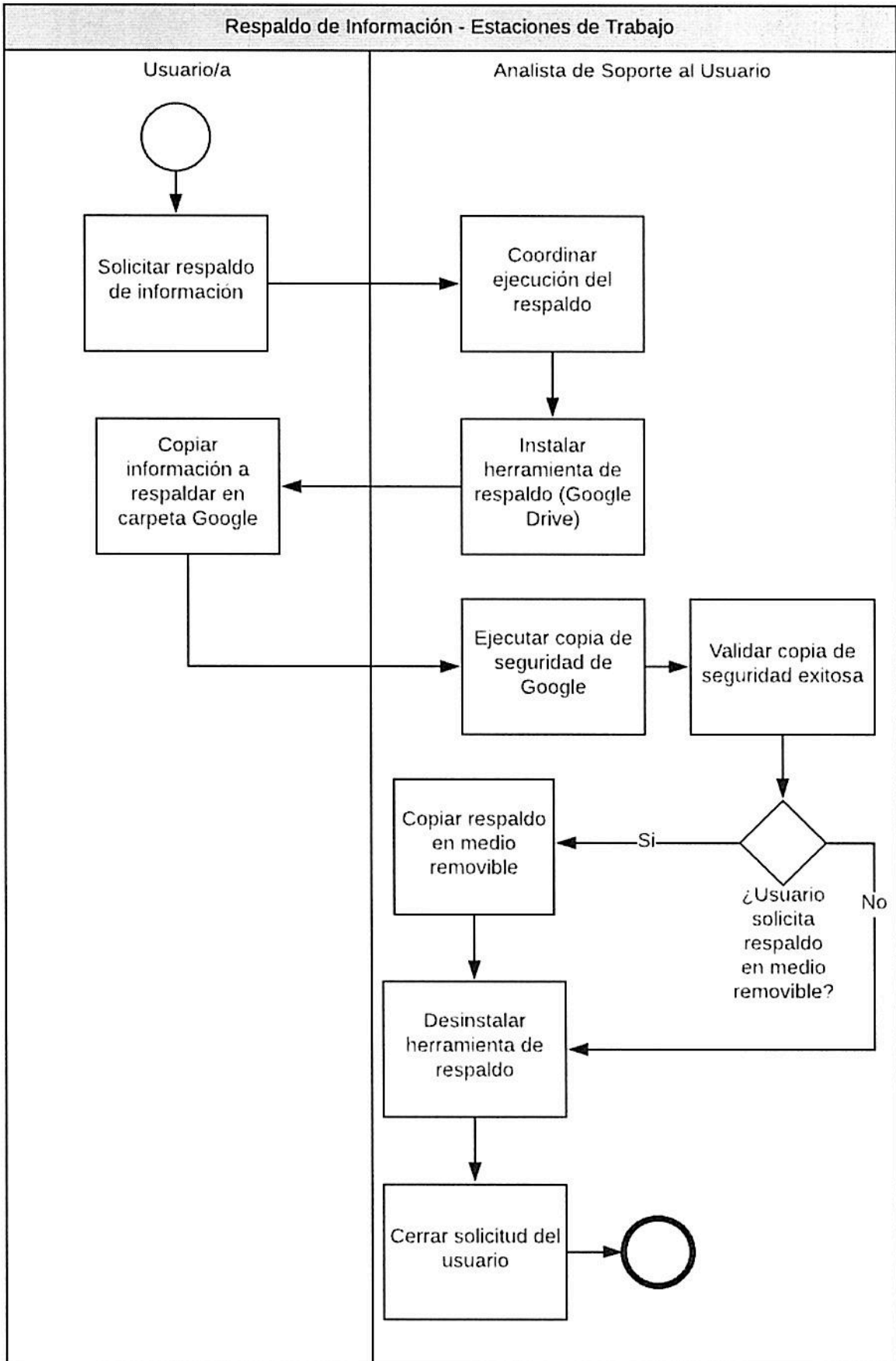
### 7.1 Flujo de Procedimiento para Respaldo de Servidores.



## 7.2 Matriz del Procedimiento para Respaldo de Servidores.

| ID | ACTIVIDAD   | DESCRIPCIÓN  | RESPONSABLE              | ID ACTIVIDAD SIGUIENTE |
|----|---|--|--------------------------|------------------------|
| 1  | Configurar respaldo de información automático de servidores | Se debe establecer la configuración sobre el sistema de información respectivo que ejecute de forma automatizada los respaldos de información de los servidores de la Agencia bajo las siguientes condiciones:<br>- Los respaldos se ejecutarán bajo una periodicidad diaria, al final de cada jornada.<br>- Los respaldos se realizarán con una base incremental diaria de 15 días hábiles, o tres (3) semanas laborales de cinco (5) días corridos en horario de 5x8.<br>- Se debe configurar el envío de un correo al Encargado de Plataforma, con copia a la Jefatura de Unidad de TIC, con el status de los respaldos una vez finalizada la ejecución de éstos, ya sea automática o manual. | Supervisor de Plataforma | 2                      |
| 2  | Ejecución de respaldo automático de servidores              | El respaldo de los servidores debe realizarse automáticamente según lo establecido en la actividad uno (1) de este procedimiento.  | Supervisor de Plataforma | 3                      |
| 3  | Verificar status de respaldos automáticos                   | Se debe revisar el reporte de status de respaldos entregado de forma automático según lo establecido en la actividad uno (1) de este procedimiento, para validar la correcta ejecución de éstos. Se pueden dar las siguientes alternativas:<br>- Los respaldos no se realizaron de forma exitosa (4).<br>- Los respaldos se ejecutaron de forma exitosa (FIN).   | Supervisor de Plataforma | 4 o FIN                |
| 4  | Identificación del problema                                 | Se debe identificar el por qué no se realizaron con éxito los respaldos y solucionar el impedimento.   | Supervisor de Plataforma | 4A                     |
| 4A | Realizar respaldos manuales                                 | Se debe realizar de forma manual el respaldo de el o los servidores sobre los cuales falló la ejecución del respaldo automático.   | Supervisor de Plataforma | 3                      |

**7.3 Flujo de Procedimiento para Respaldo de Estaciones de Trabajo.**



**7.4 Matriz del Procedimiento para Respaldo de Estaciones de Trabajo.**

| ID | ACTIVIDAD  | DESCRIPCIÓN  | RESPONSABLE                    | ID ACTIVIDAD SIGUIENTE |
|----|--|--|--------------------------------|------------------------|
| 1  | Solicitar respaldo de información                | <p>Toda petición de respaldo de la información contenida en un computador personal o activo de información de un usuario, debe ser solicitada al <i>área de Soporte</i> mediante el sistema de tickets de la organización. En éste se deben especificar la información que necesita respaldar, así como las características y condiciones que se deben considerar en el momento de efectuar el respaldo.</p> <p><b>NOTA:</b> En caso de requerir una copia del respaldo en medio removible, la solicitud debe ir acompañada del visto bueno de la jefatura correspondiente mediante solicitud firmada o correo electrónico, y autorizada por la Encargada de Seguridad de la Información. En caso de información de carácter reservada, debe incluirse la autorización de la Jefatura de División.</p> | Usuario/a                      | 2                      |
| 2  | Coordinar ejecución del respaldo                 | Se debe coordinar con el usuario solicitante, la realización del respaldo.   | Analista de Soporte al Usuario | 3                      |
| 3  | Instalar herramienta de respaldo (Google Drive)  | <p>Se debe instalar en la estación de trabajo del usuario, la herramienta de sincronización y respaldos de Google.</p> <p><b>NOTA:</b> Al momento de la instalación se solicitará acceso a la cuenta google en donde se desea almacenar el respaldo. Ésta será la cuenta de Soporte al Usuaio.</p>   | Analista de Soporte al Usuario | 4                      |
| 4  | Copiar información a respaldar en carpeta Google | Se debe copiar toda la información a respaldar en la carpeta de Google.  | Usuario                        | 5                      |
| 5  | Ejecutar la copia de seguridad de Google         | Se debe ejecutar la acción de copia de seguridad de la herramienta de Copia de Seguridad y Respaldo de Goolge.   | Analista de Soporte al Usuario | 6                      |

| ID | ACTIVIDAD                           | DESCRIPCIÓN   | RESPONSABLE                    | ID ACTIVIDAD SIGUIENTE |
|----|-------------------------------------|---|--------------------------------|------------------------|
| 6  | Validar copia de seguridad exitosa  | Se debe validar que la copia de seguridad se encuentre en la ubicación Google Drive de de la cuenta de Soporte al Usuario. Se pueden dar las siguientes opciones.<br>- El usuario solicitó copia del respaldo en medio removible (7).<br>- El usuario no solicitó copia de del respaldo en medio removible (8). | Analista de Soporte al Usuario | 7 O 8                  |
| 7  | Copiar respaldo en medio removible  | Previa validación de la existencia de las autorizaciones pertinentes, especificadas en la actividad uno (1) de este procedimiento, se procede a copiar el respaldo en un medio removible oficial de la institución.   | Analista de Soporte al Usuario | 8                      |
| 8  | Desinstalar herramienta de respaldo | Una vez realizado el respaldo de forma exitosa, se debe desinstalar la herramienta de Copia de Seguridad y Sincronización de Google.  | Analista de Soporte al Usuario | 9                      |
| 9  | Cerrar solicitud del usuario        | Se debe dar por cerrada la solicitud del usuario, con lo cual éste se dará por enterado de la ejecución exitosa de su solicitud.  | Analista de Soporte al Usuario | FIN                    |

### 7.5 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

De esta forma, la matriz de responsabilidades para respaldo de información en servidores, se estructura de la siguiente manera:

| ID | ACTIVIDAD   | ENC. SI | JEFE TIC | ENC. PLATAFORMA |
|----|---|---------|----------|-----------------|
| 1  | Configurar respaldo de información automático de servidores | I       | A        | R/E             |
| 2  | Ejecución de respaldo automático de servidores              | I       | I        | R               |
| 3  | Verificar status de respaldos automáticos                   | I       | A/C      | R/E             |
| 4  | Identificación del problema                                 | I       | I        | R               |
| 4A | Realizar respaldos manuales                                 | I       | I        | R               |

Así mismo, la matriz de responsabilidades para respaldos de estaciones de trabajo, se estructura de la siguiente manera:

| ID | ACTIVIDAD  | ENC. SI | JEFE/A | ENC. SOPORTE | USUARIO |
|----|--|---------|--------|--------------|---------|
| 1  | Solicitar respaldo de información                | I       | I      | I            | R/E     |
| 2  | Coordinar ejecución del respaldo                 | -       | -      | R/E          | R       |
| 3  | Instalar herramienta de respaldo (Google Drive)  | -       | -      | R/E          | R       |
| 4  | Copiar información a respaldar en carpeta Google | -       | -      | C            | R/E     |
| 5  | Ejecutar la copia de seguridad de Google         | -       | -      | R/E          | I       |
| 6  | Validar copia de seguridad exitosa               | -       | -      | R/E          | I       |
| 7  | Copiar respaldo en medio removible               | I       | I      | R/E          | -       |
| 8  | Desinstalar herramienta de respaldo              | -       | -      | R/E          | I       |
| 9  | Cerrar solicitud del usuario                     | I       | I      | R/E          | I       |

**8. Registro de Operación.**

| REGISTRO  | ID | RESPONSABLE/DUEÑO DEL REGISTRO | TIEMPO RETENCIÓN      | SOPORTE | LUGAR                      |
|---|----|--------------------------------|-----------------------|---------|----------------------------|
| Reporte de ejecución exitosa de respaldos de servidores                     | -  | Encargado de Plataforma        | 4 años / Archivo UTIC | Digital | PC Encargado de Plataforma |
| Reporte de tickets cerrados asociados a respaldos de estaciones de trabajo. | -  | Encargado de Soporte           | 4 años / Archivo UTIC | Digital | PC Encargado de Soporte    |

**Aprobado por:**

**Firma:**

**Fecha de Actualización:**

## 5. PROCEDIMIENTO DE CONTACTO CON GRUPOS DE INTERÉS.

| Procedimiento de Contacto con Grupos de Interés<br>Control A.06.01.04 |   |  |    |
|---|---|--|----|
| Tabla de Contenidos   |   |  |    |
| 1   | Objetivo.....   |  | 31 |
| 2   | Alcance.....  |  | 31 |
| 3   | Normas y Referencias.....   |  | 31 |
| 4   | Términos y Definiciones. ....   |  | 32 |
| 5.  | Roles y Responsabilidades .....                                       |  | 32 |
| 6.  | Grupos de Interés Especializados .....                                |  | 33 |
| 6.1   | Destinatarios de la información proveniente de grupos de interés..... |  | 34 |
| 7.  | Modo de Operación .....   |  | 34 |
| 7.1   | Flujo de Procedimiento. ....  |  | 34 |
| 7.2   | Matriz del Proceso de Contacto con grupos de interés especiales. .... |  | 35 |
| 7.3   | Matriz de Responsabilidades.....                                      |  | 36 |
| 8   | Registro de Operación.....  |  | 37 |

| REVISIONES DEL PROCEDIMIENTO |            |                       |                                  |
|------------------------------|------------|-----------------------|----------------------------------|
| Nº Versión                   | Fecha      | Motivo de la revisión | Páginas elaboradas o modificadas |
| Uno (1)                      | 28/05/2019 | Elaboración inicial   | Todas                            |

| ELABORADO POR  | VALIDACIÓN TÉCNICA                      | REVISADO POR   | APROBADO POR                       |
|--|---|--|------------------------------------|
| Sistema de Gestión de Seguridad de la Información y Ciberseguridad | Nicol Jeria Encargada de Ciberseguridad | Andrea Soto Araya Encargada de Seguridad de la Información | Comité de Seguridad de Información |

### 1. Objetivo.

El objetivo del presente documento es, en función de los objetivos de la Agencia de Calidad de la Educación, en adelante Agencia, establecidos en el Artículo 10 de la Ley 20.529, definir aquellos grupos de interés que puedan aportar con contenido relevante y concerniente a la seguridad de la información, a la elevación del nivel de madurez de la institución en estas temáticas. En base a lo anterior, se define un procedimiento formal y estructurado que permita canalizar esta información a las partes correspondientes al interior de la Agencia.

### 2. Alcance.

Este procedimiento deberá ser aplicado por todos(as) los(as) funcionarios internos de planta, contrata y personal honorarios que tengan incidencia directa en la recepción, canalización y/o difusión del contenido asociado a los grupos de interés definidos en el documento.

### 3. Normas y Referencias.

- Política General de Seguridad de la Información de la Agencia de Calidad de la Educación.
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información.

**4. Términos y Definiciones.**

|  |   |
|--|---|
| <b>Amenaza</b>                               | Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o una organización.  |
| <b>Riesgo</b>                                | Las condiciones de debilidad en los activos que pueden ser afectadas por la existencia de una amenaza concreta, y las consecuencias que esto tiene. Es el efecto o materialización de la amenaza, el cual se puede clasificar respecto de su severidad, considerando su nivel de probabilidad y el impacto que generaría su ocurrencia.   |
| <b>Autoridad</b>                             | Facultad o derecho que posee un individuo o conjunto de individuos para actuar, mandar, o exigir una determinada acción a otros, en virtud del poder que emana de su posición dentro de la organización o institución. En el caso del sistema de seguridad de la información serán entendidas como autoridades, los responsables de los procesos de continuidad del negocio y recuperación ante desastres; y los servicios de emergencia, salud, bomberos y carabineros.  |
| <b>Evento de Seguridad de la Información</b> | Se refiere a la identificación y materialización de una amenaza o riesgo detectado el cual pudiera eventualmente comprometer la continuidad operacional de la Agencia.  |
| <b>Incidente de Seguridad</b>                | Se refiere a la Identificación y materialización de una amenaza o riesgo detectado que afecte la continuidad operacional que afecte activos de información relevantes para la Agencia.  |
| <b>Vulnerabilidad</b>                        | Debilidades propias de las características propias de cada activo, que los exponen a una amenaza o riesgo.  |
| <b>Evento de Seguridad</b>                   | Se refiere a la identificación y materialización de una amenaza o riesgo detectado, que afecte la continuidad operacional dañando activos relevantes de la Agencia  |
| <b>Plan de Contingencia</b>                  | Plan de Acción donde se señala explícitamente, el procedimiento a seguir, ante la ocurrencia de un incidente de seguridad de la información, que comprometa la continuidad operacional de la Agencia.   |
| <b>Activos de Información</b>                | Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta manera es que se distingue la información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.), los equipos, sistemas, infraestructura que soportan esta información y las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales. |
| <b>Contactos críticos</b>                    | Corresponden al nivel de contacto que se necesita ubicar con urgencia en caso de dificultades tecnológicas o incidentes.  |
| <b>Red de Seguridad</b>                      | Corresponden a números telefónicos públicos de servicios de emergencia, que no referencian la identificación de una persona.  |
| <b>Seguridad de la Información</b>           | Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de informar, no repudio y confidencialidad.   |

**5. Roles y Responsabilidades.**

- f) **Encargada(o) de Seguridad de la Información:** Como Autoridad Interna líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), este rol tiene la responsabilidad de gestionar el contacto con los grupos de interés definidos por la Agencia, abarcando desde su definición de acuerdo a los tópicos que busque reforzar la institución, establecimiento del contacto de forma oficial a través de la institución, la recepción y canalización de la información recibida a las partes correspondientes.



- g) Encargada(o) de Seguridad de la Información:** Como Autoridad Interna perteneciente al Sistema de Gestión de Seguridad de Información y Ciberseguridad (SGSIC), enfocada en mantener la seguridad
- h) Jefatura de Unidad de Tecnologías de Información y Comunicación:** La jefatura de la Unidad TIC, como Autoridad Interna a cargo de velar por la mantención operativa de los servicios tecnológicos de la Agencia, se define como un rol crítico para la misma, por ende, precisa un constante flujo de información proveniente de grupos de interés especializados, referente a amenazas, vulnerabilidades y nuevas tendencias tecnológicas, tanto benignas como maliciosas que puedan afectar a la organización. Es por lo anterior, que será responsable de recibir y canalizar con su equipo, la información que se ajuste a las necesidades antes descritas.
- i) Jefaturas de División:** Las jefaturas de División, como Autoridades Internas que abarcan la mayor parte de los procesos críticos de la Agencia, y por ende la mayor parte de los colaboradores y colaboradoras de ésta, serán responsables de recibir y canalizar con la totalidad de las personas que componen sus procesos y ámbitos de responsabilidad, aquella información que provenga de grupos de interés especializados.

## **6. Grupos de Interés Especializados.**

A continuación, se establecen de forma general, las temáticas que, de acuerdo con los objetivos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, en adelante SGSIC, definidos en el numeral cinco (5) de la Política General de Seguridad de la Información, los tópicos sobre los cuales la Agencia declara que se deben mantener una constante actualización de conocimiento:

- j) Concientización en seguridad de información y ciberseguridad:** La Agencia de Calidad de la Educación, reconoce que las personas que componen la institución son cruciales para lograr una correcta disminución de la exposición a los riesgos de seguridad de información tanto actuales como futuros. Es por lo anterior, que el mantener un constante flujo de información que permita, en primer lugar, unificar el lenguaje de los colaboradores y colaboradoras bajo estas temáticas, y en segundo, concientizar sobre la importancia y cercanía que tiene esta temática, es crucial para mantener una evolución apropiada del SGSIC. Como Grupo de Interés enfocado en la generación de contenido como el descrito anteriormente, se define(n) el/los siguiente(s):
  - a. **Oficina de Seguridad del Internauta (OSI):** Boletines con material de concientización y evangelización en seguridad de información y ciberseguridad.
- k) Tendencias de Seguridad de Información y Ciberseguridad:** Es de suma importancia para la Agencia de Calidad de la Educación, que se reciba por parte de grupos de interés especializados, información sobre nuevas tendencias en protección de datos personales y consejos referentes a la protección de la organización frente a las cada vez comunes y especializadas amenazas del ciberespacio. Como Grupo de Interés enfocado en la generación de contenido como el descrito anteriormente, se define(n) el/los siguiente(s):
  - a. Instituto Nacional de Ciberseguridad de España (INCIBE): Boletines con material asociado a protección de empresas.
  - b. Webempresa.com: Boletines con material sobre nueva regulación de protección de datos personales (RGPD)
- l) Reporte de amenazas y vulnerabilidades:** Dado lo expresado en el numeral uno (1) de la Política General de Seguridad de Información, en donde se declara que la información es el activo de mayor relevancia para la Agencia de Calidad de la Educación, es indispensable mantener contacto con grupos de interés especializados que generen reportes periódicos sobre nuevas amenazas que pudiesen afectar los objetivos específicos del SGSIC. Como Grupo de Interés enfocado en la generación de contenido como el descrito anteriormente, se define(n) el/los siguiente(s):
  - a. Equipo de Respuesta ante Incidentes de Ciberseguridad del Gobierno de Chile (CSIRT-GOB)

### **6.1 Destinatarios de la información proveniente de grupos de interés.**

A continuación, se dan a conocer los destinatarios que a los cuales se deberán canalizar los boletines informativos recibidos de los grupos de interés descritos anteriormente:

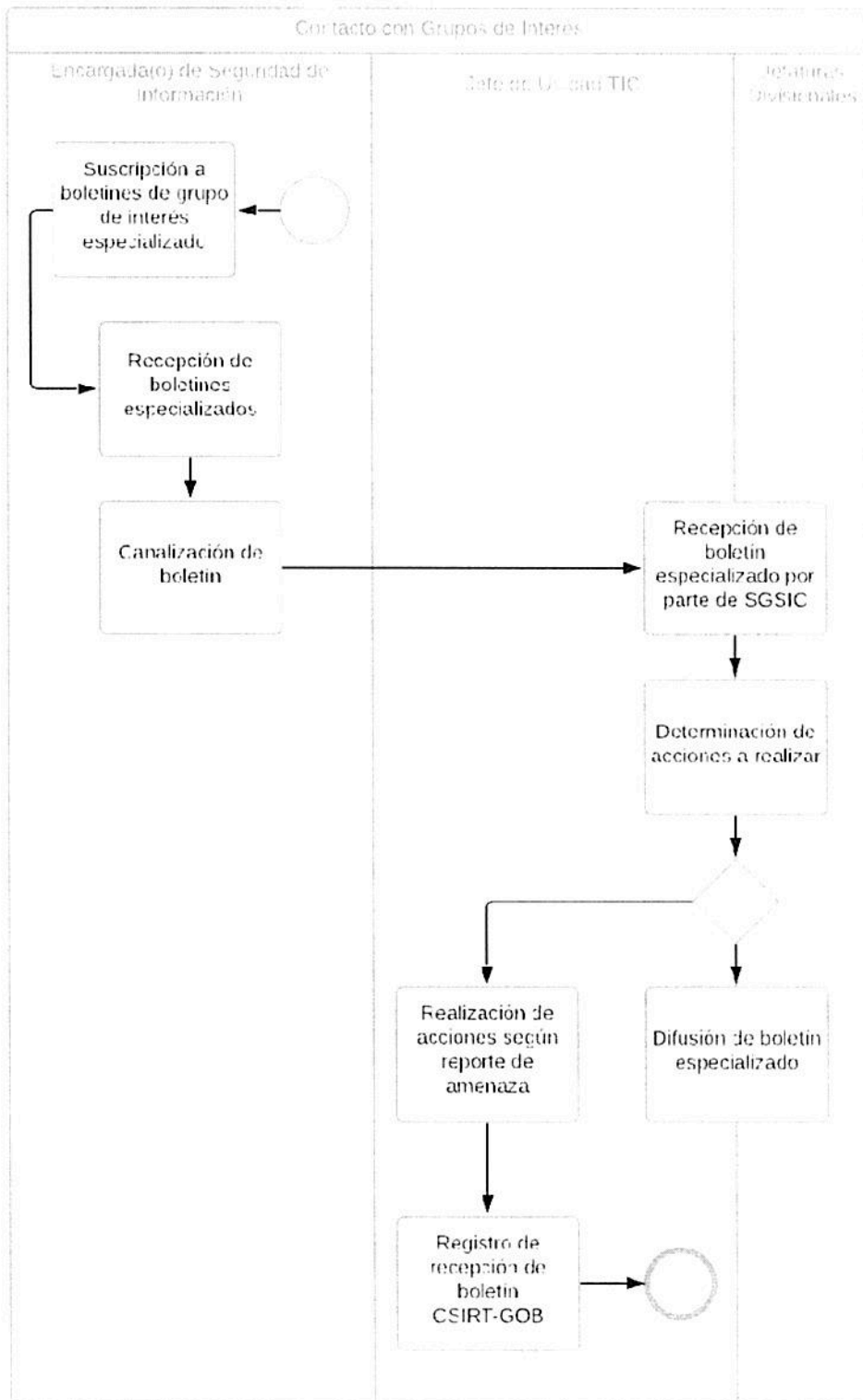
| <b>GRUPO DE INTERÉS</b> | <b>RECEPTOR</b>                         | <b>DESTINATARIO</b>  |
|-------------------------|---|--|
| <b>OSI</b>              | Encargada/o de Seguridad de Información | Jefaturas de División  |
| <b>INCIBE</b>           | Encargada/o de Seguridad de Información | Encargada/o de Seguridad de Información  |
| <b>WEBEMPRESA.COM</b>   | Encargada/o de Seguridad de Información | Encargada(o) de Seguridad de Información / Jefa Departamento Jurídico / Encargado(a) Transparencia |
| <b>CSIRT-GOB</b>        | Encargada/o de Ciberseguridad           | Jefatura Unidad TIC  |

Para estos efectos, es responsabilidad, en primer lugar, de la Encargada/o de Seguridad de la Información, el hacer recepción oficial de los boletines provenientes de los grupos de interés tipificados y canalizar con los destinatarios respectivos, mientras, que en segundo lugar, serán las Jefaturas de División, así como la Jefatura de la Unidad de Tecnologías de Información y Comunicación, los encargados de distribuir la información a las personas que se encuentren bajo su ámbito de responsabilidades según corresponda.

### **7. Modo de Operación.**

De acuerdo a los eventos descritos anteriormente, se establece un flujo comunicacional específico, en donde, de acuerdo al tipo de evento, se definen las autoridades pertinentes basado en su ámbito de responsabilidades. De esta forma, el flujo comunicacional es el siguiente:

#### **7.1 Flujo de Procedimiento.**



**7.2 Matriz del Proceso de Contacto con Grupos de Interés Especiales.**

| ID | ACTIVIDAD   | DESCRIPCIÓN   | RESPONSABLE                              | ID ACTIVIDAD SIGUIENTE |
|----|---|---|--|------------------------|
| 1  | Suscripción a boletines de grupo de interés especializado | Se debe realizar la suscripción respectiva para la recepción de los boletines de seguridad por parte de los grupos de interés especializados. Para lo anterior, se utilizará el correo institucional del Sistema de Gestión de Seguridad de Información y Ciberseguridad (seguridadinformacion@agenciaeducacion.cl) | Encargada(o) de Seguridad de Información | 2                      |

| ID | ACTIVIDAD  | DESCRIPCIÓN  | RESPONSABLE                                 | ID ACTIVIDAD SIGUIENTE |
|----|--|--|---|------------------------|
| 2  | Recepción de boletines especializados                  | Se debe hacer recepción de los boletines provenientes de los diferentes grupos de interés.   | Encargada(o) de Seguridad de Información    | 3                      |
| 3  | Canalización de boletín                                | Se debe hacer reenvío del boletín a aquellos roles asociados a las temáticas específicas del grupo de interés especializado remitente según lo especificado en el punto 6.1 del presente procedimiento.  | Encargada(o) de Seguridad de Información    | 4                      |
| 4  | Recepción de boletín especializado por parte del SGSIC | Se debe hacer recepción de del boletín de seguridad enviado por el SGSIC. Para oficializar la recepción, se debe responder un correo con el mensaje "Acuso Recibo."  | Jefe de Unidad TIC / Jefaturas Divisionales | 5                      |
| 5  | Determinación de acciones a realizar                   | Dada la naturaleza del boletín recibido, se pueden dar las siguientes opciones:<br>- Boletín no proveniente del CSIRT-GOB (6)<br>- Boletín de CSIRT-GOB (7)  | Jefe de Unidad TIC / Jefaturas Divisionales | 6 o 7                  |
| 6  | Difusión de boletín especializado                      | Se debe difundir el o los boletines de seguridad a todas aquellas personas que se encuentren bajo su ámbito de responsabilidades y/o formen parte de los procesos internos de la División/Unidad.  | Jefe de Unidad TIC / Jefaturas Divisionales | FIN                    |
| 7  | Realización de acciones según reporte de amenaza       | Se deben tomar todas las medidas necesarias para mitigar el riesgo de la amenaza reportada. Si bien éstas se encuentran indicadas en el boletín, se pueden complementar con acciones propias de la institución.<br><br><b>NOTA:</b> Para mayor detalle consultar procedimiento de gestión de incidentes seguridad de la información. | Jefe de Unidad TIC                          | 7A                     |
| 7A | Registro de recepción de boletín CSIRT-GOB             | Se debe hacer registro de la recepción del boletín en la Planilla de Recepción de Alertas de Seguridad.  | Jefe de Unidad TIC                          | FIN                    |

### 7.3 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

De esta forma, la matriz de responsabilidades se estructura de la siguiente manera:

| ID | ACTIVIDAD   | ENCARGAD A SI | JEFE TIC | JEFES DIVISI ÓN | EQUIP O TIC |
|----|---|---------------|----------|-----------------|-------------|
| 1  | Suscripción a boletines de grupo de interés especializado | R             | I/C      | I/C             | I           |
| 2  | Recepción de boletines especializados                     | R             | -        | -               | -           |
| 3  | Canalización de boletín                                   | R             | I        | I               | -           |
| 4  | Recepción de boletín especializado por parte del SGSIC    | C/I           | R        | R               | -           |
| 5  | Determinación de acciones a realizar                      | C/I           | R        | -               | C/I         |
| 6  | Difusión de boletín especializado                         | C/I           | R        | R               | I           |
| 7  | Realización de acciones según reporte de amenaza          | C/I           | R/A      | -               | E           |
| 7A | Registro de recepción de boletín CSIRT-GOB                | C/I           | R/A/C    | -               | E           |

**8. Registro de Operación.**

| <b>REGISTRO</b>   | <b>ID</b> | <b>RESPONSABLE/DUEÑO DEL REGISTRO</b>       | <b>TIEMPO DE RETENCIÓN</b> | <b>SOPORTE</b> | <b>LUGAR</b>                |
|---|-----------|---|----------------------------|----------------|-----------------------------|
| Registro de recepción de alertas de seguridad CSIRT-GOB   | -         | Encargado(a) de Seguridad de la Información | 4 años / Archivo UTIC      | Digital        | PC Responsable del Registro |
| Evidencia de suscripción a boletines de grupos de interés | -         | Encargado(a) de Seguridad de la Información | 4 años / Archivo UTIC      | Digital        | PC Responsable del Registro |

## **6. PROCEDIMIENTO DE ELABORACIÓN/ACTUALIZACIÓN DE INVENTARIO DE ACTIVOS.**

| <b>Procedimiento de Elaboración/Actualización de Inventario de Activos<br/>Control A.08.01.01</b> |  |
|---|--|
| <b>Tabla de Contenidos</b>  |  |
| <b>1</b>  | <b>Objetivo..... 38</b>  |
| <b>2</b>  | <b>Alcance..... 38</b>   |
| <b>3</b>  | <b>Normas y Referencias..... 39</b>  |
| <b>4</b>  | <b>Términos y Definiciones. .... 39</b>  |
| <b>5.</b>   | <b>Roles y Responsabilidades ..... 39</b>  |
| <b>6.</b>   | <b>Definiciones para la Construcción/Actualización del Inventario de Activos ..... 40</b>                        |
| <b>7.</b>   | <b>Modo de Operación ..... 41</b>  |
| <b>7.1</b>  | <b>Flujo de Procedimiento para Elaboración/Actualización del Inventario de Activos de Información..... 41</b>    |
| <b>7.2</b>  | <b>Matriz del Procedimiento para Elaboración/Actualización del Inventario de Activos de Información ..... 42</b> |
| <b>7.3</b>  | <b>Matriz de Responsabilidades..... 44</b>   |
| <b>8.</b>   | <b>Registro de Operación..... 44</b>   |

### **REVISIONES DEL PROCEDIMIENTO**

| <b>Nº Versión</b> | <b>Fecha</b> | <b>Motivo de la revisión</b> | <b>Páginas elaboradas o modificadas</b> |
|-------------------|--------------|------------------------------|---|
| Cero (0)          | 28/06/2019   | Elaboración inicial          | Todas                                   |

| <b>ELABORADO POR</b>  | <b>VALIDACIÓN TÉCNICA</b>                      | <b>APROBADO POR</b>   | <b>APROBADO POR</b>    |
|---|--|---|------------------------|
| <b>Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC)</b> | <b>Nicol Jeria Encargada de Ciberseguridad</b> | <b>Andrea Soto Araya Encargada de Seguridad de la Información</b> | <b>Comité de SGSIC</b> |

### **1. Objetivo.**

Según la declaración institucional efectuada en la Política General de Seguridad de Información y Ciberseguridad por la Agencia de Calidad de la Educación, en adelante la Agencia, donde ésta reconoce los activos de información como el activo más crítico para el cumplimiento de su misión institucional, y, por ende, comprende la necesidad de robustecer y mantener en constante mejora su ambiente de control, el objetivo de este procedimiento es establecer las actividades y la secuencia de acciones para la construcción y actualización del inventario de activos de información de la Agencia.

### **2. Alcance.**

Lo establecido en este procedimiento, debe aplicarse para toda la información, independiente de su formato o medio de almacenamiento, que sea creada, almacenada y/o tratada como resultado de la operación de la Agencia, o como consecuencia del cumplimiento de su misión institucional.

Así mismo, el alcance circunscrito para este procedimiento, abarca tanto la formulación desde cero de dicho inventario, así como su constante actualización. En donde independiente de las condiciones antes mencionadas en las cuales se esté ejecutando este procedimiento, se considerará la clasificación de los activos de información según su criticidad en las dimensiones de Confidencialidad, Disponibilidad, Integridad y Privacidad.

De esta forma, y, en concordancia con lo establecido en le NCh ISO 27002:2013, el presente documento tiene su alcance sobre los siguientes controles:

- A.08.01.01 – Inventario de Activos
- A.08.02.01 – Clasificación de Activos

### 3. Normas y Referencias.

- NCh ISO 27001:2013.
- NCh ISO 27002:2013.
- Política General de Seguridad de la Información y Ciberseguridad, Agencia de Calidad de la Educación.
- Estructura Funcional del Sistema de Gestión de Seguridad de Información y Ciberseguridad, Agencia de Calidad de la Educación.

### 4. Términos y Definiciones.

|                                       |   |
|---------------------------------------|---|
| <b>Contraseña:</b>                    | Autenticación del usuario que utiliza información   |
| <b>Active Directory (AD)</b>          | Es el sistema de Directorio que posee la Agencia y que gestiona la Unidad TIC para identificar a todos los usuarios con el objetivo de administrar los inicios de sesión de los equipos en red.   |
| <b>Sistemas Informáticos</b>          | Sistemas que permiten almacenar y procesar información.   |
| <b>Acceso a la información</b>        | Derecho que tiene un usuario para buscar, recibir y difundir información del Servicio.  |
| <b>Restringir el acceso</b>           | Delimitar el acceso de los funcionarios (as), servidores públicos a honorarios y terceras partes a determinados recursos.   |
| <b>Estación de Trabajo</b>            | Es un computador que facilita a los usuarios (as) el acceso a los servidores y periféricos de la red.   |
| <b>Autenticación</b>                  | Proceso de confirmación de la identidad del (de la) usuario (a) que utiliza un sistema informático.   |
| <b>Identificador de autenticación</b> | Mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos.  |
| <b>Autenticar (o autenticar)</b>      | Se refiere a comprobar que esa persona es quien dice ser. Ello se logra cuando se cotejan uno o más datos en dicha identificación oficial contra (i) los datos en alguna otra identificación, documento, certificado digital (como el de la firma electrónica) o dispositivo que tenga la persona, (ii) los datos que sepa o tenga memorizados (su firma autógrafa o su contraseña, por ejemplo) o (iii) una o más características que coincidan con lo que es dicha persona (fotografía o huella dactilar, por ejemplo). |
| <b>Autorizar</b>                      | Se refiere al acceso que se le permite a la persona que se ha identificado y autenticado apropiadamente.  |
| <b>Identificador Único Global</b>     | Abreviado bajo la sigla Guid es una implementación del sistema Active Directory que permite que cada usuario sea único e irrepetible.   |

### 5. Roles y Responsabilidades.

- Encargada(o) de Seguridad de la Información:** Como líder del SGSIC, este rol será el encargado de supervisar la correcta ejecución de este procedimiento, así como la constante actualización del inventario de activos de información. Debe garantizar la correcta ejecución de éste procedimiento, tomando un rol consultor o asesor para impulsar la correcta y oportuna elaboración y/o actualización del inventario de activos de información consolidado de la Agencia.
- Encargada(o) de Ciberseguridad:** Este rol será responsable de apoyar directamente en la elaboración y mantención actualizada del inventario de activos de información de la Agencia de Calidad de la Educación.
- Jefatura de Unidad de Tecnologías de Información y Comunicación:** Será este rol el encargado de mantener y proveer a la Encargada(o) de Seguridad de la Información un inventario de activos tecnológicos actualizado, con la finalidad de ser un insumo para el inventario de activos de información de la Agencia.
- Propietario de Activos:** Serán estos roles los encargados de elaborar y mantener actualizado de un inventario de aquellos activos de información que se encuentran bajo su gestión, y por ende, bajo su ámbito de responsabilidades. Éste inventario de activos

constituye un insumo de gran importancia para la conformación del inventario de activos de la organización.

## **6. Definiciones para la Construcción/Actualización del Inventario de Activos.**

Para dar con el cumplimiento tanto del objetivo de este documento como con los objetivos estratégicos del Sistema de Gestión de Seguridad de la Información (SGSIC), se deberá elaborar y mantener actualizado un inventario de activos de información institucional, el cual considera la totalidad de activos de esta índole de la Agencia de Calidad de la Educación.

Para lo anterior, y en concordancia con la responsabilidad atribuida en la Estructura Funcional del SGSIC, serán los Propietarios de los Activos de Información, los encargados de cada uno proveer el Inventario de los Activos de Información que se encuentran bajo su gestión. De esta forma, el consolidado de éstos conformará el Inventario de Activos Institucional. Es así, como cada Inventario de Activos de los Propietarios de los Activos debe considerar:

- a. Un levantamiento o identificación de activos de información.
- b. Asignación de nombre único a cada activo de información. Se debe considerar que éste debe ser pensado para su mantención en el tiempo, por ende, debe estar relacionado lo más posible con el nombre que se le da a diario en la operación del proceso o unidad de negocio que soporta.
- c. Descripción funcional de cada activo de información. En otras palabras, debe considerar una descripción que especifique la función y relevancia que cumple cada activo para el proceso o unidad de negocio que soporta.
- d. Asociación con tecnología. Se debe establecer el medio tecnológico sobre el cual es almacenado o tratado cada activo de información. Para lo anterior se deben considerar, herramientas o sistemas web, carpetas compartidas, repositorios de almacenamiento de información, medios removibles, servidores, etc.
- e. Finalmente, se debe clasificar cada activo de información de acuerdo a sus niveles de criticidad en aspectos de Confidencialidad, Disponibilidad, Integridad y Privacidad.

De forma particular, para la clasificación de los activos de información se deben tener en cuenta los siguientes niveles de criticidad:

| <b>DIMENSIÓN</b> | <b>DESCRIPCIÓN</b>   | <b>NIVEL CRITICIDAD</b> | <b>DESCRIPCIÓN</b>   | <b>EJEMPLOS</b> |
|------------------|--|-------------------------|--|-----------------|
| Conf.            | Hace referencia al nivel de secreto o resguardo que debe tener un activo de información en específico. Frente a esto se debe responder siguiente la pregunta ¿Cuán secreto debe ser este activo para mantener la confidencialidad de la información que fluye por el área/proceso? | Alto                    | Información a la que tienen acceso únicamente los miembros de un grupo reducido dentro de la organización.                       |                 |
|                  |  | Medio                   | Información a la que tienen acceso únicamente los miembros de la organización.   |                 |
|                  |  | Bajo                    | Información de carácter público a la que tienen acceso tanto los miembros de la organización como aquellos que no lo son.        |                 |
| Disp.            | Hace referencia a la necesidad de consulta o dependencia en el uso del activo de información dentro del área/proceso. Frente a esto el rol debe intentar contestar la pregunta ¿Qué tan necesario es el acceso al activo para el funcionamiento del área/proceso?                  | Alto                    | La indisponibilidad de estos activos genera consecuencias de tipo negativo inmediatas para la operación normal del área/proceso. |                 |



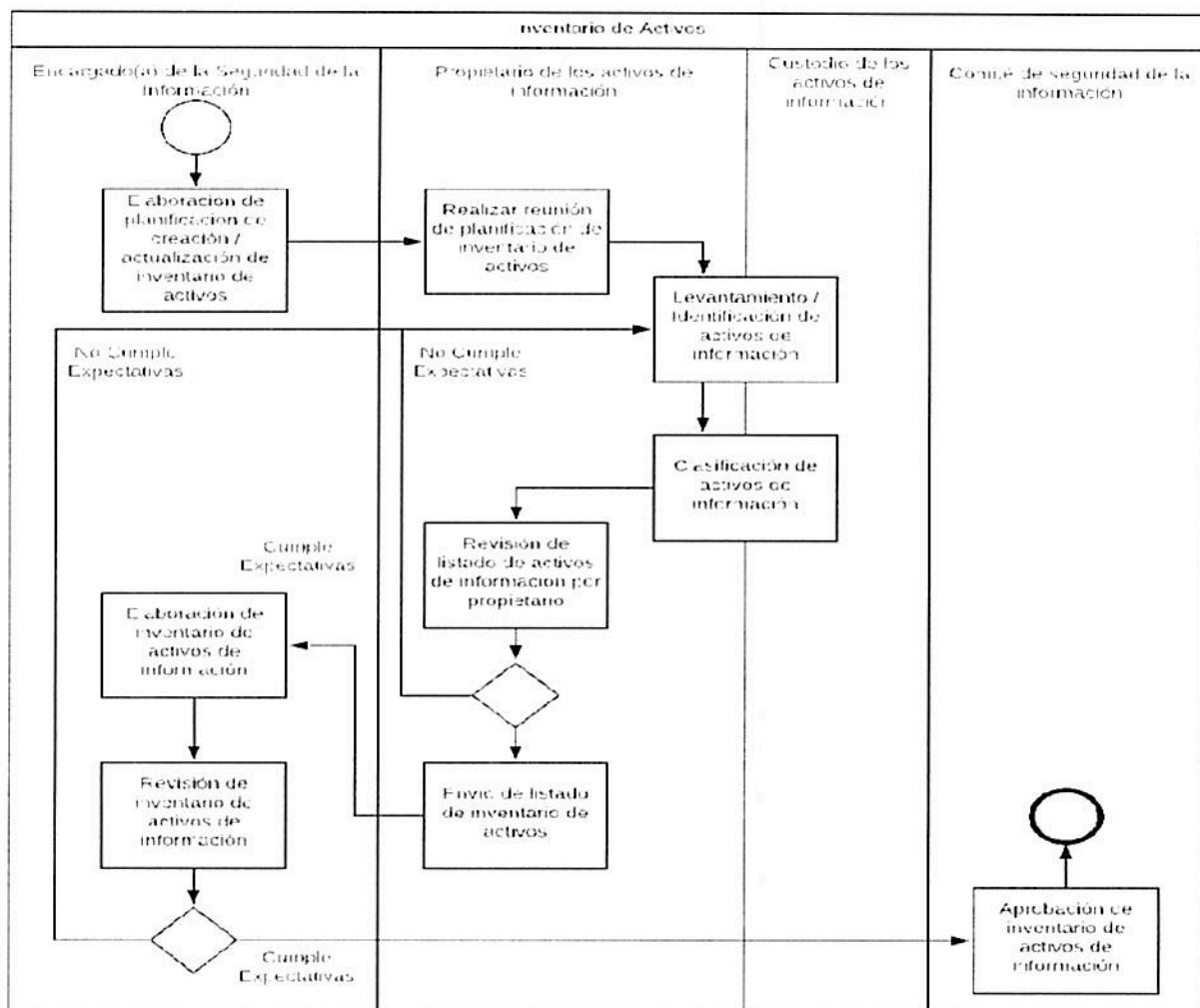
| DIMENSIÓN | DESCRIPCIÓN  | NIVEL CRITICIDAD | DESCRIPCIÓN   | EJEMPLOS |
|-----------|--|------------------|---|----------|
|           |  | Medio            | La indisponibilidad de estos activos tolerable por un corto periodo de tiempo antes de generar consecuencias negativas para la operación normal del área/proceso. |          |
|           |  | Bajo             | La indisponibilidad de estos activos solo generara consecuencias negativas para el área/proceso que soporta en el mediano-largo plazo.                            |          |
| Int.      | Hace referencia a que la información no contenga errores y/o modificaciones no autorizadas. Para esta clasificación se deben considerar aquellos activos relevantes para la elaboración de otros activos, reportes, informes y/o toma de decisiones al interior de la organización.    | Alto             | La integridad es relevante para la elaboración de otros activos de información importantes para la operación normal del área/proceso                              |          |
|           |  | Bajo             | La integridad no es relevante para la elaboración de otros activos de información importantes para la operación normal del área/proceso.                          |          |
| Priv.     | Este atributo hace referencia a cuán importante es que un activo no pueda ser individualizado o relacionado a una persona. Para poder clasificar el activo, el rol debe preguntarse ¿cuán importante es que la información no pueda ser individualizada en el caso de hacerse pública? | Alto             | Se debe velar por la NO individualización de la información contenida en el activo  |          |
|           |  | Bajo             | La individualización de la información contenida en el activo no es una característica por la cual se deba velar  |          |

Finalmente, se entenderá por "Activo de Información", a la información que, como producto de su operación, genera, almacena, trata y/o transita por los procesos de la Agencia de Calidad de la Educación, independiente de su formato o medio de almacenamiento.

## **7. Modo de Operación.**

A continuación, se describen los flujos procedimentales para la elaboración y actualización del inventario de activos de la Agencia de Calidad de la Educación.

### **7.1 Flujo de Procedimiento para Elaboración/Actualización del Inventario de Activos de Información.**



## 7.2 Matriz del Procedimiento para Elaboración/Actualización del Inventario de Activos de Información.

| ID | ACTIVIDAD   | DESCRIPCIÓN   | RESPONSABLE                                  | ID ACTIVIDAD SIGUIENTE |
|----|---|---|--|------------------------|
| 1  | Elaboración de planificación de creación / actualización de inventario de activos | El/La Encargada(o) de Seguridad de la Información debe elaborar una planificación del proceso de creación/actualización del inventario de activos de información de la Agencia. Esta planificación debe realizarse al menos una vez al año calendario, y debe ser enviada a la totalidad de los roles propietarios de activos de la institución para que puedan alinearse a ésta. | Encargada(o) de Seguridad de la Información  | 2                      |
| 2  | Realizar reunión de planificación de inventario de activos                        | Tanto el propietario, como sus custodios designados, deben realizar una reunión con el objetivo de relacionar los activos de información que deben formar parte del inventario.   | Propietario(a) de los activos de información | 3                      |

| ID | ACTIVIDAD   | DESCRIPCIÓN   | RESPONSABLE                                       | ID ACTIVIDAD SIGUIENTE |
|----|---|---|---|------------------------|
| 3  | Levantamiento/Identificación de Activos de Información        | Se debe realizar el levantamiento de activos de información inicial y conformar un listado de activos de información que contenga su nombre, propietario, división, descripción funcional, ubicación y/o medio de almacenamiento.<br><br><b>NOTA:</b> Si ya existe un listado de activos de información, esta actividad tendrá carácter de actualización para éste. | Propietario(a)/Custodio de Activos de Información | 4                      |
| 4  | Clasificación de activos de información                       | Una vez elaborada/actualizada la lista de los activos de información bajo la gestión del Propietario de Activos, se debe realizar la clasificación de éstos según la criticidad que tengan en los objetivos del SGSIC, establecidos en la Política General de Seguridad de Información.   | Propietario(a)/Custodio de Activos de Información | 5                      |
| 5  | Revisión de Listado de Activos de Información por Propietario | Se debe validar el listado de activos de información.<br>Se pueden dar las siguientes opciones:<br>- El Listado de Inventario de Activos de Información no cumple con las expectativas (3)<br>- El Listado de Inventario de Activos de Información cumple con las expectativas (6)  | Propietario(a) de Activos de Información          | 3 o 6                  |
| 6  | Envío de listado de inventario de activos                     | Se debe enviar el listado de activos de información al/la Encargada(o) de Seguridad de Información.   | Propietario(a) de Activos de Información          | 7                      |
| 7  | Elaboración de inventario de activos de información           | Se deben consolidar los listados de activos de información recibidos por parte de los Propietarios de los Activos, en el documento "[años]_SGSIC-RO-A.8.1.1_InventarioActivosInformacion".  | Encargada(o) de Seguridad de Información          | 8                      |
| 8  | Revisión de inventario de activos de información              | Se debe revisar y validar el inventario de activos de información recién elaborado. Se pueden dar las siguientes alternativas:<br>- El Listado de Inventario de Activos de Información no cumple con las expectativas (3)<br>- El Listado de Inventario de Activos de Información cumple con las expectativas (9)   | Encargada(o) de Seguridad de Información          | 3 o 9                  |

| ID | ACTIVIDAD  | DESCRIPCIÓN   | RESPONSABLE                        | ID ACTIVIDAD SIGUIENTE |
|----|--|---|------------------------------------|------------------------|
| 9  | Aprobación de inventario de activos de información | El inventario de activos de información debe ser aprobado en sesión del Comité de Seguridad de Información. Se pueden dar las siguientes alternativas:<br>- El Listado de Inventario de Activos de Información no cumple con las expectativas (8)<br>- El Listado de Inventario de Activos de Información cumple con las expectativas (FIN) | Comité de Seguridad de Información | 8 o FIN                |

### 7.3 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

Se esta forma, la matriz de responsabilidades se estructura de la siguiente manera:

| ID | ACTIVIDAD   | PROPIETARIO O ACTIVO | CUSTODIO ACTIVO | ENCARGADO A SI | COMITÉ SEGURIDAD |
|----|---|----------------------|-----------------|----------------|------------------|
| 1  | Elaboración de planificación de creación / actualización de inventario de activos | -                    | I               | R/E            | I                |
| 2  | Realizar reunión de planificación de inventario de activos                        | R                    | C               | I              | -                |
| 3  | Levantamiento/Identificación de Activos de Información                            | R/E                  | E               | C              | -                |
| 4  | Clasificación de activos de información   | R/E                  | E               | C              | -                |
| 5  | Revisión de Listado de Activos de Información por Propietario                     | R/E                  | I/C             | C              | -                |
| 6  | Envío de listado de inventario de activos   | R/E                  | I               | I              | -                |
| 7  | Elaboración de inventario de activos de información                               | C                    | -               | R/E            | -                |
| 8  | Revisión de inventario de activos de información                                  | C                    | -               | R/E            | I                |
| 9  | Aprobación de inventario de activos de información                                | I                    | I               | I/C            | R/E              |

### 8. Registro de Operación.

| REGISTRO                             | ID | RESPONSABLE/DUEÑO DEL REGISTRO               | TIEMPO RETENCIÓN      | SOPORTE | LUGAR |
|--------------------------------------|----|--|-----------------------|---------|-------|
| Inventario de Activos de Información | -  | Encargada(o) de Seguridad de la Información. | 4 años / Archivo UTIC | Digital | PC    |

## 7. PROCEDIMIENTO DE INICIO DE SESIÓN SEGURO.

| Procedimiento de Inicio de Sesión Seguro<br>Control A.09.04.02 |   |
|--|---|
| Tabla de Contenidos  |   |
| 1  | Objetivo..... 45  |
| 2  | Alcance..... 45   |
| 3  | Normas y Referencias..... 45                                  |
| 4  | Términos y Definiciones. .... 46                              |
| 5.   | Roles y Responsabilidades ..... 46                            |
| 6.   | Directrices Generales para el inicio de sesión seguro..... 46 |
| 7.   | Modo de Operación ..... 47                                    |
| 7.1  | Flujo de Procedimiento para Inicio de Sesión Seguro..... 47   |
| 7.2  | Matriz del Procedimiento para Inicio de Sesión Seguro..... 48 |
| 7.3  | Matriz de Responsabilidades..... 48                           |
| 8.   | Registro de Operación. .... 48                                |

### REVISIONES DEL PROCEDIMIENTO

| Nº Versión | Fecha      | Motivo de la revisión | Páginas elaboradas o modificadas |
|------------|------------|-----------------------|----------------------------------|
| Cero (0)   | 31/05/2019 | Elaboración inicial   | Todas                            |

| ELABORADO POR  | VALIDACIÓN TÉCNICA             | APROBADO POR  | APROBADO POR    |
|--|--------------------------------|---|-----------------|
| Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC) | Patrik Soto<br>Jefe Unidad TIC | Andrea Soto Araya<br>Encargada de Seguridad de la Información | Comité de SGSIC |

### 1. Objetivo.

En función de los objetivos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), declarado en la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, en adelante la Agencia, el presente documento tiene por objetivo establecer y definir las actividades necesarias que permitan aplicar las reglas de acceso a las estaciones de trabajo de propiedad del servicio.

### 2. Alcance.

Este procedimiento deberá ser aplicado por todos(as) los(as) funcionarios(as) de planta y contrata, personal a honorarios y toda aquella persona natural o jurídica que preste servicios (terceros y proveedores) y que, a raíz de ello, tengan acceso a estaciones de trabajo de la Agencia y por consiguiente, tenga acceso a información del servicio.

### 3. Normas y Referencias.

- Política General de Seguridad de la Información de la Agencia de Calidad de la Educación
- Política de Gestión de usuarios y Contraseñas
- Procedimiento de Entrega de Acceso a los Usuarios
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información

#### 4. Términos y Definiciones.

|                                       |   |
|---------------------------------------|---|
| <b>Contraseña:</b>                    | Autenticación del usuario que utiliza información   |
| <b>Active Directory (AD)</b>          | Es el sistema de Directorio que posee la Agencia y que gestiona la Unidad TIC para identificar a todos los usuarios con el objetivo de administrar los inicios de sesión de los equipos en red.   |
| <b>Sistemas Informáticos</b>          | Sistemas que permiten almacenar y procesar información.   |
| <b>Acceso a la información</b>        | Derecho que tiene un usuario para buscar, recibir y difundir información del Servicio.  |
| <b>Restringir el acceso</b>           | Delimitar el acceso de los funcionarios (as), servidores públicos a honorarios y terceras partes a determinados recursos.   |
| <b>Estación de Trabajo</b>            | Es un computador que facilita a los usuarios (as) el acceso a los servidores y periféricos de la red.   |
| <b>Autenticación</b>                  | Proceso de confirmación de la identidad del (de la) usuario (a) que utiliza un sistema informático.   |
| <b>Identificador de autenticación</b> | Mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos.  |
| <b>Autenticar (o autenticar)</b>      | Se refiere a comprobar que esa persona es quien dice ser. Ello se logra cuando se cotejan uno o más datos en dicha identificación oficial contra (i) los datos en alguna otra identificación, documento, certificado digital (como el de la firma electrónica) o dispositivo que tenga la persona, (ii) los datos que sepa o tenga memorizados (su firma autógrafa o su contraseña, por ejemplo) o (iii) una o más características que coincidan con lo que es dicha persona (fotografía o huella dactilar, por ejemplo). |
| <b>Autorizar</b>                      | Se refiere al acceso que se le permite a la persona que se ha identificado y autenticado apropiadamente.  |
| <b>Identificador Único Global</b>     | Abreviado bajo la sigla Guid es una implementación del sistema Active Directory que permite que cada usuario sea único e irrepetible.   |

#### 5. Roles y Responsabilidades

- a) **Encargada(o) de Seguridad de la Información:** Como líder del SGSIC, este rol será el encargado de velar por el cumplimiento de este procedimiento.
- b) **Usuario:** Responsable de recordar e ingresar sus credenciales de inicio de sesión con éxito.
- c) **Jefatura de Unidad de Tecnologías de Información y Comunicación:** Será responsable de garantizar la ejecución de este procedimiento, así como de determinar el método técnico de protección adecuado para el acceso a la información. Además, será el encargado de entregar las directrices necesarias para su mejora continua en el tiempo.
- d) **Encargado de Plataforma y Operaciones TI:** Será éste el rol responsable de implementar, administrar y mantener las medidas de seguridad técnicas para proveer control de acceso a las estaciones de trabajo de la Agencia.

#### 6. Directrices Generales para el inicio de sesión seguro.

Se debe tener en cuenta, que si bien, de forma previa a la ejecución de este procedimiento, el perfilamiento de privilegios de acceso a la información se efectúa basado en roles según lo indicado en la Política de Gestión de Usuarios y Contraseñas, se pueden solicitar accesos específicos según las necesidades de la División, Departamento o Unidad a la que pertenezca el usuario o usuaria que requiere el acceso, según lo detallado en el Procedimiento de Entrega de Acceso a los Usuarios.

Para la autenticación e identificación de todos los usuarios de la agencia, se definió la utilización de un sistema de Directorio, específicamente MS Active Directory, en adelante AD, el cual permite localizar el acceso a la red del servicio, con el fin de facilitar su localización y administración.

Así mismo, con respecto al acceso a los sistemas, el personal para ingresar a un computador o a la red de Trabajo de la Agencia, deberá autenticarse e ingresar su usuario y contraseña de AD, con ello es reconocido (al ser identificador único) por los Sistemas Informáticos de la Agencia. Este acceso es la única puerta de entrada a todos los sistemas e información de la institución.

El sistema AD cumple una serie de requisitos que permiten respaldar la generación de identificadores de usuarios, considerando que todas las acciones parten de la base del identificador único global, siendo éste irrepetible. Este identificador se genera cuando un usuario es creado por la Unidad de

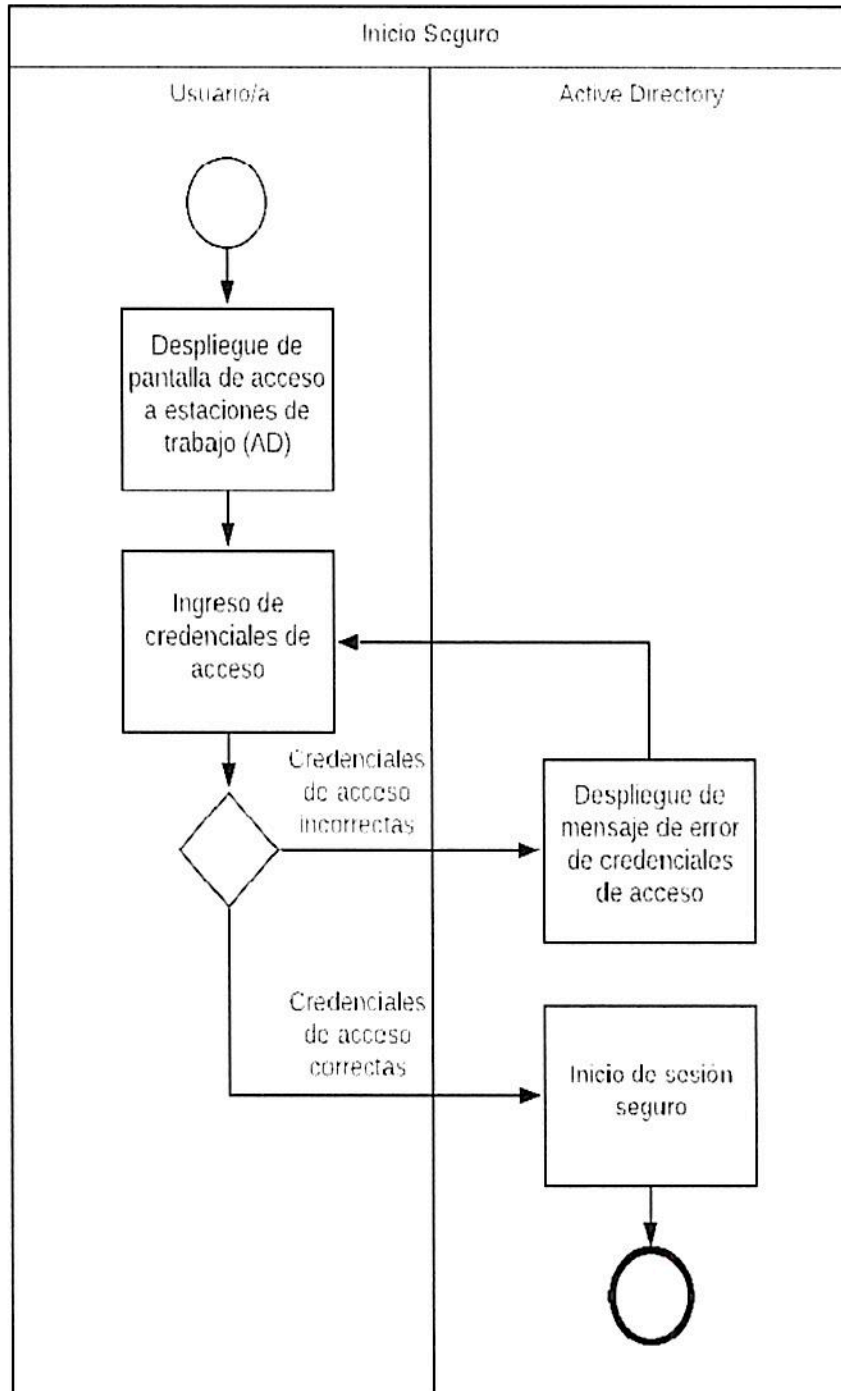
Tecnologías de la Información en el AD. De esta forma, si el equipo de un usuario se encuentra en red, la Unidad TIC mediante controladores de dominio asignará una IP para identificar sus actividades.

El sistema AD permite que un usuario pueda ingresar al sistema independiente del punto físico donde se encuentre, accediendo ya sea desde Nivel Central o Macrozonas, como también permite ingresar por diversos equipos computacionales a los sistemas de la Agencia.

### 7. Modo de Operación.

A continuación, se describen los flujos procedimentales para el inicio de sesión seguro en estaciones de trabajo de la Agencia de Calidad de la Educación.

#### 7.1 Flujo de Procedimiento para Inicio de Sesión Seguro.



**7.2 Matriz del Procedimiento para Inicio de Sesión Seguro.**

| ID | ACTIVIDAD   | DESCRIPCIÓN  | RESPONSABLE      | ID ACTIVIDAD SIGUIENTE |
|----|---|--|------------------|------------------------|
| 1  | Despliegue de pantalla de acceso a estaciones de trabajo (AD) | Al momento de encender una estación de trabajo el sistema AD mostrará una pantalla con las indicaciones para desplegar la solicitud de credenciales de acceso para inicio de sesión seguro, como se muestra en el Anexo I.<br><br><b>NOTA:</b> Se debe presionar simultáneamente las teclas Ctrl+Alt+Suprimir. | Usuario/a        | 2                      |
| 2  | Ingreso de credenciales de acceso                             | El usuario ingresa sus credenciales de acceso en la pantalla desplegada, como se muestra en el Anexo I. Se pueden dar las siguientes alternativas:<br>- Credenciales de acceso incorrectas (3)<br>- Credenciales de acceso correctas (4)   | Usuario/a        | 3 o 4                  |
| 3  | Despliegue de mensaje de error de credenciales de acceso      | El sistema AD despliega un mensaje indicando que las credenciales de acceso son incorrectas.   | Active Directory | 2                      |
| 4  | Inicio de sesión seguro                                       | El sistema AD concede acceso a los sistemas de la institución  | Active Directory | FIN                    |

**7.3 Matriz de Responsabilidades.**

No Aplica.

**8. Registro de Operación.**

| REGISTRO  | ID | RESPONSABLE/DUEÑO DEL REGISTRO | TIEMPO RETENCIÓN      | SOPORTE | LUGAR                                   |
|---|----|--------------------------------|-----------------------|---------|---|
| Evidencia de la configuración adecuada del sistema Active Directory para inicio de sesión seguro. | -  | Encargado de Plataforma        | 4 años / Archivo UTIC | Digital | Panel de configuración Active Directory |

**Aprobado por:**

**Firma:**

**Fecha de Actualización:**



## 8. PROCEDIMIENTO DE MANTENCIÓN DE EQUIPOS CRÍTICOS.

| Procedimiento de Mantenimiento de Equipos Críticos<br>Control A.11.02.04 |  |
|--|--|
| Tabla de Contenidos  |  |
| 1  | Objetivo..... 49   |
| 2  | Alcance..... 49  |
| 3  | Normas y Referencias..... 50                                   |
| 4  | Términos y Definiciones. .... 50                               |
| 5.   | Roles y Responsabilidades ..... 50                             |
| 6.   | Definición de Equipamiento Crítico..... 51                     |
| 7.   | Modo de Operación ..... 51                                     |
| 7.1  | Flujo de Procedimiento para Mantenciones Preventivas..... 51   |
| 7.2  | Matriz del Procedimiento para Mantenciones Preventivas..... 52 |
| 7.3  | Flujo de Procedimiento para Mantenciones Correctivas ..... 53  |
| 7.4  | Matriz de Procedimientos para Mantenciones Correctivas..... 54 |
| 7.5  | Matriz de Responsabilidades..... 55                            |
| 8.   | Registro de Operación. .... 56                                 |

### REVISIONES DEL PROCEDIMIENTO

| Nº Versión | Fecha      | Motivo de la revisión | Páginas elaboradas o modificadas |
|------------|------------|-----------------------|----------------------------------|
| Cero (0)   | 31/05/2019 | Elaboración inicial   | Todas                            |

| ELABORADO POR   | VALIDACIÓN TÉCNICA             | APROBADO POR  | APROBADO POR    |
|---|--------------------------------|---|-----------------|
| Sistema de Gestión de Seguridad de Información y Ciberseguridad | Patrik Soto<br>Jefe Unidad TIC | Andrea Soto Araya<br>Encargada de Seguridad de la Información | Comité de SGSIC |

### 1. Objetivo.

En función de lo establecido en el punto tres (3), sobre el Marco General de Protección de los Activos de Información, de la Política de Seguridad de la Información de la Agencia de Calidad de la Educación, en adelante la Agencia, el objetivo del presente documento es especificar el procedimiento asociado al mantenimiento tanto preventivo como correctivo de los recursos o equipamiento computacional, de soporte y plataforma de la Agencia, buscando así, la mitigación de la ocurrencia de riesgos que desencadenen algún evento o incidente que se pueda producir por falta de mantenimiento al equipamiento, y, en su defecto, la reducción de la gravedad del impacto cuando éstos se producen.

### 2. Alcance.

Este procedimiento se debe aplicar a todo el equipamiento computacional, de soporte y plataforma de la Agencia, considerado como crítico, es decir, aquellos que por la relevancia de los procesos que soportan, no puedan presentar indisponibilidad prolongada de su servicio.

Adicionalmente, se consideran dentro del alcance de este procedimiento, las mantenciones tanto preventivas como correctivas.

### 3. Normas y Referencias.

- Política General de Seguridad de la Información de la Agencia de Calidad de la Educación
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información.

### 4. Términos y Definiciones.

|  |   |
|--|---|
| <b>Amenaza</b>                               | Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o una organización.  |
| <b>Riesgo</b>                                | Las condiciones de debilidad en los activos que pueden ser afectadas por la existencia de una amenaza concreta, y las consecuencias que esto tiene. Es el efecto o materialización de la amenaza, el cual se puede clasificar respecto de su severidad, considerando su nivel de probabilidad y el impacto que generaría su ocurrencia.   |
| <b>Autoridad</b>                             | Facultad o derecho que posee un individuo o conjunto de individuos para actuar, mandar, o exigir una determinada acción a otros, en virtud del poder que emana de su posición dentro de la organización o institución. En el caso del sistema de seguridad de la información serán entendidas como autoridades, los responsables de los procesos de continuidad del negocio y recuperación ante desastres; y los servicios de emergencia, salud, bomberos y carabineros.  |
| <b>Evento de Seguridad de la Información</b> | Se refiere a la identificación y materialización de una amenaza o riesgo detectado el cual pudiera eventualmente comprometer la continuidad operacional de la Agencia.  |
| <b>Incidente de Seguridad</b>                | Se refiere a la Identificación y materialización de una amenaza o riesgo detectado que afecte la continuidad operacional que afecte activos de información relevantes para la Agencia.  |
| <b>Vulnerabilidad</b>                        | Debilidades propias de las características propias de cada activo, que los exponen a una amenaza o riesgo.  |
| <b>Evento de Seguridad</b>                   | Se refiere a la identificación y materialización de una amenaza o riesgo detectado, que afecte la continuidad operacional dañando activos relevantes de la Agencia  |
| <b>Plan de Contingencia</b>                  | Plan de Acción donde se señala explícitamente, el procedimiento a seguir, ante la ocurrencia de un incidente de seguridad de la información, que comprometa la continuidad operacional de la Agencia.   |
| <b>Activos de Información</b>                | Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta manera es que se distingue la información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.), los equipos, sistemas, infraestructura que soportan esta información y las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales. |
| <b>Contactos críticos</b>                    | Corresponden al nivel de contacto que se necesita ubicar con urgencia en caso de dificultades tecnológicas o incidentes.  |
| <b>Red de Seguridad</b>                      | Corresponden a números telefónicos públicos de servicios de emergencia, que no referencian la identificación de una persona.  |
| <b>Seguridad de la Información</b>           | Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de informar, no repudio y confidencialidad.   |

### 5. Roles y Responsabilidades.

- a) **Encargada(o) de Seguridad de la Información:** Como rol líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), tiene la responsabilidad de monitorear el cumplimiento de este procedimiento, así como de mantenerse al tanto de los diferentes eventos que desencadenen mantenciones de tipo correctivas a los equipos críticos de la Agencia.

**b) Jefatura de Unidad de Tecnologías de Información y Comunicación:** La jefatura de la Unidad TIC, como Autoridad Interna a cargo de velar por la mantención operativa de los servicios tecnológicos de la Agencia, debe velar por el fiel cumplimiento del proceso en cuanto a mantención del equipamiento.

**c) Encargado de Plataforma:** El encargado de plataforma será el rol responsable de administrar y ejecutar el proceso de mantención tanto preventiva como correctiva, de los recursos tecnológicos a los que este procedimiento hace referencia en su alcance.

**6. Definición de Equipamiento Crítico.**

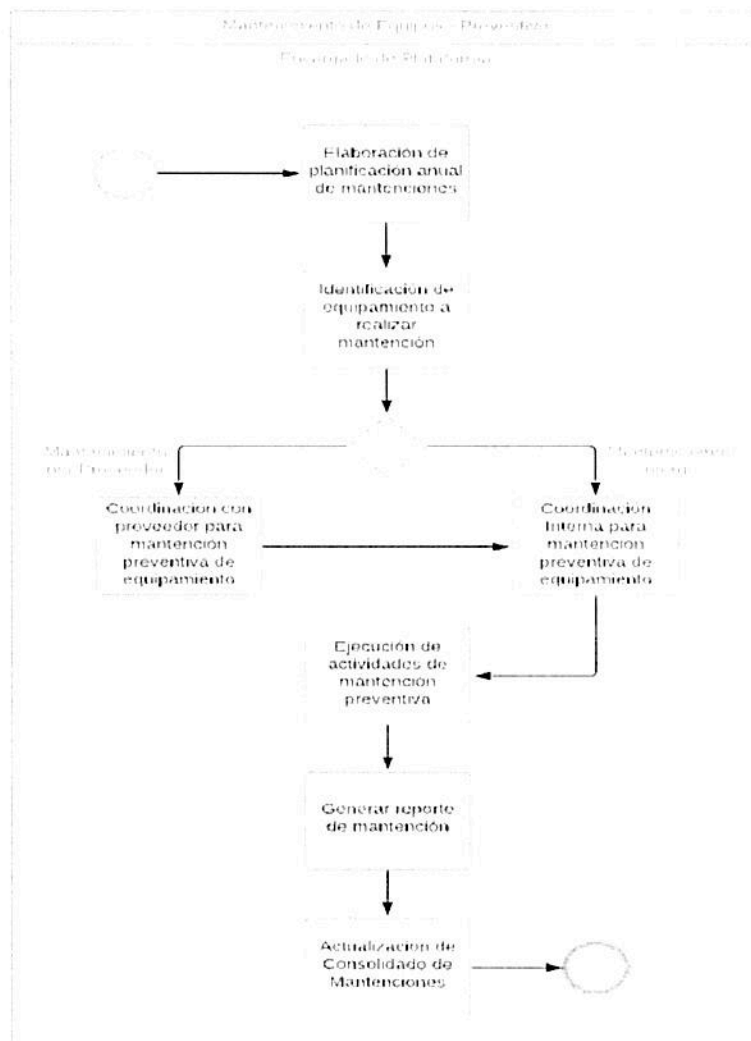
Dado que la actividad central de la Agencia, declarada en la Política General de Seguridad de Información, corresponde a la manipulación de información propia confidencial y sensible de terceros, y que ésta debe ser segura durante todo su ciclo de vida, es que se declaran como críticos todos aquellos elementos tecnológicos que dan soporte a las fases del ciclo de vida antes mencionado. Dentro de este conjunto de equipamiento tecnológico, se encuentran:

- SAI o UPS
- Storage
- Plataforma de Virtualización (VMWare)
- Equipamiento de Comunicaciones (Switches)
- Planta telefónica; Cisco Call Manager, SBC, Liric GSM
- Equipamiento de Firewall
- Servidores

**7. Modo de Operación.**

A continuación, se describen los flujos procedimentales para las mantenciones tanto preventivas como correctivas del equipamiento tecnológico crítico:

**7.1 Flujo de Procedimiento para Mantenciones Preventivas.**

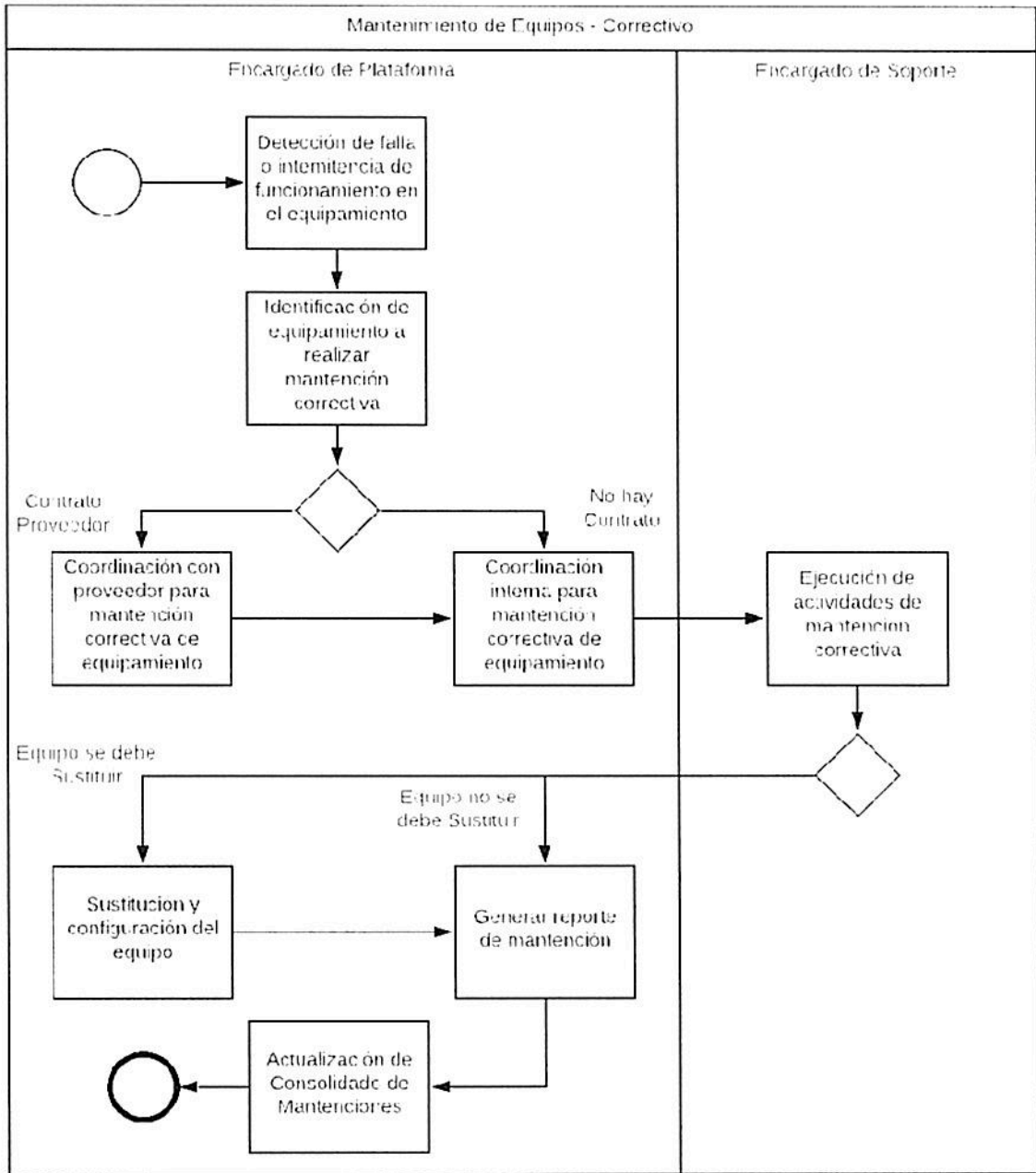


**7.2 Matriz del Procedimiento para Mantenciones Preventivas.**

| ID | ACTIVIDAD   | DESCRIPCIÓN   | RESPONSABLE             | ID ACTIVIDAD SIGUIENTE |
|----|---|---|-------------------------|------------------------|
| 1  | Elaboración de planificación anual de mantenciones preventivas        | Se debe realizar anualmente, una planificación de mantenciones preventivas, calendarizando las actividades a lo largo del año. Esta planificación debe considerar cada área y tipo de equipamiento, además de que éstas se deben ejecutar fuera de horario laboral con el objetivo de no entorpecer las funciones de los colaboradores(as) de la Agencia y realizarlas con celeridad y mayor organización.  | Encargado de Plataforma | 2                      |
| 2  | Identificación de equipamiento a realizar mantención                  | Se deben identificar los equipos o recursos a los cuales les corresponde la mantención preventiva según la planificación. Se pueden dar las siguientes alternativas:<br>- El mantenimiento se debe hacer mediante proveedor (3)<br>- El mantenimiento se realiza con personal interno (4)   | Encargado de Plataforma | 3 o 4                  |
| 3  | Coordinación con proveedor para mantención preventiva de equipamiento | Se debe coordinar con el proveedor apropiado, la ejecución de las mantenciones preventivas consideradas en el alcance según planificación. Éstas deben estar alineadas con las definiciones descritas en la actividad uno (1) de este flujo.<br><br><b>NOTA:</b> Las actividades de mantención del proveedores deben ser supervisadas por el Encargado de Soporte.  | Encargado de Plataforma | 4                      |
| 4  | Coordinación interna para mantención preventiva de equipamiento       | Se deben coordinar de forma interna, y al menos con 24 horas de anticipación, las actividades de mantención consideradas en el alcance de la planificación, se debe considerar:<br>- Coordinación con Encargado de Soporte, quien ejecutará las actividades de mantención cuando estas se lleven a cabo de forma interna.<br>- Comunicación, ya sea a la organización completa o a aquellos roles directamente involucrados en esta actividad, las medidas y consideraciones que deben tener de forma previa a la ejecución de éstas. | Encargado de Plataforma | 5                      |

| ID | ACTIVIDAD   | DESCRIPCIÓN  | RESPONSABLE             | ID ACTIVIDAD SIGUIENTE |
|----|---|--|-------------------------|------------------------|
| 5  | Ejecución de actividades de mantención preventiva | Se deben ejecutar las actividades de mantención preventiva consideradas en el alcance de la planificación.     | Encargado de Plataforma | 6                      |
| 6  | Generar reporte de mantención                     | Se debe generar el reporte de mantención según lo indicado en el Anexo 1 de este documento.                    | Encargado de Plataforma | 7                      |
| 7  | Actualización de Consolidado de Mantenciones      | Se debe actualizar el consolidado de mantenciones preventivas según se indica en el Anexo 2 de este documento. | Encargado de Plataforma | FIN                    |

**7.3 Flujo de Procedimiento para Mantenciones Correctivas.**



**7.4 Matriz de Procedimientos para Mantenciones Correctivas.**

| ID | ACTIVIDAD   | DESCRIPCIÓN  | RESPONSABLE             | ID ACTIVIDAD SIGUIENTE |
|----|---|--|-------------------------|------------------------|
| 1  | Detección de falla o intermitencia de funcionamiento en el equipamiento | <p>La detección de fallas en el equipamiento crítico se puede dar de las siguientes formas:</p> <ul style="list-style-type: none"> <li>- Indicadores de monitoreo, donde el mismo personal de la Unidad de TIC detecta la falla.</li> <li>- Mediante el sistema de tickets de la organización, donde un colaborador o colaboradora notifica fallas en el funcionamiento del equipamiento tecnológico.</li> </ul>                         | Encargado de Plataforma | 2                      |
| 2  | Identificación de equipamiento a realizar mantención correctiva         | <p>Si bien la notificación de la falla en el equipamiento puede llegar desde dos fuentes distintas, se debe identificar claramente qué elemento tecnológico presenta la falla para proceder a su mantención correctiva. Se pueden dar las siguientes alternativas:</p> <ul style="list-style-type: none"> <li>- El equipo cuenta con contrato con proveedor (3)</li> <li>- El equipo no cuenta con contrato con proveedor (4)</li> </ul> | Encargado de Plataforma | 3 o 4                  |
| 3  | Coordinación con proveedor para mantención correctiva de equipamiento   | <p>Se debe coordinar con el proveedor apropiado, la ejecución de las mantenciones correctivas asociadas a la falla presentada.</p> <p><b>NOTA:</b> Las actividades de mantención del proveedores deben ser supervisadas por el Encargado de Soporte.</p>   | Encargado de Plataforma | 4                      |

| ID | ACTIVIDAD   | DESCRIPCIÓN   | RESPONSABLE             | ID ACTIVIDAD SIGUIENTE |
|----|---|---|-------------------------|------------------------|
| 4  | Coordinación interna para mantención correctiva de equipamiento | Se deben coordinar de forma interna, y al menos con 24 horas de anticipación, las actividades de mantención consideradas en el alcance de la planificación, se debe considerar:<br>- Coordinación con Encargado de Soporte, quien ejecutará las actividades de mantención cuando estas se lleven a cabo de forma interna.<br>- Comunicación, ya sea a la organización completa o a aquellos roles directamente involucrados en esta actividad, las medidas y consideraciones que deben tener de forma previa a la ejecución de éstas. | Encargado de Plataforma | 5                      |
| 5  | Ejecución de actividades de mantención correctiva               | Se deben ejecutar las actividades de mantención preventiva consideradas en el alcance de la planificación. Se pueden dar las siguientes opciones:<br>- El equipo debe ser reemplazo (6).<br>- El equipo debe ser reparado (7)   | Encargado de Soporte    | 6 o 7                  |
| 6  | Sustitución y configuración del equipo                          | El equipo debe ser reemplazo por uno nuevo, el cual debe ser configurado, ya sea por el proveedor o por personal interno según corresponda.   | Encargado de Plataforma | 7                      |
| 7  | Generar reporte de mantención                                   | Se debe generar el reporte de mantención según lo indicado en el Anexo 1 de este documento.   | Encargado de Plataforma | 8                      |
| 8  | Actualización de Consolidado de Mantenciones                    | Se debe actualizar el consolidado de mantenciones preventivas según se indica en el Anexo 2 de este documento.  | Encargado de Plataforma | FIN                    |

### 7.5 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

De esta forma, la matriz de responsabilidades para la mantención preventiva del equipamiento se estructura de la siguiente manera:

| ID | ACTIVIDAD  | ENC. SI | JEFE TIC | ENC. PLATAFORMA | ENC. SOPORTE |
|----|--|---------|----------|-----------------|--------------|
| 1  | Elaboración de planificación anual de mantenciones preventivas | I       | A        | R/E             | I            |

|   |  |   |   |     |   |
|---|--|---|---|-----|---|
| 2 | Identificación de equipamiento a realizar mantenimiento                  | I | I | R   | I |
| 3 | Coordinación con proveedor para mantenimiento preventiva de equipamiento | I | A | R/E | I |
| 4 | Coordinación interna para mantenimiento preventiva de equipamiento       | I | I | R/E | I |
| 5 | Ejecución de actividades de mantenimiento preventiva                     | I | I | R   | E |
| 6 | Generar reporte de mantenimiento   |   |   | A   | R |
| 7 | Actualización de Consolidado de Mantenciones                             | I | I | R   | - |

Así mismo, la matriz de responsabilidades para la mantenimiento correctiva del equipamiento se estructura de la siguiente manera:

| ID | ACTIVIDAD  | ENC. SI | JEFE TIC | ENC. PLATAFORMA | ENC. SOPORTE |
|----|--|---------|----------|-----------------|--------------|
| 1  | Detección de falla o intermitencia de funcionamiento en el equipamiento  | I       | I        | R               | R            |
| 2  | Identificación de equipamiento a realizar mantenimiento correctiva       | I       | I        | R/C             | E/C          |
| 3  | Coordinación con proveedor para mantenimiento correctiva de equipamiento | I       | A        | R/E             | I            |
| 4  | Coordinación interna para mantenimiento preventiva de equipamiento       | I       | I        | R/E             | I            |
| 5  | Ejecución de actividades de mantenimiento correctiva                     | I       | I        | R               | E            |
| 6  | Sustitución y configuración del equipo                                   | I       | A        | R               | E            |
| 7  | Generar reporte de mantenimiento   | -       | -        | A               | R            |
| 8  | Actualización de Consolidado de Mantenciones                             | I       | I        | R               | -            |

#### 8. Registro de Operación.

| REGISTRO  | ID | RESPONSABLE/DUEÑO DEL REGISTRO | TIEMPO RETENCIÓN      | SOPORTE | LUGAR                      |
|---|----|--------------------------------|-----------------------|---------|----------------------------|
| Planificación anual de mantenimientos preventivos | -  | Encargado de Plataforma        | 1 años / Archivo UTIC | Digital | PC Encargado de Plataforma |
| Consolidado anual de reportes de mantenimiento    | -  | Encargado de Plataforma        | 1 años / Archivo UTIC | Digital | PC Encargado de Plataforma |



## 9. PROCEDIMIENTO DE EQUIPO DE USUARIO DESATENDIDO.

| Procedimiento de Equipo de Usuario Desatendido<br>Control A.11.02.08 |   |  |    |
|--|---|--|----|
| Tabla de Contenidos  |   |  |    |
| 1  | Objetivo.....   |  | 57 |
| 2  | Alcance.....  |  | 57 |
| 3  | Normas y Referencias.....   |  | 57 |
| 4  | Términos y Definiciones.....  |  | 58 |
| 5.   | Roles y Responsabilidades .....   |  | 58 |
| 6.   | Directrices Generales para la Entrega y Devolución de Recursos .....    |  | 58 |
| 7.   | Modo de Operación .....   |  | 59 |
| 7.1  | Flujo de Procedimiento .....  |  | 59 |
| 7.2  | Matriz del Proceso de Protección de Equipo de Usuario Desatendido ..... |  | 59 |
| 7.3  | Matriz de Responsabilidades.....  |  | 60 |
| 8.   | Registro de Operación.....  |  | 60 |

| REVISIONES DEL PROCEDIMIENTO |          |                       |                                  |
|------------------------------|----------|-----------------------|----------------------------------|
| Nº Versión                   | Fecha    | Motivo de la revisión | Páginas elaboradas o modificadas |
| Cero (0)                     | 28-06-19 | Elaboración inicial   | Todas                            |

| ELABORADO POR   | VALIDACIÓN TÉCNICA       | APROBADO POR  | APROBADO POR    |
|---|--------------------------|---|-----------------|
| Sistema de Gestión de Seguridad de Información y Ciberseguridad | Patrick Soto<br>Jefe TIC | Andrea Soto Araya<br>Encargada de Seguridad de la Información | Comité de SGSIC |

### 1. Objetivo.

El presente procedimiento tiene por finalidad establecer las actividades y paso a paso para promover e instaurar el bloqueo del computador por parte del usuario una vez que éste ha desocupado su estación de trabajo, a modo de proteger los Activos de Información que se encuentran almacenados en el computador o en la nube a la que el usuario tiene acceso mediante su equipo.

### 2. Alcance.

El procedimiento debe ser aplicado por todos los computadores que estén en funcionamiento, tanto dentro como fuera de la Agencia de Calidad de la Educación, que contengan información relacionada con la institución.

### 3. Normas y Referencias.

- Decreto Supremo N° 83, Norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Resolución Exenta N° 1440, Política General de Seguridad de la Información.
- Norma NCh-ISO 27001:2009, Sistemas de Gestión de la Seguridad de la Información - Requisitos. Anexo A, A.10.5.1
- Norma NCh-ISO 27002:2009, Código de prácticas para la gestión de la seguridad de la información, Control 10.5.1.

#### 4. Términos y Definiciones.

|                              |   |
|------------------------------|---|
| <b>Proteger Documentos</b>   | Acción de bloquear el computador, con la finalidad de proteger los activos de información contenidos en este. Esta acción se lleva a cabo mediante la combinación de teclas: Ctrl + Alt+ Supr<br>Esta acción es también realizada por la Unidad TIC mediante la utilización de Active Directory para bloquear el computador luego de que han pasado cinco (5) minutos de inactividad. |
| <b>Usuario</b>               | Hace referencia al responsable del bloqueo de su computador, el cual contiene información sensible para la institución.   |
| <b>Activo de Información</b> | La información es un activo fundamental para el desarrollo, operativa, control y gestión de la institución. Esta es considerada como información propiamente tal, abstrayéndola del medio en el que se encuentra almacenada.  |
| <b>Restricción de Acceso</b> | Delimitar el acceso de los usuarios, servidores públicos a honorarios y terceras partes a determinados recursos de la organización.   |
| <b>Estación de Trabajo</b>   | Un computador que facilita a los usuarios(as) el acceso a los servidores y periféricos de la organización.  |
| <b>Active Directory</b>      | Es el termino usado por Microsoft para referirse a la implementación de un servicio de directorio en una red distribuida de computadores. En la Agencia de Calidad de la Educación, es el sistema implementado para acceder a cada equipo computacional.  |
| <b>Contraseña</b>            | Forma de autenticación que utiliza información secreta para controlar el acceso a cierto recurso.   |

#### 5. Roles y Responsabilidades.

- a) **Unidad de Tecnologías de Información y Comunicación:** Es responsabilidad de la Unidad el proteger los computadores de la organización mediante la activación del bloqueo automático en cada uno de los equipos de los funcionarios, cumplido cierto espacio de tiempo determinado, mediante la utilización de la herramienta Active Directory.
- b) **Encargado(a) de Seguridad de la Información:** Como rol líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), tiene la responsabilidad de monitorear el cumplimiento de este procedimiento.
- c) **Usuario:** Es responsabilidad del trabajador perteneciente a la Agencia de Calidad de la Educación, bloquear su estación de trabajo una vez ha dejado de utilizarla.

#### 6. Directrices Generales para la Protección del Usuario Desatendido.

Teniendo en consideración la importancia de la protección de la información manipulada dentro de la organización, es necesario tomar precauciones pertinentes para que agentes externos no tengan acceso a esta mediante la utilización del equipo desatendido de alguno de los trabajadores de la institución. En función de lo anterior, se especifican a continuación las posibles formas de protección de información y bloqueo del equipo:

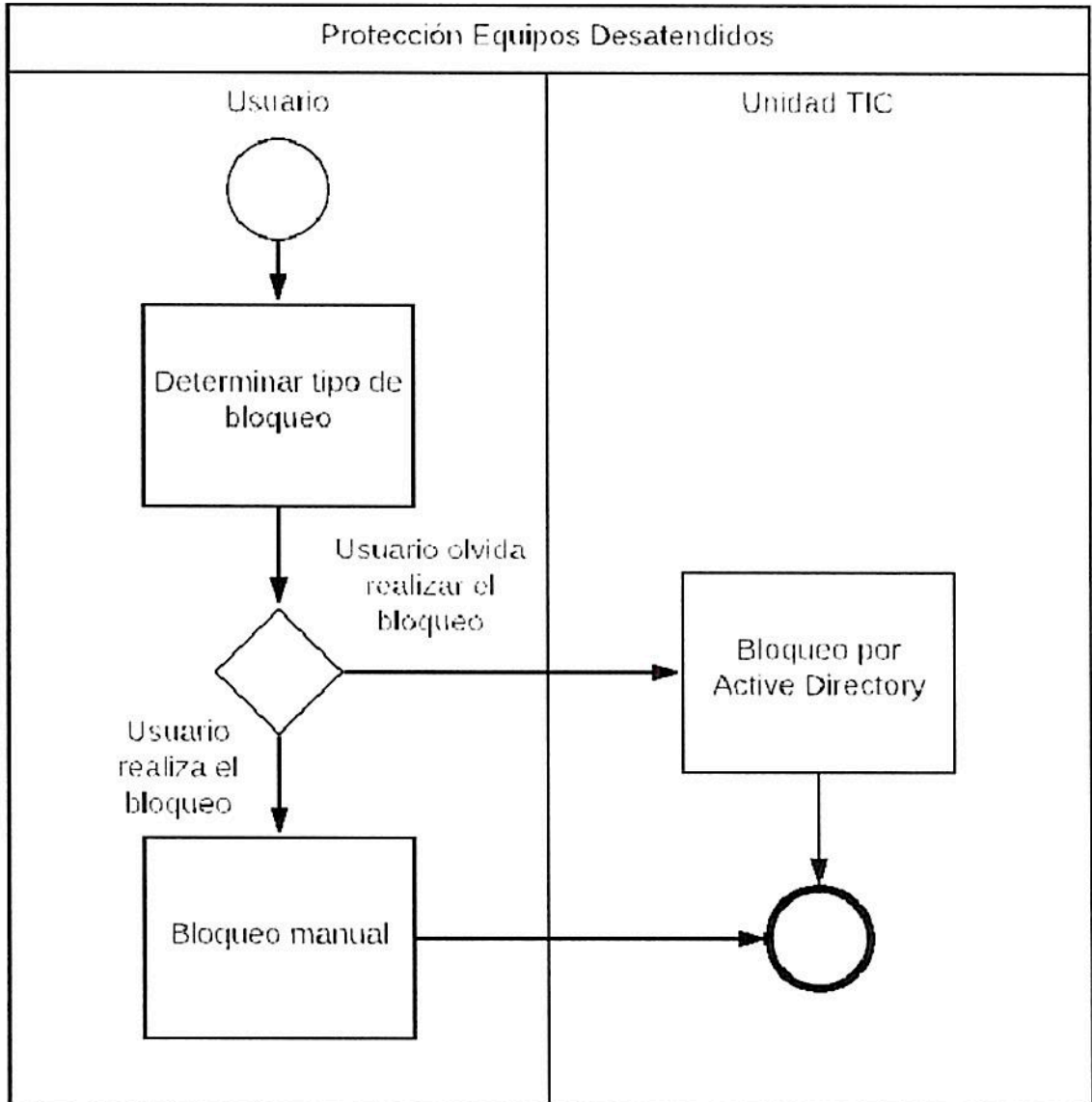
| <b>TIPO DE BLOQUEO</b>              | <b>EJECUTOR</b> | <b>FORMA DE PROTECCIÓN DE INFORMACIÓN</b>   |
|-------------------------------------|-----------------|---|
| <b>Bloqueo Manual</b>               | Usuario         | Hace referencia al bloqueo del equipo que realiza el usuario a quien pertenece este, el cual es realizado mediante la combinación de las teclas: Ctrl + Alt + Spr   |
| <b>Bloqueo por Active Directory</b> | Unidad TIC      | Bloqueo remoto efectuado por la Unidad TIC sobre todos los computadores de la institución mediante Active Directory. Este bloqueo se activa sobre el equipo en cuestión una vez que ha estado desatendido por un periodo de cinco (5) minutos. Se pueden encontrar los detalles de esta configuración en el Anexo I: Configuración Active Directory para bloqueo automático de estaciones de trabajo. |

Es importante detallar que cada uno de los usuarios tiene la responsabilidad de bloquear su equipo una vez que ha dejado de utilizarlo.

**7. Modo de Operación.**

De acuerdo con los tipos de bloqueo descritos anteriormente, se establece un flujo de actividades específico, en donde, de acuerdo con el tipo de evento, se definen las tareas pertinentes, así como los roles responsables de la realización de estas.

**7.1 Flujo de Procedimiento.**



**7.2 Matriz del Proceso de Protección de Equipo de Usuario Desatendido.**

| ID | ACTIVIDAD                  | DESCRIPCIÓN   | RESPONSABLE | ID ACTIVIDAD SIGUIENTE |
|----|----------------------------|---|-------------|------------------------|
| 1  | Determinar tipo de bloqueo | Una vez que el usuario ha terminado de utilizar el equipo, se deberá determinar el tipo de bloqueo que tendrá efecto: <ul style="list-style-type: none"> <li>- Bloqueo Manual (2)</li> <li>- Bloqueo por Active Directory (3)</li> </ul> <b>Nota:</b> Es importante especificar que es responsabilidad del usuario realizar el bloqueo de su equipo, por lo que el bloqueo por Active Directory está implementado como una medida preventiva en caso de que el usuario olvide realizar el bloqueo manual. | Usuario     | 2, 3                   |

| ID | ACTIVIDAD                    | DESCRIPCIÓN   | RESPONSABLE      | ID ACTIVIDAD SIGUIENTE |
|----|------------------------------|---|------------------|------------------------|
| 2  | Bloqueo Manual               | El usuario deberá realizar el bloqueo manual del equipo mediante la utilización de la combinación de teclas: Ctrl + Alt+ Supr | Usuario          | FIN                    |
| 3  | Bloqueo por Active Directory | Una vez que el computador este ha estado desatendido por cinco (5) minutos o más, se bloqueará automáticamente.               | Active Directory | FIN                    |

### 7.3 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

De esta forma, la matriz de responsabilidades para el proceso es:

| ID | ACTIVIDAD                    | UNIDAD TIC | USUARIO |
|----|------------------------------|------------|---------|
| 1  | Determinar tipo de bloqueo   | -          | E/R     |
| 2  | Bloqueo Manual               | -          | E/R     |
| 3  | Bloqueo por Active Directory | R/E        | -       |

### 8. Registro de Operación.

| REGISTRO                            | ID | RESPONSABLE/DUEÑO DEL REGISTRO | TIEMPO RETENCIÓN      | SOPORTE | LUGAR                       |
|-------------------------------------|----|--------------------------------|-----------------------|---------|-----------------------------|
| Pantalla de AD con la configuración | -  | Unidad TIC                     | 4 años / Archivo UTIC | Digital | PC Responsable del Registro |

Finalmente, y por lo manifestado previamente, solicito a ustedes puedan difundir el material aquí transcrito, y que se acompaña adjunto, entre todo el personal que se desarrolla labores en sus dependencias.

Saluda atentamente a usted,



**JUAN BRAVO MIRANDA**  
**SECRETARIO EJECUTIVO (S)**  
**AGENCIA DE CALIDAD DE LA EDUCACIÓN**

Distribución:

- Divisiones (5)
- Archivo Secretaría Ejecutiva
- Unidad de Planificación
- Departamento de Auditoría
- Departamento Jurídico
- Oficina de Partes

|  |   |                   |         |                          |
|--|---|-------------------|---------|--------------------------|
|  <b>Agencia de<br/>Calidad de la<br/>Educación</b><br><br>Gobierno de Chile | <b>Procedimiento de Contactos con Grupos de Interés</b> |                   |         |                          |
|  | Nivel de Confidencialidad                               | -                 | Páginas | <b>1 de 8</b>            |
|  | Fecha versión del documento                             | <b>28-05-2019</b> | Versión | <b>1</b>                 |
|  |   |                   | Código  | <b>SGSIC-PRO-A.6.1.4</b> |
| <b>Procedimiento de Contactos con Grupos de Interés</b>  |   |                   |         |                          |

## Procedimiento de Contacto con Grupos de Interés

### Control A.06.01.04

#### Tabla de Contenidos

|            |   |          |
|------------|---|----------|
| <b>1</b>   | <b>Objetivo.....</b>  | <b>1</b> |
| <b>2</b>   | <b>Alcance.....</b>   | <b>1</b> |
| <b>3</b>   | <b>Normas y Referencias.....</b>  | <b>2</b> |
| <b>4</b>   | <b>Términos y Definiciones. ....</b>  | <b>2</b> |
| <b>5.</b>  | <b>Roles y Responsabilidades.....</b>   | <b>3</b> |
| <b>6.</b>  | <b>Grupos de Interés Especializados.....</b>                                  | <b>3</b> |
| <b>6.1</b> | <b>Destinatarios de la información proveniente de grupos de interés .....</b> | <b>4</b> |
| <b>7.</b>  | <b>Modo de Operación .....</b>  | <b>5</b> |
| <b>7.1</b> | <b>Flujo de Procedimiento.....</b>  | <b>5</b> |
| <b>7.2</b> | <b>Matriz del Proceso de Contacto con grupos de interés especiales.....</b>   | <b>6</b> |
| <b>7.3</b> | <b>Matriz de Responsabilidades. ....</b>                                      | <b>6</b> |
| <b>8</b>   | <b>Registro de Operación.....</b>   | <b>7</b> |

#### REVISIONES DEL PROCEDIMIENTO

| Nº Versión | Fecha      | Motivo de la revisión | Páginas elaboradas o modificadas |
|------------|------------|-----------------------|----------------------------------|
| Uno (1)    | 28/05/2019 | Elaboración inicial   | Todas                            |

|  |  |  |                                    |
|--|--|--|------------------------------------|
| <b>ELABORADO POR</b>   | <b>VALIDACIÓN TÉCNICA</b>  | <b>REVISADO POR</b>  | <b>APROBADO POR</b>                |
| Sistema de Gestión de Seguridad de la Información y Ciberseguridad | <br><b>Nicol Jeria</b><br>Encargada de Ciberseguridad | <br><b>Andrea Soto Araya</b><br>Encargada de Seguridad de la Información | Comité de Seguridad de Información |

#### 1. Objetivo.

El objetivo del presente documento es, en función de los objetivos de la Agencia de Calidad de la Educación, en adelante Agencia, establecidos en el Artículo 10 de la Ley 20.529, definir aquellos grupos de interés que puedan aportar con contenido relevante y concerniente a la seguridad de la información, a la elevación del nivel de madurez de la institución en estas temáticas. En base a lo anterior, se define un procedimiento formal y estructurado que permita canalizar esta información a las partes correspondientes al interior de la Agencia.

#### 2. Alcance.

Este procedimiento deberá ser aplicado por todos(as) los(as) funcionarios internos de planta, contrata y personal honorarios que tengan incidencia directa en la recepción,

canalización y/o difusión del contenido asociado a los grupos de interés definidos en el documento.

### 3. Normas y Referencias.

- Política General de Seguridad de la Información de la Agencia de Calidad de la Educación.
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información.

### 4. Términos y Definiciones.

|  |   |
|--|---|
| <b>Amenaza</b>                               | Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o una organización.  |
| <b>Riesgo</b>                                | Las condiciones de debilidad en los activos que pueden ser afectadas por la existencia de una amenaza concreta, y las consecuencias que esto tiene. Es el efecto o materialización de la amenaza, el cual se puede clasificar respecto de su severidad, considerando su nivel de probabilidad y el impacto que generaría su ocurrencia.   |
| <b>Autoridad</b>                             | Facultad o derecho que posee un individuo o conjunto de individuos para actuar, mandar, o exigir una determinada acción a otros, en virtud del poder que emana de su posición dentro de la organización o institución. En el caso del sistema de seguridad de la información serán entendidas como autoridades, los responsables de los procesos de continuidad del negocio y recuperación ante desastres; y los servicios de emergencia, salud, bomberos y carabineros.  |
| <b>Evento de Seguridad de la Información</b> | Se refiere a la identificación y materialización de una amenaza o riesgo detectado el cual pudiera eventualmente comprometer la continuidad operacional de la Agencia.  |
| <b>Incidente de Seguridad</b>                | Se refiere a la Identificación y materialización de una amenaza o riesgo detectado que afecte la continuidad operacional que afecte activos de información relevantes para la Agencia.  |
| <b>Vulnerabilidad</b>                        | Debilidades propias de las características propias de cada activo, que los exponen a una amenaza o riesgo.  |
| <b>Evento de Seguridad</b>                   | Se refiere a la identificación y materialización de una amenaza o riesgo detectado, que afecte la continuidad operacional dañando activos relevantes de la Agencia  |
| <b>Plan de Contingencia</b>                  | Plan de Acción donde se señala explícitamente, el procedimiento a seguir, ante la ocurrencia de un incidente de seguridad de la información, que comprometa la continuidad operacional de la Agencia.   |
| <b>Activos de Información</b>                | Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta manera es que se distingue la información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.), los equipos, sistemas, infraestructura que soportan esta información y las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales. |
| <b>Contactos</b>                             | Corresponden al nivel de contacto que se necesita ubicar con  |

|                                    |   |
|------------------------------------|---|
| <b>críticos</b>                    | urgencia en caso de dificultades tecnológicas o incidentes.   |
| <b>Red de Seguridad</b>            | Corresponden a números telefónicos públicos de servicios de emergencia, que no referencian la identificación de una persona.  |
| <b>Seguridad de la Información</b> | Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de informar, no repudio y confidencialidad. |

##### **5. Roles y Responsabilidades.**

- a) **Encargada(o) de Seguridad de la Información:** Como Autoridad Interna líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), este rol tiene la responsabilidad de gestionar el contacto con los grupos de interés definidos por la Agencia, abarcando desde su definición de acuerdo a los tópicos que busque reforzar la institución, establecimiento del contacto de forma oficial a través de la institución, la recepción y canalización de la información recibida a las partes correspondientes.
- b) **Encargada(o) de Seguridad de la Información:** Como Autoridad Interna perteneciente al Sistema de Gestión de Seguridad de Información y Ciberseguridad (SGSIC), enfocada en mantener la seguridad
- c) **Jefatura de Unidad de Tecnologías de Información y Comunicación:** La jefatura de la Unidad TIC, como Autoridad Interna a cargo de velar por la mantención operativa de los servicios tecnológicos de la Agencia, se define como un rol crítico para la misma, por ende, precisa un constante flujo de información proveniente de grupos de interés especializados, referente a amenazas, vulnerabilidades y nuevas tendencias tecnológicas, tanto benignas como maliciosas que puedan afectar a la organización. Es por lo anterior, que será responsable de recibir y canalizar con su equipo, la información que se ajuste a las necesidades antes descritas.
- d) **Jefaturas de División:** Las jefaturas de División, como Autoridades Internas que abarcan la mayor parte de los procesos críticos de la Agencia, y por ende la mayor parte de los colaboradores y colaboradoras de ésta, serán responsables de recibir y canalizar con la totalidad de las personas que componen sus procesos y ámbitos de responsabilidad, aquella información que provenga de grupos de interés especializados.

##### **6. Grupos de Interés Especializados.**

A continuación, se establecen de forma general, las temáticas que, de acuerdo con los objetivos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, en adelante SGSIC, definidos en el numeral cinco (5) de la Política General de Seguridad de la Información, los tópicos sobre los cuales la Agencia declara que se deben mantener una constante actualización de conocimiento:

- a) **Concientización en seguridad de información y ciberseguridad:** La Agencia de Calidad de la Educación, reconoce que las personas que componen la institución son cruciales para lograr una correcta disminución de la exposición a los riesgos de seguridad de información tanto actuales como futuros. Es por lo anterior, que el mantener un constante flujo de información que permita, en primer lugar, unificar el lenguaje de los colaboradores y colaboradoras bajo estas temáticas, y en segundo, concientizar sobre la importancia y cercanía que tiene esta temática, es crucial para mantener una evolución apropiada del SGSIC. Como Grupo de Interés enfocado en la generación de contenido como el descrito anteriormente, se define(n) el/los siguiente(s):

- i. **Oficina de Seguridad del Internauta (OSI):** Boletines con material de concientización y evangelización en seguridad de información y ciberseguridad.
- b) Tendencias de Seguridad de Información y Ciberseguridad:** Es de suma importancia para la Agencia de Calidad de la Educación, que se reciba por parte de grupos de interés especializados, información sobre nuevas tendencias en protección de datos personales y consejos referentes a la protección de la organización frente a las cada vez comunes y especializadas amenazas del ciberespacio. Como Grupo de Interés enfocado en la generación de contenido como el descrito anteriormente, se define(n) el/los siguiente(s):
- i. Instituto Nacional de Ciberseguridad de España (INCIBE): Boletines con material asociado a protección de empresas.
  - ii. Webempresa.com: Boletines con material sobre nueva regulación de protección de datos personales (RGPD)
- c) Reporte de amenazas y vulnerabilidades:** Dado lo expresado en el numeral uno (1) de la Política General de Seguridad de Información, en donde se declara que la información es el activo de mayor relevancia para la Agencia de Calidad de la Educación, es indispensable mantener contacto con grupos de interés especializados que generen reportes periódicos sobre nuevas amenazas que pudiesen afectar los objetivos específicos del SGSIC. Como Grupo de Interés enfocado en la generación de contenido como el descrito anteriormente, se define(n) el/los siguiente(s):
- i. Equipo de Respuesta ante Incidentes de Ciberseguridad del Gobierno de Chile (CSIRT-GOB)

#### **6.1 Destinatarios de la información proveniente de grupos de interés**

A continuación, se dan a conocer los destinatarios que a los cuales se deberán canalizar los boletines informativos recibidos de los grupos de interés descritos anteriormente:

| <b>GRUPO DE INTERÉS</b> | <b>RECEPTOR</b>                         | <b>DESTINATARIO</b>  |
|-------------------------|---|--|
| <b>OSI</b>              | Encargada/o de Seguridad de Información | Jefaturas de División  |
| <b>INCIBE</b>           | Encargada/o de Seguridad de Información | Encargada/o de Seguridad de Información  |
| <b>WEBEMPRESA.COM</b>   | Encargada/o de Seguridad de Información | Encargada(o) de Seguridad de Información / Jefa Departamento Jurídico / Encargado(a) Transparencia |
| <b>CSIRT-GOB</b>        | Encargada/o de Ciberseguridad           | Jefatura Unidad TIC  |

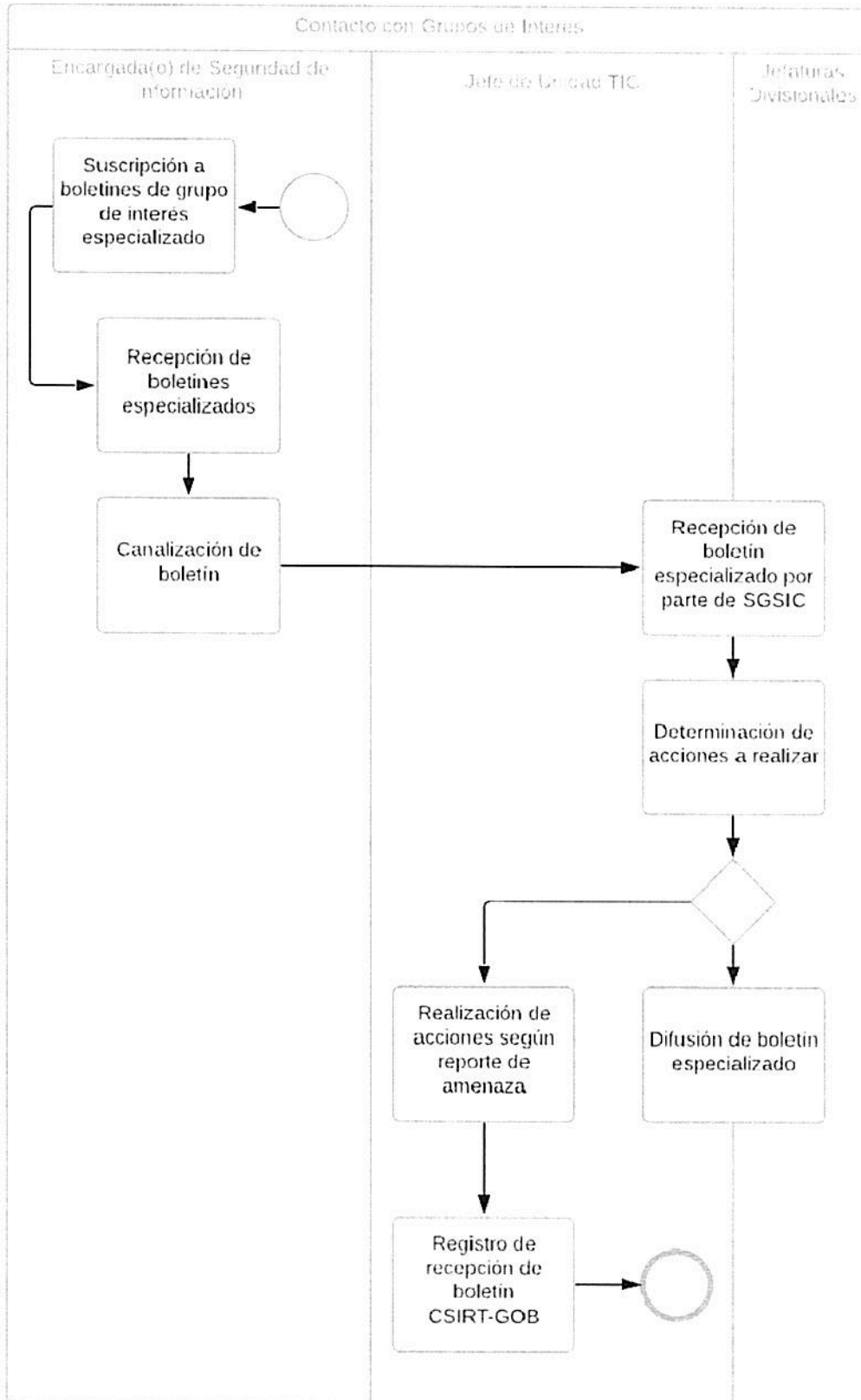
Para estos efectos, es responsabilidad, en primer lugar, de la Encargada/o de Seguridad de la Información, el hacer recepción oficial de los boletines provenientes de los grupos de interés tipificados y canalizar con los destinatarios respectivos, mientras, que en segundo lugar, serán las Jefaturas de División, así como la Jefatura de la Unidad de Tecnologías de Información y Comunicación, los encargados de distribuir la información a las personas que se encuentren bajo su ámbito de responsabilidades según corresponda.



## 7. Modo de Operación.

De acuerdo a los eventos descritos anteriormente, se establece un flujo comunicacional específico, en donde, de acuerdo al tipo de evento, se definen las autoridades pertinentes basado en su ámbito de responsabilidades. De esta forma, el flujo comunicacional es el siguiente:

### 7.1 Flujo de Procedimiento.



## **7.2 Matriz del Proceso de Contacto con Grupos de Interés Especiales.**

| <b>ID</b> | <b>ACTIVIDAD</b>  | <b>DESCRIPCIÓN</b>   | <b>RESPONSABLE</b>                          | <b>ID ACTIVIDAD SIGUIENTE</b> |
|-----------|---|--|---|-------------------------------|
| 1         | Suscripción a boletines de grupo de interés especializado | Se debe realizar la suscripción respectiva para la recepción de los boletines de seguridad por parte de los grupos de interés especializados. Para lo anterior, se utilizará el correo institucional del Sistema de Gestión de Seguridad de Información y Ciberseguridad (seguridadinformacion@agenciaeducacion.cl)                  | Encargada(o) de Seguridad de Información    | 2                             |
| 2         | Recepción de boletines especializados                     | Se debe hacer recepción de los boletines provenientes de los diferentes grupos de interés.   | Encargada(o) de Seguridad de Información    | 3                             |
| 3         | Canalización de boletín                                   | Se debe hacer reenvío del boletín a aquellos roles asociados a las temáticas específicas del grupo de interés especializado remitente según lo especificado en el punto 6.1 del presente procedimiento.  | Encargada(o) de Seguridad de Información    | 4                             |
| 4         | Recepción de boletín especializado por parte del SGSIC    | Se debe hacer recepción de del boletín de seguridad enviado por el SGSIC. Para oficializar la recepción, se debe responder un correo con el mensaje "Acuso Recibo."  | Jefe de Unidad TIC / Jefaturas Divisionales | 5                             |
| 5         | Determinación de acciones a realizar                      | Dada la naturaleza del boletín recibido, se pueden dar las siguientes opciones:<br>- Boletín no proveniente del CSIRT-GOB (6)<br>- Boletín de CSIRT-GOB (7)  | Jefe de Unidad TIC / Jefaturas Divisionales | 6 o 7                         |
| 6         | Difusión de boletín especializado                         | Se debe difundir el o los boletines de seguridad a todas aquellas personas que se encuentren bajo su ámbito de responsabilidades y/o formen parte de los procesos internos de la División/Unidad.  | Jefe de Unidad TIC / Jefaturas Divisionales | FIN                           |
| 7         | Realización de acciones según reporte de amenaza          | Se deben tomar todas las medidas necesarias para mitigar el riesgo de la amenaza reportada. Si bien éstas se encuentran indicadas en el boletín, se pueden complementar con acciones propias de la institución.<br><br><b>NOTA:</b> Para mayor detalle consultar procedimiento de gestión de incidentes seguridad de la información. | Jefe de Unidad TIC                          | 7A                            |
| 7A        | Registro de recepción de boletín CSIRT-GOB                | Se debe hacer registro de la recepción del boletín en la Planilla de Recepción de Alertas de Seguridad.  | Jefe de Unidad TIC                          | FIN                           |

## **7.3 Matriz de Responsabilidades.**

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado

- I: Informado
- E: Ejecutor

De esta forma, la matriz de responsabilidades se estructura de la siguiente manera:

| ID | ACTIVIDAD   | ENCARGA<br>DA SI | JEFE<br>TIC | JEFES<br>DIVISI<br>ÓN | EQUIP<br>O TIC |
|----|---|------------------|-------------|-----------------------|----------------|
| 1  | Suscripción a boletines de grupo de interés especializado | R                | I/C         | I/C                   | I              |
| 2  | Recepción de boletines especializados                     | R                | -           | -                     | -              |
| 3  | Canalización de boletín                                   | R                | I           | I                     | -              |
| 4  | Recepción de boletín especializado por parte del SGSIC    | C/I              | R           | R                     | -              |
| 5  | Determinación de acciones a realizar                      | C/I              | R           | -                     | C/I            |
| 6  | Difusión de boletín especializado                         | C/I              | R           | R                     | I              |
| 7  | Realización de acciones según reporte de amenaza          | C/I              | R/A         | -                     | E              |
| 7A | Registro de recepción de boletín CSIRT-GOB                | C/I              | R/A/<br>C   | -                     | E              |

#### 8. Registro de Operación.

| REGISTRO  | ID | RESPONSABLE/D<br>UEÑO DEL<br>REGISTRO       | TIEMPO<br>RETENCIÓN      | SOPORTE | LUGAR                                 |
|---|----|---|--------------------------|---------|---------------------------------------|
| Registro de recepción de alertas de seguridad CSIRT-GOB   | -  | Encargado(a) de Seguridad de la Información | 4 años /<br>Archivo UTIC | Digital | PC<br>Responsab<br>le del<br>Registro |
| Evidencia de suscripción a boletines de grupos de interés | -  | Encargado(a) de Seguridad de la Información | 4 años /<br>Archivo UTIC | Digital | PC<br>Responsab<br>le del<br>Registro |





**LISTA DE ASISTENCIA**  
**Comité de Seguridad de la Información**  
**Implementación PMG- Sistema de Seguridad de la Información**

- I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Estructura funcional del Sistema de Gestión de Seguridad de la Información y Ciberseguridad al interior de la Agencia de Calidad de la Educación
  2. Procedimiento de Contacto con Autoridades. Control A.6.1.3
  3. Procedimiento de Contacto con Grupos de Interés. Control A.6.1.4
  4. Política de Seguridad para Recursos Humanos. Control A.7.1.2
  5. Procedimiento de elaboración / Actualización de inventario de Activos. Control A.8.1.1 y su registro de operación.
  6. Procedimiento de Asignación y Devolución de Recursos. Control A.8.1.4
  7. Política de Control de Acceso físico y lógico. Control A.9.1.1 y A. 11.1.1
  8. Procedimiento de Inicio de Sesión Seguro. Control A.9.4.2
  9. Política de Ubicación y Protección del Equipamiento de la Agencia de Calidad de la Educación. Control A.11.2.1
  10. Procedimiento de Mantenimiento de Equipos Críticos. Control A.11.02.04
  11. Procedimiento de eliminación o Reutilización de Equipamiento. Control A.11.2.7
  12. Procedimiento de Equipo de Usuario Desatendido. Control A.11.02.08
  13. Política de Escritorio y Pantalla limpios. Control A.11.2.9
  14. Procedimiento de Respaldo de Información. Control A.12.03.01

Fecha: 3 de julio de 2019

| N° | Nombre                   | Cargo                                    | Firma |
|----|--------------------------|--|-------|
| 1  | Juan Bravo               | Secretario Ejecutivo (S)                 |       |
| 2  | Gino Cortez              | Jefe de DEOD (S)                         |       |
| 3  | Cristóbal Alarcón        | Jefe de DIAC                             |       |
| 4  | Mariana Segura           | Jefa de D( )A(S) y DAG (S)               |       |
| 5  | María de la Luz González | Jefa de DIEST (S)                        |       |
| 6  | Andrea Soto Araya        | Encargada de SSI                         |       |
| 7  | Nicol Jeria              | Encargada de Ciberseguridad              |       |
| 8  | Sergio Hidalgo           | Jefe Departamento de Auditoría           |       |
| 9  | Gabriel Cáceres          | Encargado de Unidad de Planificación (s) |       |
| 10 | YATIRICK SOTO            | Jefe Unidad TIC                          |       |
| 11 | Yerko Braun              | Proteccionista DIAC                      |       |
| 12 | Claudio Conado           | Consultor Externo                        |       |



| Procedimiento de Elaboración/Actualización de Inventario de Activos |            |         |                  |
|---|------------|---------|------------------|
| Nivel de Confidencialidad   | -          | Páginas | 1 de 8           |
|   |            | Versión | 0                |
| Fecha versión del documento   | 28-06-2019 | Código  | SGIC-PRO-A.8.1.1 |
| Procedimiento de Elaboración/Actualización de Inventario de Activos |            |         |                  |

## Procedimiento de Elaboración/Actualización de Inventario de Activos

### Control A.08.01.01

#### Tabla de Contenidos

|            |  |          |
|------------|--|----------|
| <b>1</b>   | <b>Objetivo.....</b>   | <b>1</b> |
| <b>2</b>   | <b>Alcance.....</b>  | <b>2</b> |
| <b>3</b>   | <b>Normas y Referencias.....</b>   | <b>2</b> |
| <b>4</b>   | <b>Términos y Definiciones. ....</b>   | <b>2</b> |
| <b>5.</b>  | <b>Roles y Responsabilidades.....</b>  | <b>3</b> |
| <b>6.</b>  | <b>Definiciones para la Construcción/Actualización del Inventario de Activos</b>                             | <b>3</b> |
| <b>7.</b>  | <b>Modo de Operación .....</b>   | <b>5</b> |
| <b>7.1</b> | <b>Flujo de Procedimiento para Elaboración/Actualización del Inventario de Activos de Información .....</b>  | <b>5</b> |
| <b>7.2</b> | <b>Matriz del Procedimiento para Elaboración/Actualización del Inventario de Activos de Información.....</b> | <b>6</b> |
| <b>7.3</b> | <b>Matriz de Responsabilidades. ....</b>   | <b>7</b> |
| <b>8.</b>  | <b>Registro de Operación. ....</b>   | <b>8</b> |

#### REVISIONES DEL PROCEDIMIENTO

| Nº Versión | Fecha      | Motivo de la revisión | Páginas elaboradas o modificadas |
|------------|------------|-----------------------|----------------------------------|
| Cero (0)   | 28/06/2019 | Elaboración inicial   | Todas                            |

|  |  |   |                     |
|--|--|---|---------------------|
| <b>ELABORADO POR</b>   | <b>VALIDACIÓN TÉCNICA</b>                  | <b>APROBADO POR</b>   | <b>APROBADO POR</b> |
| Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC) | Nicol Jeria<br>Encargada de Ciberseguridad | Andrea Soto Araya<br>Encargada de Seguridad de la Información | Comité de SGSIC     |



#### 1. Objetivo.

Según la declaración institucional efectuada en la Política General de Seguridad de Información y Ciberseguridad por la Agencia de Calidad de la Educación, en adelante la Agencia, donde ésta reconoce los activos de información como el activo más crítico para el cumplimiento de su misión institucional, y, por ende, comprende la necesidad de robustecer y mantener en constante mejora su ambiente de control, el objetivo de este procedimiento es establecer las actividades y la secuencia de acciones para la construcción y actualización del inventario de activos de información de la Agencia.

## 2. Alcance.

Lo establecido en este procedimiento, debe aplicarse para toda la información, independiente de su formato o medio de almacenamiento, que sea creada, almacenada y/o tratada como resultado de la operación de la Agencia, o como consecuencia del cumplimiento de su misión institucional.

Así mismo, el alcance circunscrito para este procedimiento, abarca tanto la formulación desde cero de dicho inventario, así como su constante actualización. En donde independiente de las condiciones antes mencionadas en las cuales se esté ejecutando este procedimiento, se considerará la clasificación de los activos de información según su criticidad en las dimensiones de Confidencialidad, Disponibilidad, Integridad y Privacidad.

De esta forma, y, en concordancia con lo establecido en la NCh ISO 27002:2013, el presente documento tiene su alcance sobre los siguientes controles:

- A.08.01.01 – Inventario de Activos
- A.08.02.01 – Clasificación de Activos

## 3. Normas y Referencias.

- NCh ISO 27001:2013.
- NCh ISO 27002:2013.
- Política General de Seguridad de la Información y Ciberseguridad, Agencia de Calidad de la Educación.
- Estructura Funcional del Sistema de Gestión de Seguridad de Información y Ciberseguridad, Agencia de Calidad de la Educación.

## 4. Términos y Definiciones.

|                                       |   |
|---------------------------------------|---|
| <b>Contraseña:</b>                    | Autenticación del usuario que utiliza información   |
| <b>Active Directory (AD)</b>          | Es el sistema de Directorio que posee la Agencia y que gestiona la Unidad TIC para identificar a todos los usuarios con el objetivo de administrar los inicios de sesión de los equipos en red.   |
| <b>Sistemas Informáticos</b>          | Sistemas que permiten almacenar y procesar información.   |
| <b>Acceso a la información</b>        | Derecho que tiene un usuario para buscar, recibir y difundir información del Servicio.  |
| <b>Restringir el acceso</b>           | Delimitar el acceso de los funcionarios (as), servidores públicos a honorarios y terceras partes a determinados recursos.   |
| <b>Estación de Trabajo</b>            | Es un computador que facilita a los usuarios (as) el acceso a los servidores y periféricos de la red.   |
| <b>Autenticación</b>                  | Proceso de confirmación de la identidad del (de la) usuario (a) que utiliza un sistema informático.   |
| <b>Identificador de autenticación</b> | Mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos.  |
| <b>Autenticar (o autenticar)</b>      | Se refiere a comprobar que esa persona es quien dice ser. Ello se logra cuando se cotejan uno o más datos en dicha identificación oficial contra (i) los datos en alguna otra identificación, documento, certificado digital (como el de la firma electrónica) o dispositivo que tenga la persona, (ii) los datos que sepa o tenga memorizados (su firma autógrafa o su contraseña, por ejemplo) o (iii) una o más características que coincidan con lo que es dicha persona (fotografía o huella dactilar, por ejemplo). |
| <b>Autorizar</b>                      | Se refiere al acceso que se le permite a la persona que se ha identificado y autenticado apropiadamente.  |
| <b>Identificador Único Global</b>     | Abreviado bajo la sigla GUID es una implementación del sistema Active Directory que permite que cada usuario sea único e irrepetible.   |

## **5. Roles y Responsabilidades.**

- a) **Encargada(o) de Seguridad de la Información:** Como líder del SGSIC, este rol será el encargado de supervisar la correcta ejecución de este procedimiento, así como la constante actualización del inventario de activos de información. Debe garantizar la correcta ejecución de éste procedimiento, tomando un rol consultor o asesor para impulsar la correcta y oportuna elaboración y/o actualización del inventario de activos de información consolidado de la Agencia.
- b) **Encargada(o) de Ciberseguridad:** Este rol será responsable de apoyar directamente en la elaboración y mantención actualizada del inventario de activos de información de la Agencia de Calidad de la Educación.
- c) **Jefatura de Unidad de Tecnologías de Información y Comunicación:** Será este rol el encargado de mantener y proveer a la Encargada(o) de Seguridad de la Información un inventario de activos tecnológicos actualizado, con la finalidad de ser un insumo para el inventario de activos de información de la Agencia.
- d) **Propietario de Activos:** Serán estos roles los encargados de elaborar y mantener actualizado de un inventario de aquellos activos de información que se encuentran bajo su gestión, y por ende, bajo su ámbito de responsabilidades. Éste inventario de activos constituye un insumo de gran importancia para la conformación del inventario de activos de la organización.

## **6. Definiciones para la Construcción/Actualización del Inventario de Activos.**

Para dar con el cumplimiento tanto del objetivo de este documento como con los objetivos estratégicos del Sistema de Gestión de Seguridad de la Información (SGSIC), se deberá elaborar y mantener actualizado un inventario de activos de información institucional, el cual considera la totalidad de activos de esta índole de la Agencia de Calidad de la Educación.

Para lo anterior, y en concordancia con la responsabilidad atribuida en la Estructura Funcional del SGSIC, serán los Propietarios de los Activos de Información, los encargados de cada uno proveer el Inventario de los Activos de Información que se encuentran bajo su gestión. De esta forma, el consolidado de éstos conformará el Inventario de Activos Institucional. Es así, como cada Inventario de Activos de los Propietarios de los Activos debe considerar:

- a. Un levantamiento o identificación de activos de información.
- b. Asignación de nombre único a cada activo de información. Se debe considerar que éste debe ser pensado para su mantención en el tiempo, por ende, debe estar relacionado lo más posible con el nombre que se le da a diario en la operación del proceso o unidad de negocio que soporta.
- c. Descripción funcional de cada activo de información. En otras palabras, debe considerar una descripción que especifique la función y relevancia que cumple cada activo para el proceso o unidad de negocio que soporta.
- d. Asociación con tecnología. Se debe establecer el medio tecnológico sobre el cual es almacenado o tratado cada activo de información. Para lo anterior se deben considerar, herramientas o sistemas web, carpetas compartidas, repositorios de almacenamiento de información, medios removibles, servidores, etc.
- e. Finalmente, se debe clasificar cada activo de información de acuerdo a sus niveles de criticidad en aspectos de Confidencialidad, Disponibilidad, Integridad y Privacidad.

De forma particular, para la clasificación de los activos de información se deben tener en cuenta los siguientes niveles de criticidad:



| DIMENSIÓN | DESCRIPCIÓN   | NIVEL CRITICIDAD | DESCRIPCIÓN   | EJEMPLOS |
|-----------|---|------------------|---|----------|
| Conf.     | Hace referencia al nivel de secreto o resguardo que debe tener un activo de información en específico. Frente a esto se debe responder siguiente la pregunta ¿Cuán secreto debe ser este activo para mantener la confidencialidad de la información que fluye por el área/proceso?  | Alto             | Información a la que tienen acceso únicamente los miembros de un grupo reducido dentro de la organización.  |          |
|           |   | Medio            | Información a la que tienen acceso únicamente los miembros de la organización.  |          |
|           |   | Bajo             | Información de carácter público a la que tienen acceso tanto los miembros de la organización como aquellos que no lo son.   |          |
| Disp.     | Hace referencia a la necesidad de consulta o dependencia en el uso del activo de información dentro del área/proceso. Frente a esto el rol debe intentar contestar la pregunta ¿Qué tan necesario es el acceso al activo para el funcionamiento del área/proceso?                   | Alto             | La indisponibilidad de estos activos genera consecuencias de tipo negativo inmediatas para la operación normal del área/proceso.                                  |          |
|           |   | Medio            | La indisponibilidad de estos activos tolerable por un corto período de tiempo antes de generar consecuencias negativas para la operación normal del área/proceso. |          |
|           |   | Bajo             | La indisponibilidad de estos activos solo generara consecuencias negativas para el área/proceso que soporta en el mediano-largo plazo.                            |          |
| Int.      | Hace referencia a que la información no contenga errores y/o modificaciones no autorizadas. Para esta clasificación se deben considerar aquellos activos relevantes para la elaboración de otros activos, reportes, informes y/o toma de decisiones al interior de la organización. | Alto             | La integridad es relevante para la elaboración de otros activos de información importantes para la operación normal del área/proceso                              |          |
|           |   | Bajo             | La integridad no es relevante para la elaboración de otros activos de información importantes para la operación normal del área/proceso.                          |          |

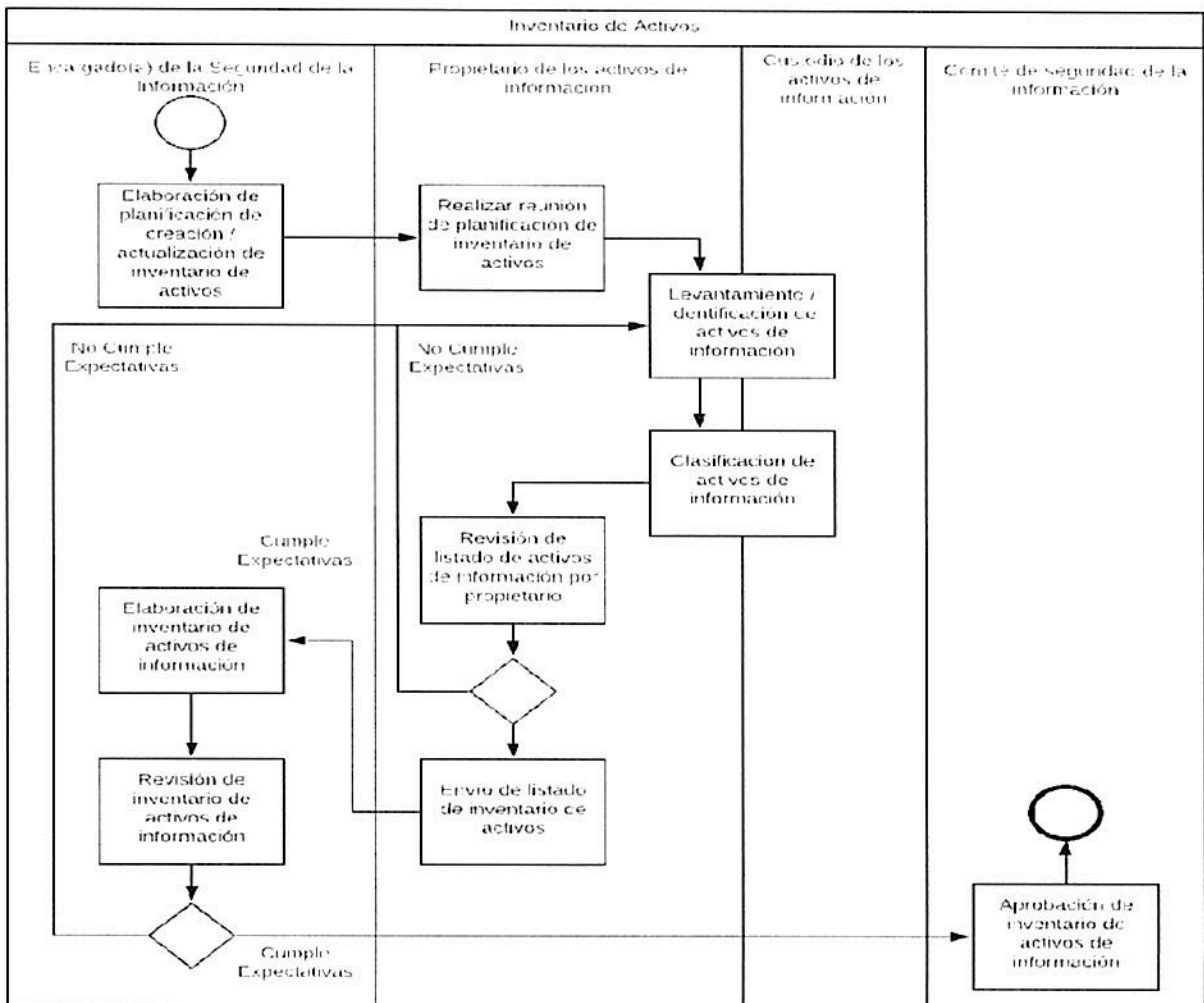
| DIMENSIÓN | DESCRIPCIÓN  | NIVEL CRITICIDAD | DESCRIPCIÓN  | EJEMPLOS |
|-----------|--|------------------|--|----------|
| Priv.     | Este atributo hace referencia a cuán importante es que un activo no pueda ser individualizado o relacionado a una persona. Para poder clasificar el activo, el rol debe preguntarse ¿cuán importante es que la información no pueda ser individualizada en el caso de hacerse pública? | Alto             | Se debe velar por la individualización de la información contenida en el activo                                  |          |
|           |  | Bajo             | La individualización de la información contenida en el activo no es una característica por la cual se deba velar |          |

Finalmente, se entenderá por "Activo de Información", a la información que, como producto de su operación, genera, almacena, trata y/o transita por los procesos de la Agencia de Calidad de la Educación, independiente de su formato o medio de almacenamiento.

### 7. Modo de Operación.

A continuación, se describen los flujos procedimentales para la elaboración y actualización del inventario de activos de la Agencia de Calidad de la Educación.

#### 7.1 Flujo de Procedimiento para Elaboración/Actualización del Inventario de Activos de Información.



**7.2 Matriz del Procedimiento para Elaboración/Actualización del Inventario de Activos de Información.**

| ID | ACTIVIDAD   | DESCRIPCIÓN   | RESPONSABLE                                       | ID ACTIVIDAD SIGUIENTE |
|----|---|---|---|------------------------|
| 1  | Elaboración de planificación de creación / actualización de inventario de activos | El/La Encargada(o) de Seguridad de la Información debe elaborar una planificación del proceso de creación/actualización del inventario de activos de información de la Agencia. Esta planificación debe realizarse al menos una vez al año calendario, y debe ser enviada a la totalidad de los roles propietarios de activos de la institución para que puedan alinearse a ésta. | Encargada(o) de Seguridad de la Información       | 2                      |
| 2  | Realizar reunión de planificación de inventario de activos                        | Tanto el propietario, como sus custodios designados, deben realizar una reunión con el objetivo de relacionar los activos de información que deben formar parte del inventario.   | Propietario(a) de los activos de información      | 3                      |
| 3  | Levantamiento/Identificación de Activos de Información                            | Se debe realizar el levantamiento de activos de información inicial y conformar un listado de activos de información que contenga su nombre, propietario, división, descripción funcional, ubicación y/o medio de almacenamiento.<br><br><b>NOTA:</b> Si ya existe un listado de activos de información, esta actividad tendrá carácter de actualización para éste.               | Propietario(a)/Custodio de Activos de Información | 4                      |
| 4  | Clasificación de activos de información   | Una vez elaborada/actualizada la lista de los activos de información bajo la gestión del Propietario de Activos, se debe realizar la clasificación de éstos según la criticidad que tengan en los objetivos del SGSIC, establecidos en la Política General de Seguridad de Información.   | Propietario(a)/Custodio de Activos de Información | 5                      |

| ID | ACTIVIDAD   | DESCRIPCIÓN   | RESPONSABLE                              | ID ACTIVIDAD SIGUIENTE |
|----|---|---|--|------------------------|
| 5  | Revisión de Listado de Activos de Información por Propietario | Se debe validar el listado de activos de información.<br>Se pueden dar las siguientes opciones:<br>- El Listado de Inventario de Activos de Información no cumple no cumple con las expectativas (3)<br>- El Listado de Inventario de Activos de Información cumple con las expectativas (6)  | Propietario(a) de Activos de Información | 3 o 6                  |
| 6  | Envío de listado de inventario de activos                     | Se debe enviar el listado de activos de información al/la Encargada(o) de Seguridad de Información.   | Propietario(a) de Activos de Información | 7                      |
| 7  | Elaboración de inventario de activos de información           | Se deben consolidar los listados de activos de información recibidos por parte de los Propietarios de los Activos, en el documento "[añosmes]_SGSIC-RO-A.8.1.1_InventarioActivosInformacion".   | Encargada(o) de Seguridad de Información | 8                      |
| 8  | Revisión de inventario de activos de información              | Se debe revisar y validar el inventario de activos de información recién elaborado.<br>Se pueden dar las siguientes alternativas:<br>- El Listado de Inventario de Activos de Información no cumple no cumple con las expectativas (3)<br>- El Listado de Inventario de Activos de Información cumple con las expectativas (9)                        | Encargada(o) de Seguridad de Información | 3 o 9                  |
| 9  | Aprobación de inventario de activos de información            | El inventario de activos de información debe ser aprobado en sesión del Comité de Seguridad de Información. Se pueden dar las siguientes alternativas:<br>- El Listado de Inventario de Activos de Información no cumple no cumple con las expectativas (8)<br>- El Listado de Inventario de Activos de Información cumple con las expectativas (FIN) | Comité de Seguridad de Información       | 8 o FIN                |

### **7.3 Matriz de Responsabilidades.**

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

Se esta forma, la matriz de responsabilidades se estructura de la siguiente manera:

| ID | ACTIVIDAD   | PROPIETARIO ACTIVO | CUSTODIO ACTIVO | ENCARGADA SI | COMITÉ SEGURIDAD |
|----|---|--------------------|-----------------|--------------|------------------|
| 1  | Elaboración de planificación de creación / actualización de inventario de activos | -                  | I               | R/E          | I                |
| 2  | Realizar reunión de planificación de inventario de activos                        | R                  | C               | I            | -                |
| 3  | Levantamiento/Identificación de Activos de Información                            | R/E                | E               | C            | -                |
| 4  | Clasificación de activos de información   | R/E                | E               | C            |                  |
| 5  | Revisión de Listado de Activos de Información por Propietario                     | R/E                | I/C             | C            | -                |
| 6  | Envío de listado de inventario de activos   | R/E                | I               | I            | -                |
| 7  | Elaboración de inventario de activos de información                               | C                  | -               | R/E          | -                |
| 8  | Revisión de inventario de activos de información                                  | C                  | -               | R/E          | I                |
| 9  | Aprobación de inventario de activos de información                                | I                  | I               | I/C          | R/E              |

#### 8. Registro de Operación.

| REGISTRO                             | ID | RESPONSABLE/DUEÑO DEL REGISTRO               | TIEMPO RETENCIÓN      | SOPORTE | LUGAR |
|--------------------------------------|----|--|-----------------------|---------|-------|
| Inventario de Activos de Información | -  | Encargada(o) de Seguridad de la Información. | 4 años / Archivo UTIC | Digital | PC    |



**LISTA DE ASISTENCIA**  
**Comité de Seguridad de la Información**  
**Implementación PMG- Sistema de Seguridad de la Información**

- I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
  1. Estructura funcional del Sistema de Gestión de Seguridad de la Información y Ciberseguridad al interior de la Agencia de Calidad de la Educación
  2. Procedimiento de Contacto con Autoridades. Control A.6.1.3
  3. Procedimiento de Contacto con Grupos de Interés. Control A.6.1.4
  4. Política de Seguridad para Recursos Humanos. Control A.7.1.2
  5. Procedimiento de elaboración / Actualización de inventario de Activos. Control A.8.1.1 y su registro de operación.
  6. Procedimiento de Asignación y Devolución de Recursos. Control A.8.1.4
  7. Política de Control de Acceso físico y lógico. Control A.9.1.1 y A. 11.1.1
  8. Procedimiento de Inicio de Sesión Seguro. Control A.9.4.2
  9. Política de Ubicación y Protección del Equipamiento de la Agencia de Calidad de la Educación. Control A.11.2.1
  10. Procedimiento de Mantenimiento de Equipos Críticos. Control A.11.02.04
  11. Procedimiento de eliminación o Reutilización de Equipamiento. Control A.11.2.7
  12. Procedimiento de Equipo de Usuario Desatendido. Control A.11.02.08
  13. Política de Escritorio y Pantalla limpios. Control A.11.2.9
  14. Procedimiento de Respaldo de Información. Control A.12.03.01

Fecha: 3 de julio de 2019

| N° | Nombre                   | Cargo                                    | Firma |
|----|--------------------------|--|-------|
| 1  | Juan Bravo               | Secretario Ejecutivo (S)                 |       |
| 2  | Gino Cortez              | Jefe de DEOD (S)                         |       |
| 3  | Cristóbal Alarcón        | Jefe de DIAC                             |       |
| 4  | Mariana Segura           | Jefa de DCA(S) y DAG (S)                 |       |
| 5  | María de la Luz González | Jefa de DIEST (S)                        |       |
| 6  | Andrea Soto Araya        | Encargada de SSI                         |       |
| 7  | Nicol Jeria              | Encargada de Ciberseguridad              |       |
| 8  | Sergio Hidalgo           | Jefe Departamento de Auditoría           |       |
| 9  | Gabriel Cáceres          | Encargado de Unidad de Planificación (s) |       |
| 10 | TATNICK SOTO             | Jefe Unidad TIC                          |       |
| 11 | Yerko Braun              | Profesional DIAC                         |       |
| 12 | CRISTÓBAL ALARCÓN        | Consultor Externo                        |       |



| Procedimiento de Contactos con Autoridades |            |         |                   |
|--|------------|---------|-------------------|
| Nivel de Confidencialidad                  | -          | Páginas | 1 de 11           |
| Fecha versión del documento                | 28-05-2019 | Versión | 1                 |
|  |            | Código  | SGSIC-PRO-A.6.1.3 |
| Procedimiento de Contactos con Autoridades |            |         |                   |

## Procedimiento de Contacto con Autoridades Control A.06.01.03

**Tabla de Contenidos**

|   |          |
|---|----------|
| <b>1. Objetivo.....</b>   | <b>1</b> |
| <b>2. Alcance.....</b>  | <b>1</b> |
| <b>3. Normas y Referencias.....</b>   | <b>2</b> |
| <b>4. Términos y Definiciones. ....</b>   | <b>2</b> |
| <b>5. Roles y Responsabilidades.....</b>  | <b>3</b> |
| <b>6. Eventos de Seguridad de la Información .....</b>  | <b>3</b> |
| <b>6.1 Asignación de Autoridades ante diferentes tipos de evento. ....</b>  | <b>4</b> |
| <b>7. Modo de Operación .....</b>   | <b>4</b> |
| <b>7.1 Flujo de Procedimiento.....</b>  | <b>5</b> |
| <b>7.2 Matriz del Proceso de Contacto con Autoridades en caso de Eventos de Seguridad de la Información. ....</b> | <b>5</b> |
| <b>7.3 Matriz de Responsabilidades. ....</b>  | <b>8</b> |
| <b>8. Registro de Operación.....</b>  | <b>9</b> |

**REVISIONES DEL PROCEDIMIENTO**

| Nº Versión | Fecha      | Motivo de la revisión | Páginas elaboradas o modificadas |
|------------|------------|-----------------------|----------------------------------|
| Uno (1)    | 28/05/2019 | Elaboración inicial   | Todas                            |

| ELABORADO POR  | VALIDACIÓN TÉCNICA             | REVISADO POR  | APROBADO POR                          |
|--|--------------------------------|---|---------------------------------------|
| Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC) | Patrik Soto<br>Jefe Unidad TIC | Andrea Soto Araya<br>Encargada de Seguridad de la Información | Comité de Seguridad de la Información |

**1. Objetivo.**

El objetivo del presente documento es, definir un flujo comunicacional, oficial y estructurado, orientado a hacer frente a los diferentes tipos de eventos que pudiesen afectar la disponibilidad, integridad, confidencialidad, autenticidad y privacidad de los activos de información críticos de la Agencia, identificando aquellas autoridades tanto internas como externas que representan, según sus diferentes competencias, un apoyo para la gestión y solución de éstos.

**2. Alcance.**

Este procedimiento deberá ser aplicado por todos(as) los(as) funcionarios internos de planta, contrata y personal honorarios que tengan acceso de forma directa o indirecta a los activos de información de la Agencia.

### 3. Normas y Referencias.

- Política General de Seguridad de la Información de la Agencia, aprobada por Resolución Exenta N° 0589, de 16 de mayo de 2019, de la Agencia de Calidad de la Educación.
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información.

### 4. Términos y Definiciones.

|  |   |
|--|---|
| <b>Amenaza</b>                               | Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o una organización.  |
| <b>Riesgo</b>                                | Las condiciones de debilidad en los activos que pueden ser afectadas por la existencia de una amenaza concreta, y las consecuencias que esto tiene. Es el efecto o materialización de la amenaza, el cual se puede clasificar respecto de su severidad, considerando su nivel de probabilidad y el impacto que generaría su ocurrencia.   |
| <b>Autoridad</b>                             | Facultad o derecho que posee un individuo o conjunto de individuos para actuar, mandar, o exigir una determinada acción a otros, en virtud del poder que emana de su posición dentro de la organización o institución. En el caso del sistema de seguridad de la información serán entendidas como autoridades, los responsables de los procesos de continuidad del negocio y recuperación ante desastres; y los servicios de emergencia, salud, bomberos y carabineros.  |
| <b>Evento de Seguridad de la Información</b> | Se refiere a la identificación y materialización de una amenaza o riesgo detectado el cual pudiera eventualmente comprometer la continuidad operacional de la Agencia.  |
| <b>Incidente de Seguridad</b>                | Se refiere a la Identificación y materialización de una amenaza o riesgo detectado que afecte la continuidad operacional que afecte activos de información relevantes para la Agencia.  |
| <b>Vulnerabilidad</b>                        | Debilidades propias de las características propias de cada activo, que los exponen a una amenaza o riesgo.  |
| <b>Evento de Seguridad</b>                   | Se refiere a la identificación y materialización de una amenaza o riesgo detectado, que afecte la continuidad operacional dañando activos relevantes de la Agencia  |
| <b>Plan de Contingencia</b>                  | Plan de Acción donde se señala explícitamente, el procedimiento a seguir, ante la ocurrencia de un incidente de seguridad de la información, que comprometa la continuidad operacional de la Agencia.   |
| <b>Activos de Información</b>                | Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta manera es que se distingue la información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.), los equipos, sistemas, infraestructura que soportan esta información y las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales. |
| <b>Contactos</b>                             | Corresponden al nivel de contacto que se necesita ubicar con  |



|                                    |   |
|------------------------------------|---|
| <b>críticos</b>                    | urgencia en caso de dificultades tecnológicas o incidentes.   |
| <b>Red de Seguridad</b>            | Corresponden a números telefónicos públicos de servicios de emergencia, que no referencian la identificación de una persona.  |
| <b>Seguridad de la Información</b> | Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de informar, no repudio y confidencialidad. |

## **5. Roles y Responsabilidades.**

- a) **Funcionarios internos de la Agencia:** Todo colaborador o colaboradora interna de la Agencia de Calidad de la Educación, que de forma directa o indirecta detecte un evento o suceso que pueda perjudicar alguno de los objetivos específicos del SGSIC, establecidos en la Política General de Seguridad de Información, aprobada mediante resolución exenta número 0589, tiene la responsabilidad de informarlo, tanto a su jefatura directa, como a la Encargada(o) de Seguridad de la Información del servicio, según indica el flujo comunicacional de este procedimiento descrito en el punto 7 de este documento.
- b) **Encargada(o) de Seguridad de la Información:** Como Autoridad Interna líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), este rol tiene la responsabilidad de liderar el flujo comunicacional con las autoridades ante a la notificación de un evento de seguridad de información, así como realizar el seguimiento de la misma, apoyando de forma constante en la toma de decisiones.
- c) **Jefatura de Unidad de Tecnologías de Información y Comunicación:** La jefatura de la Unidad TIC, como Autoridad Interna a cargo de velar por la mantención operativa de los servicios tecnológicos de la Agencia, será responsable de recibir, liderar y delegar las acciones necesarias para resolver los eventos de seguridad que estén dentro de su ámbito de responsabilidades, tanto con su equipo, como con los proveedores críticos que estén bajo su gestión.
- d) **Jefatura de División de Administración General:** La jefatura de la DAG, como Autoridad Interna a cargo de la administración general de la institución, será responsable de recibir, liderar y delegar las acciones necesarias para resolver los eventos de seguridad que estén dentro de su ámbito de responsabilidades, tanto a través de la Jefatura de Unidad de Administración General, como a través de los proveedores críticos asociados.

## **6. Eventos de Seguridad de la Información.**

A continuación, se establecen de forma general, los tipos de eventos que pudiesen afectar el correcto funcionamiento de los procesos críticos de la Agencia. Éstos pueden ocasionar daños en los activos de información relevantes para la Agencia, por lo que, para cada uno de ellos, se deberá realizar una eficiente y coordinada gestión comunicacional que permita hacer frente éstos. Parte de esta gestión es el contacto apropiado con las autoridades relevantes y competentes que permitan la mitigación de los efectos de la ocurrencia del mismo.

- a) **Eventos de origen ambiental:** Corresponden a aquellos eventos que suceden sin intervención directa del ser humano. Afectan de forma directa recursos como instalaciones, hardware, redes comunicacionales, soportes de información y equipamiento auxiliar, generando así un impacto directo en la disponibilidad de los activos de información. Como ejemplos de este tipo de eventos, se tiene: desastres naturales.
- b) **Eventos de origen industrial:** Corresponden a aquellos eventos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estos

eventos pueden darse de forma accidental o deliberada, y, al igual que los eventos de origen ambiental, afectan recursos como instalaciones, hardware, redes comunicacionales, soportes de información y equipamiento auxiliar, generando así un impacto directo en la disponibilidad de los activos de información. Como ejemplos de este tipo de eventos, se tiene: daños por agua, fuego y desastres industriales.

- c) Eventos de origen tecnológico:** Corresponden a aquellos eventos que tienen su génesis en el incorrecto o no funcionamiento de los componentes tecnológicos que apalancan los procesos críticos de la Agencia, los cuales pueden ser generados tanto de forma intencional como no intencional por el ser humano. Éstos eventos pueden impactar de forma transversal tanto la disponibilidad, confidencialidad, integridad, autenticidad y privacidad de los activos de información del servicio. Como ejemplos de este tipo de eventos, se tiene: indisponibilidad o intermitencia de plataformas y software, fallas de configuración, vulnerabilidades técnicas, errores de usuarios y/o administradores, difusión de código malicioso, entre otros.
- d) Eventos de origen en el proveedor:** Corresponden a aquellos eventos que tienen su origen en la indisponibilidad o corte de un servicio prestado por un proveedor. Al igual que en el punto anterior, éste tipo de eventos pueden generar un impacto transversal en la disponibilidad, confidencialidad, integridad, autenticidad y privacidad de los activos de información del servicio. Como ejemplos de este tipo de eventos, tenemos: corte de servicio de conexión a internet, indisponibilidad de servicio de correo electrónico y almacenamiento en la nube, corte de servicios básicos.

### **6.1 Asignación de Autoridades ante diferentes tipos de evento.**

A continuación, se dan a conocer aquellos contactos críticos a los que se debe recurrir en caso de la ocurrencia de un evento de seguridad de la información según lo señalado en el punto anterior:

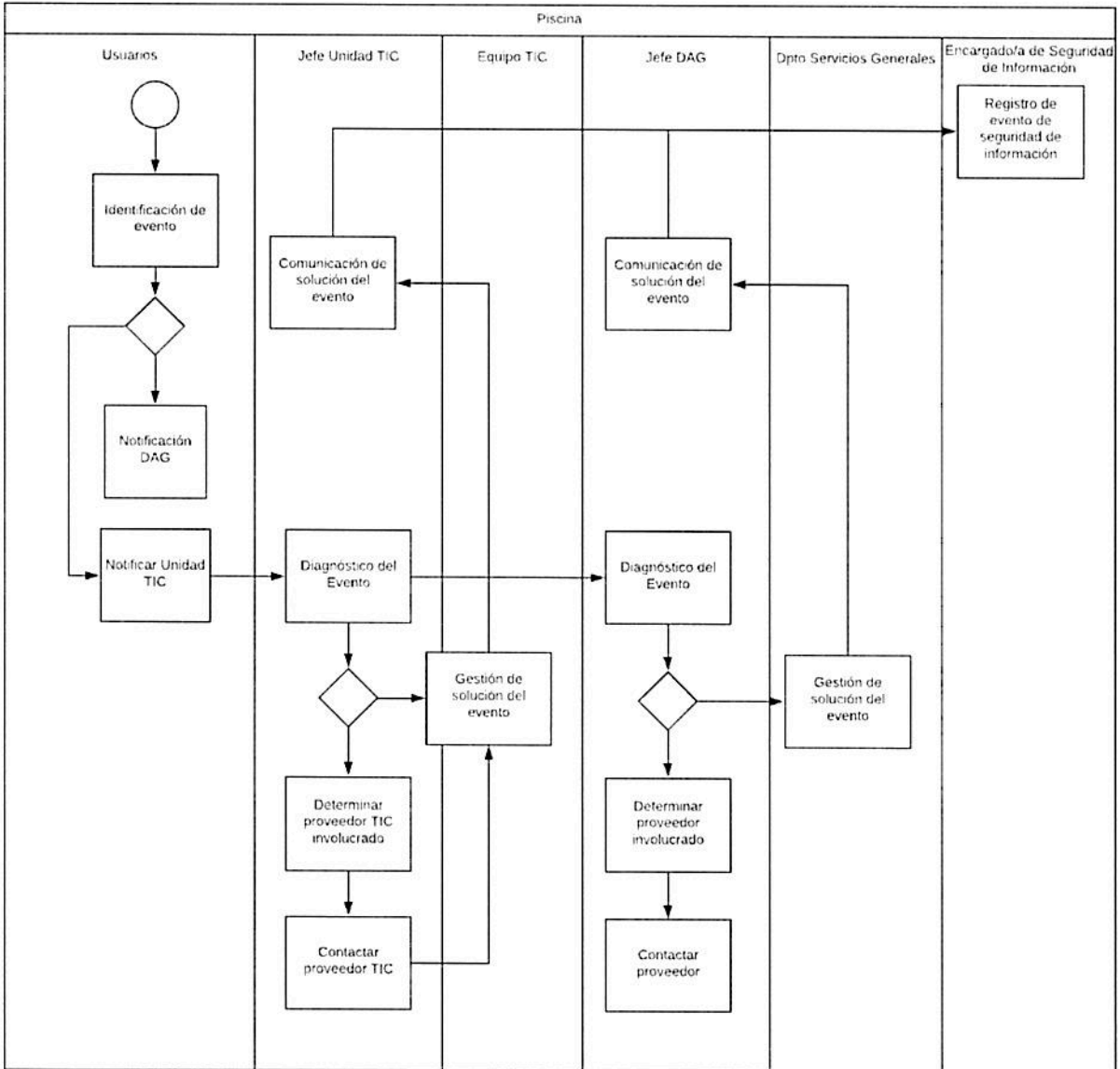
| <b>TIPO DE EVENTO</b>      | <b>AUTORIDAD</b>                                | <b>INTERNA/EXTERNA</b>   | <b>CONTACTO</b> |
|----------------------------|---|--------------------------|-----------------|
| <b>Origen Ambiental</b>    | <b>Jefe DAG / Unidad Administración General</b> | <b>Interna</b>           | <b>Anexo I</b>  |
| <b>Origen Industrial</b>   | <b>Jefe DAG / Unidad Administración General</b> | <b>Interna</b>           | <b>Anexo I</b>  |
| <b>Origen Tecnológico</b>  | <b>Jefe Unidad TIC</b>                          | <b>Interna</b>           | <b>Anexo I</b>  |
| <b>Origen en Proveedor</b> | <b>Jefe DAG/Unidad TIC y Proveedor</b>          | <b>Interna y Externa</b> | <b>Anexo II</b> |

Para estos efectos, es responsabilidad de la División, Departamento o Unidad encargada de gestionar el incidente de seguridad recurrir al listado de contactos críticos de la Agencia. Este debe contener una lista amplia de contactos de emergencia, para atender cualquier situación imprevista.

### **7. Modo de Operación.**

De acuerdo con los eventos descritos anteriormente, se establece un flujo comunicacional específico, en donde, de acuerdo al tipo de evento, se definen las autoridades pertinentes basado en su ámbito de responsabilidades. De esta forma, el flujo comunicacional es el siguiente:

## 7.1 Flujo de Procedimiento.



## 7.2 Matriz del Proceso de Contacto con Autoridades en caso de Eventos de Seguridad de la Información.

| ID | ACTIVIDAD                          | DESCRIPCIÓN   | RESPONSABLE      | ID ACTIVIDAD SIGUIENTE |
|----|------------------------------------|---|------------------|------------------------|
| 1  | Comunicación preliminar del evento | <p>Se debe notificar de forma inmediata, sobre el evento de seguridad a:</p> <ul style="list-style-type: none"> <li>- Jefatura Directa</li> <li>- Encargada(o) de Seguridad de la Información</li> </ul> <p>Esta notificación debe hacerse mediante el medio de comunicación más eficiente que se encuentre disponible, o bajo la siguiente prioridad:</p> <ul style="list-style-type: none"> <li>- Sistema de Tickets</li> <li>- Anexo telefónico</li> <li>- Correo institucional</li> <li>- Celular personal</li> </ul> | Funcionarios(as) | 2                      |

| ID | ACTIVIDAD                        | DESCRIPCIÓN   | RESPONSABLE                     | ID ACTIVIDAD SIGUIENTE |
|----|----------------------------------|---|---------------------------------|------------------------|
| 2  | Determinación del tipo de evento | <p>Según los tipos de evento descritos en el punto seis (6) de este documento, se pueden dar las siguientes posibilidades:</p> <ul style="list-style-type: none"> <li>- El evento es de origen tecnológico (3)</li> <li>- El evento es de origen natural y/o industrial (5)</li> </ul>  | Funcionario(a)                  | 3 o 5                  |
| 3  | Notificar a Unidad TIC           | <p>Se debe notificar del evento a:</p> <ul style="list-style-type: none"> <li>- Jefe de Unidad TIC</li> <li>- Soporte Interno TIC</li> </ul> <p>La notificación del evento debe indicar la mayor cantidad de antecedentes sobre el mismo y debe hacerse mediante el medio de comunicación más eficiente que se encuentre disponible, o bajo la siguiente prioridad:</p> <ul style="list-style-type: none"> <li>- Anexo telefónico</li> <li>- Correo institucional</li> <li>- Celular personal</li> </ul> <p><b>NOTA:</b> El detalle de contacto con el equipo TIC se encuentra en el documento de "Listado de Responsables por tipo de Evento de Seguridad", sección de contactos para soporte interno.</p> | Funcionario(a)                  | 4                      |
| 4  | Diagnóstico del evento           | <p>Al momento de diagnosticar el evento reportado, se pueden dar las siguientes alternativas:</p> <ul style="list-style-type: none"> <li>- El evento puede ser solucionado por el equipo TIC (4A)</li> <li>- El evento incluye a un proveedor TIC (4B)</li> </ul>   | Jefe de Unidad TIC              | 4A o 4B                |
| 4A | Solución de evento               | Se deben realizar las actividades necesarias para volver a la normalidad en el servicio tecnológico afectado.   | Jefe de Unidad TIC / Equipo TIC | 7                      |

| ID | ACTIVIDAD                                | DESCRIPCIÓN  | RESPONSABLE                                 | ID ACTIVIDAD SIGUIENTE |
|----|--|--|---|------------------------|
| 4B | Determinar proveedor TIC involucrado     | <p>Se debe determinar el o los proveedores TIC involucrados en el evento para establecer contacto directo con la contraparte asignada. Se pueden dar las siguientes alternativas:</p> <ul style="list-style-type: none"> <li>- Entel</li> <li>- Microsoft</li> <li>- Google</li> <li>- AWS</li> </ul> <p><b>NOTA:</b> El detalle de los servicios asociados a cada proveedor están detallados en el documento de "Listado de Responsables por tipo de Evento de Seguridad", sección de proveedores TIC</p> | Jefe de Unidad TIC                          | 4C                     |
| 4C | Contactar proveedor TIC                  | <p>Se debe establecer contacto con la contraparte asignada con el proveedor para soporte técnico.</p> <p><b>NOTA:</b> El detalle de contacto asociado a cada proveedor se encuentra en el documento de "Listado de Responsables por tipo de Evento de Seguridad", sección de proveedores TIC</p>   | Jefe de Unidad TIC                          | 4a                     |
| 5  | Notificar a DAG                          | <p>Se debe notificar del evento a:</p> <ul style="list-style-type: none"> <li>- Jefe DAG</li> </ul> <p>La notificación del evento debe indicar la mayor cantidad de antecedentes sobre el mismo.</p> <p><b>NOTA:</b> El detalle de contacto para notificación de eventos se encuentra en el documento de "Listado de Responsables por tipo de Evento de Seguridad" de contactos de Administración General.</p>   | Funcionario(a)                              | 6                      |
| 6  | Diagnóstico del evento                   | <p>Al momento de diagnosticar el evento reportado, se pueden dar las siguientes alternativas:</p> <ul style="list-style-type: none"> <li>- El evento puede ser solucionado por alguna unidad DAG(6A)</li> <li>- El evento incluye a un proveedor General (6B)</li> </ul>   | Jefe DAG                                    | 6A o 6B                |
| 6A | Solución de evento                       | Se deben realizar las actividades necesarias para volver a la normalidad en el servicio tecnológico afectado.  | Jefe DAG / Unidad de Administración General | 7                      |
| 6B | Determinar proveedor General involucrado | Se debe determinar el o los proveedores Generales involucrados en el evento para establecer contacto directo con la contraparte asignada.  | Jefe DAG                                    | 6C                     |

| ID | ACTIVIDAD   | DESCRIPCIÓN   | RESPONSABLE                              | ID ACTIVIDAD SIGUIENTE |
|----|---|---|--|------------------------|
| 6C | Contactar proveedor General                       | Se debe establecer contacto con la contraparte asignada por el proveedor.<br><br><b>NOTA:</b> El detalle de contacto asociado a cada proveedor se encuentra en el documento de "Listado de Responsables por tipo de Evento de Seguridad" sección de proveedores TIC   | Jefe DAG                                 | 6A                     |
| 7  | Comunicación de solución de evento                | Se debe notificar la solución definitiva del evento a:<br><br>- Encargada de Seguridad de la Información<br>- Jefatura directa del funcionario(a) que alertó del evento<br>- Equipos participantes en las actividades de solución del evento<br><br>La comunicación se debe llevar a cabo mediante el correo electrónico corporativo. | Jefe Unidad TIC o Jefe DAG               | 8                      |
| 8  | Registro de evento de seguridad de la información | Se debe registrar el evento según lo establecido en el Procedimiento de Gestión de Incidentes de Seguridad de la Información.   | Encargada de Seguridad de la Información | FIN                    |

### 7.3 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

Se esta forma, la matriz de responsabilidades se estructura de la siguiente manera:

| ID | ACTIVIDAD                          | FUNCI<br>ONARI<br>O | JEFATU<br>RA<br>DIRECT<br>A | ENCARGA<br>DA SI | JEFE<br>TIC | JEFE<br>DAG | EQUIP<br>O TIC | UNIDA<br>D<br>ADMI<br>N.<br>GENER<br>AL |
|----|------------------------------------|---------------------|-----------------------------|------------------|-------------|-------------|----------------|---|
| 1  | Comunicación preliminar del evento | E/R                 | I                           | I                | -           | -           | -              | -                                       |
| 2  | Determinación del tipo de evento   | R                   | C                           | I                | -           | C           | -              | -                                       |
| 3  | Notificar a Unidad TIC             | R/E                 | I                           | I                | I           | -           | I              | -                                       |
| 4  | Diagnóstico del evento             | -                   | -                           | C/I              | R/A         | -           | E              | -                                       |
| 4A | Solución de evento                 | -                   | I                           | C/I              | R/A         | -           | E              | -                                       |
| 4B | Determinar proveedor TIC           | -                   | -                           | C/I              | R/A         | -           | E              | -                                       |

|           |  |     |   |     |     |     |   |    |
|-----------|--|-----|---|-----|-----|-----|---|----|
|           | <b>involucrado</b>                                       |     |   |     |     |     |   |    |
| <b>4C</b> | <b>Contactar proveedor TIC</b>                           | -   | - | C/I | R/A | -   | E | -  |
| <b>5</b>  | <b>Notificar a DAG</b>                                   | R/E | I | I   | -   | C   | - | I  |
| <b>6</b>  | <b>Diagnóstico del evento</b>                            | -   | - | C/I | -   | R/A | - | E  |
| <b>6A</b> | <b>Solución de evento</b>                                | -   | I | C/I | -   | R/A | - | E  |
| <b>6B</b> | <b>Determinar proveedor General involucrado</b>          | -   | - | C/I | -   | R/A | - | E  |
| <b>6C</b> | <b>Contactar proveedor General</b>                       | -   | - | C/I | -   | R/A | - | E  |
| <b>7</b>  | <b>Comunicación de solución de evento</b>                | -   | I | I   | R/E | R/E | I | I- |
| <b>8</b>  | <b>Registro de evento de seguridad de la información</b> | C   | C | R/E | C   | C   | C | C  |

**8. Registro de Operación.**

| <b>REGISTRO</b>   | <b>ID</b> | <b>RESPONSABLE/DUEÑO DEL REGISTRO</b>       | <b>TIEMPO RETENCIÓN</b> | <b>SOPORTE</b> | <b>LUGAR</b>                |
|---|-----------|---|-------------------------|----------------|-----------------------------|
| Listado de responsables por tipo de evento de Seguridad | -         | Encargado(a) de Seguridad de la Información | 4 años / Archivo UTIC   | Digital        | PC Responsable del Registro |

**ANEXO I**

**Listado de Responsables por tipo de Eventos de Seguridad de la Agencia de Calidad de la Educación (ejemplo de formato)**

**1. Soporte Informático Agencia de Calidad de la Educación.**

| <b>NOMBRE</b> | <b>ROL</b> | <b>CELULAR</b> | <b>ANEXO</b> | <b>CORREO ELECTRÓNICO</b> |
|---------------|------------|----------------|--------------|---------------------------|
|               |            |                |              |                           |
|               |            |                |              |                           |

**2. Seguridad de la Información.**

| <b>NOMBRE</b> | <b>ROL</b> | <b>CELULAR</b> | <b>ANEXO</b> | <b>CORREO ELECTRÓNICO</b> |
|---------------|------------|----------------|--------------|---------------------------|
|               |            |                |              |                           |
|               |            |                |              |                           |

**3. Proveedores TIC.**

| <b>PROVEEDOR</b> | <b>SERVICIO</b> | <b>NOMBRE</b> | <b>CELULAR/FONO</b> | <b>CORREO ELECTRÓNICO</b> |
|------------------|-----------------|---------------|---------------------|---------------------------|
|                  |                 |               |                     |                           |
|                  |                 |               |                     |                           |
|                  |                 |               |                     |                           |
|                  | -               |               |                     |                           |
|                  | -               |               |                     |                           |
|                  | -               |               |                     |                           |

**4. Proveedores Generales (a través del Departamento de Administración General).**

| <b>PROVEEDOR</b> | <b>SERVICIO</b> | <b>NOMBRE</b> | <b>CELULAR/FONO</b> | <b>CORREO ELECTRÓNICO</b> |
|------------------|-----------------|---------------|---------------------|---------------------------|
|                  |                 |               |                     |                           |
|                  |                 |               |                     |                           |
|                  |                 |               |                     |                           |

**5. Contactos de Servicios Básicos Genéricos.**

| <b>PROVEEDOR</b> | <b>CORREO ELECTRÓNICO</b> |
|------------------|---------------------------|
|                  |                           |



|  |  |
|--|--|
|  |  |
|  |  |
|  |  |

**Aprobado por:**

**Firma:**

**Fecha de Actualización:**



## LISTA DE ASISTENCIA

### Comité de Seguridad de la Información

#### Implementación PMG- Sistema de Seguridad de la Información

- I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
  1. Estructura funcional del Sistema de Gestión de Seguridad de la Información y Ciberseguridad al interior de la Agencia de Calidad de la Educación
  2. Procedimiento de Contacto con Autoridades. Control A.6.1.3
  3. Procedimiento de Contacto con Grupos de Interés. Control A.6.1.4
  4. Política de Seguridad para Recursos Humanos. Control A.7.1.2
  5. Procedimiento de elaboración / Actualización de inventario de Activos. Control A.8.1.1 y su registro de operación.
  6. Procedimiento de Asignación y Devolución de Recursos. Control A.8.1.4
  7. Política de Control de Acceso físico y lógico. Control A.9.1.1 y A. 11.1.1
  8. Procedimiento de Inicio de Sesión Seguro. Control A.9.4.2
  9. Política de Ubicación y Protección del Equipamiento de la Agencia de Calidad de la Educación. Control A.11.2.1
  10. Procedimiento de Mantenimiento de Equipos Críticos. Control A.11.02.04
  11. Procedimiento de eliminación o Reutilización de Equipamiento. Control A.11.2.7
  12. Procedimiento de Equipo de Usuario Desatendido. Control A.11.02.08
  13. Política de Escritorio y Pantalla limpios. Control A.11.2.9
  14. Procedimiento de Respaldo de Información. Control A.12.03.01

Fecha: 3 de julio de 2019

| N° | Nombre                   | Cargo                                    | Firma |
|----|--------------------------|--|-------|
| 1  | Juan Bravo               | Secretario Ejecutivo (S)                 |       |
| 2  | Gino Cortez              | Jefe de DEOD (S)                         |       |
| 3  | Cristóbal Alarcón        | Jefe de DIAC                             |       |
| 4  | Mariana Segura           | Jefa de DEIA(S) y DAG (S)                |       |
| 5  | María de la Luz González | Jefa de DIEST (S)                        |       |
| 6  | Andrea Soto Araya        | Encargada de SSI                         |       |
| 7  | Nicol Jeria              | Encargada de Ciberseguridad              |       |
| 8  | Sergio Hidalgo           | Jefe Departamento de Auditoría           |       |
| 9  | Gabriel Cáceres          | Encargado de Unidad de Planificación (s) |       |
| 10 | YATINCK SOTO S.          | Jefe Unidad TIC                          |       |
| 11 | Yerko Braun              | Proteccionista DIAC                      |       |
| 12 | Claudio Corado           | Consultor Externo                        |       |

|   |   |                   |         |                          |
|---|---|-------------------|---------|--------------------------|
| <br><b>Agencia de<br/>Calidad de la<br/>Educación</b><br><br>Gobierno de Chile | <b>Procedimiento de Mantenición de Equipos Críticos</b> |                   |         |                          |
|   | Nivel de Confidencialidad                               | -                 | Páginas | <b>1 de 11</b>           |
|   | Fecha versión del documento                             | <b>31-05-2019</b> | Versión | <b>0</b>                 |
|   |   |                   | Código  | <b>SGIC-PRO-A.11.2.4</b> |
| <b>Procedimiento de Mantenición de Equipos Críticos</b>   |   |                   |         |                          |

## Procedimiento de Mantenición de Equipos Críticos


### Control A.11.02.04

#### Tabla de Contenidos

|            |  |           |
|------------|--|-----------|
| <b>1</b>   | <b>Objetivo.....</b>   | <b>1</b>  |
| <b>2</b>   | <b>Alcance.....</b>  | <b>1</b>  |
| <b>3</b>   | <b>Normas y Referencias.....</b>                                   | <b>2</b>  |
| <b>4</b>   | <b>Términos y Definiciones.....</b>                                | <b>2</b>  |
| <b>5.</b>  | <b>Roles y Responsabilidades.....</b>                              | <b>3</b>  |
| <b>6.</b>  | <b>Definición de Equipamiento Crítico.....</b>                     | <b>3</b>  |
| <b>7.</b>  | <b>Modo de Operación.....</b>                                      | <b>3</b>  |
| <b>7.1</b> | <b>Flujo de Procedimiento para Mantenciones Preventivas.....</b>   | <b>4</b>  |
| <b>7.2</b> | <b>Matriz del Procedimiento para Mantenciones Preventivas.....</b> | <b>4</b>  |
| <b>7.3</b> | <b>Flujo de Procedimiento para Mantenciones Correctivas.....</b>   | <b>7</b>  |
| <b>7.4</b> | <b>Matriz de Procedimientos para Mantenciones Correctivas.....</b> | <b>7</b>  |
| <b>7.5</b> | <b>Matriz de Responsabilidades.....</b>                            | <b>9</b>  |
| <b>8.</b>  | <b>Registro de Operación.....</b>                                  | <b>10</b> |

#### REVISIONES DEL PROCEDIMIENTO

| Nº Versión | Fecha      | Motivo de la revisión | Páginas elaboradas o modificadas |
|------------|------------|-----------------------|----------------------------------|
| Cero (0)   | 31/05/2019 | Elaboración inicial   | Todas                            |

|   |   |  |                     |
|---|---|--|---------------------|
| <b>ELABORADO POR</b>  | <b>VALIDACIÓN TÉCNICA</b>   | <b>APROBADO POR</b>  | <b>APROBADO POR</b> |
| Sistema de Gestión de Seguridad de Información y Ciberseguridad | Patrik Soto<br>Jefe Unidad TIC  | Andrea Soto Araya<br>Encargada de Seguridad de la Información                        | Comité de SGSIC     |
|   |  |  |                     |

#### 1. Objetivo.

En función de lo establecido en el punto tres (3), sobre el Marco General de Protección de los Activos de Información, de la Política de Seguridad de la Información de la Agencia de Calidad de la Educación, en adelante la Agencia, el objetivo del presente documento es especificar el procedimiento asociado al mantenimiento tanto preventivo como correctivo de los recursos o equipamiento computacional, de soporte y plataforma de la Agencia, buscando así, la mitigación de la ocurrencia de riesgos que desencadenen algún evento o incidente que se pueda producir por falta de mantenimiento al equipamiento, y, en su defecto, la reducción de la gravedad del impacto cuando éstos se producen.

#### 2. Alcance.

Este procedimiento se debe aplicar a todo el equipamiento computacional, de soporte y plataforma de la Agencia, considerado como crítico, es decir, aquellos que por la relevancia

de los procesos que soportan, no puedan presentar indisponibilidad prolongada de su servicio.

Adicionalmente, se consideran dentro del alcance de este procedimiento, las mantenciones tanto preventivas como correctivas.

### 3. Normas y Referencias.

- Política General de Seguridad de la Información de la Agencia de Calidad de la Educación
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información.

### 4. Términos y Definiciones.

|  |   |
|--|---|
| <b>Amenaza</b>                               | Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o una organización.  |
| <b>Riesgo</b>                                | Las condiciones de debilidad en los activos que pueden ser afectadas por la existencia de una amenaza concreta, y las consecuencias que esto tiene. Es el efecto o materialización de la amenaza, el cual se puede clasificar respecto de su severidad, considerando su nivel de probabilidad y el impacto que generaría su ocurrencia.   |
| <b>Autoridad</b>                             | Facultad o derecho que posee un individuo o conjunto de individuos para actuar, mandar, o exigir una determinada acción a otros, en virtud del poder que emana de su posición dentro de la organización o institución. En el caso del sistema de seguridad de la información serán entendidas como autoridades, los responsables de los procesos de continuidad del negocio y recuperación ante desastres; y los servicios de emergencia, salud, bomberos y carabineros.  |
| <b>Evento de Seguridad de la Información</b> | Se refiere a la identificación y materialización de una amenaza o riesgo detectado el cual pudiera eventualmente comprometer la continuidad operacional de la Agencia.  |
| <b>Incidente de Seguridad</b>                | Se refiere a la Identificación y materialización de una amenaza o riesgo detectado que afecte la continuidad operacional que afecte activos de información relevantes para la Agencia.  |
| <b>Vulnerabilidad</b>                        | Debilidades propias de las características propias de cada activo, que los exponen a una amenaza o riesgo.  |
| <b>Evento de Seguridad</b>                   | Se refiere a la identificación y materialización de una amenaza o riesgo detectado, que afecte la continuidad operacional dañando activos relevantes de la Agencia  |
| <b>Plan de Contingencia</b>                  | Plan de Acción donde se señala explícitamente, el procedimiento a seguir, ante la ocurrencia de un incidente de seguridad de la información, que comprometa la continuidad operacional de la Agencia.   |
| <b>Activos de Información</b>                | Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta manera es que se distingue la información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.), los equipos, sistemas, infraestructura que soportan esta información y las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales. |

|                                    |   |
|------------------------------------|---|
| <b>Contactos críticos</b>          | Corresponden al nivel de contacto que se necesita ubicar con urgencia en caso de dificultades tecnológicas o incidentes.  |
| <b>Red de Seguridad</b>            | Corresponden a números telefónicos públicos de servicios de emergencia, que no referencian la identificación de una persona.  |
| <b>Seguridad de la Información</b> | Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de informar, no repudio y confidencialidad. |

## **5. Roles y Responsabilidades.**

- a) **Encargada(o) de Seguridad de la Información:** Como rol líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), tiene la responsabilidad de monitorear el cumplimiento de este procedimiento, así como de mantenerse al tanto de los diferentes eventos que desencadenen mantenciones de tipo correctivas a los equipos críticos de la Agencia.
- b) **Jefatura de Unidad de Tecnologías de Información y Comunicación:** La jefatura de la Unidad TIC, como Autoridad Interna a cargo de velar por la mantención operativa de los servicios tecnológicos de la Agencia, debe velar por el fiel cumplimiento del proceso en cuanto a mantención del equipamiento.
- c) **Encargado de Plataforma:** El encargado de plataforma será el rol responsable de administrar y ejecutar el proceso de mantención tanto preventiva como correctiva, de los recursos tecnológicos a los que este procedimiento hace referencia en su alcance.

## **6. Definición de Equipamiento Crítico.**

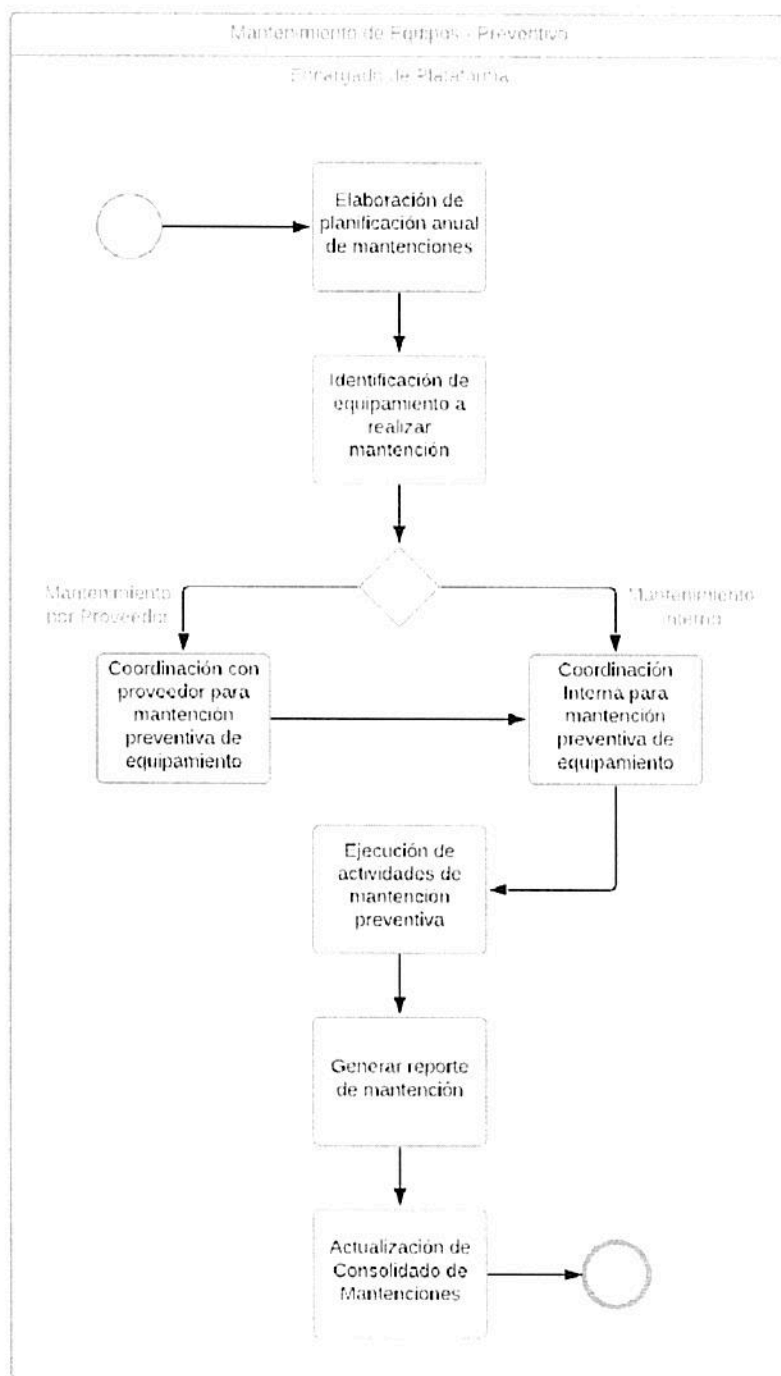
Dado que la actividad central de la Agencia, declarada en la Política General de Seguridad de Información, corresponde a la manipulación de información propia confidencial y sensible de terceros, y que ésta debe ser segura durante todo su ciclo de vida, es que se declaran como críticos todos aquellos elementos tecnológicos que dan soporte a las fases del ciclo de vida antes mencionado. Dentro de este conjunto de equipamiento tecnológico, se encuentran:

- SAI o UPS
- Storage
- Plataforma de Virtualización (VMWare)
- Equipamiento de Comunicaciones (Switches)
- Planta telefónica; Cisco Call Manager, SBC, Liric GSM
- Equipamiento de Firewall
- Servidores

## **7. Modo de Operación.**

A continuación, se describen los flujos procedimentales para las mantenciones tanto preventivas como correctivas del equipamiento tecnológico crítico:

## 7.1 Flujo de Procedimiento para Mantenciones Preventivas.



## 7.2 Matriz del Procedimiento para Mantenciones Preventivas.

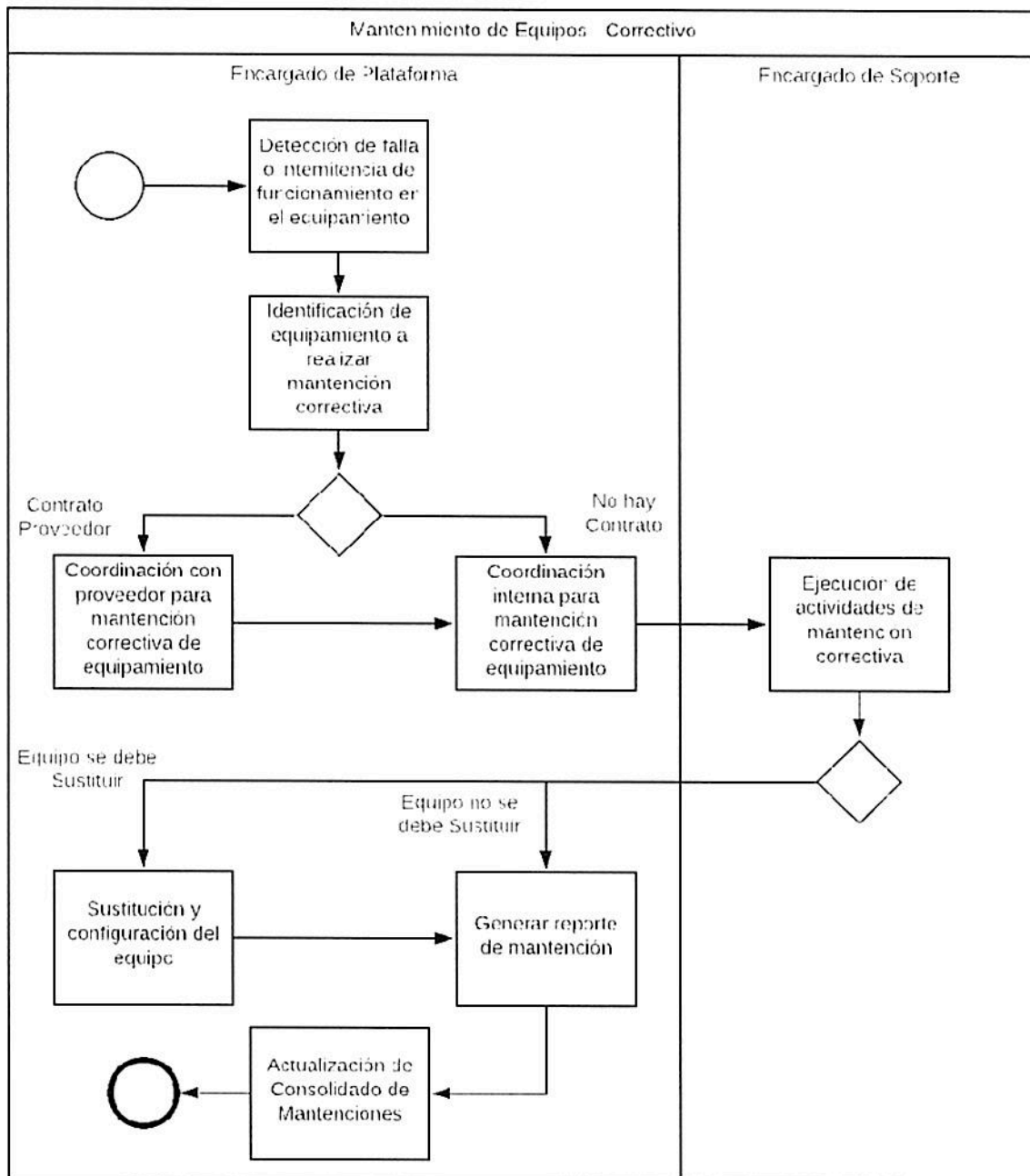
| ID | ACTIVIDAD | DESCRIPCIÓN | RESPONSABLE | ID ACTIVIDAD SIGUIENTE |
|----|-----------|-------------|-------------|------------------------|
|----|-----------|-------------|-------------|------------------------|

| ID | ACTIVIDAD   | DESCRIPCIÓN  | RESPONSABLE             | ID ACTIVIDAD SIGUIENTE |
|----|---|--|-------------------------|------------------------|
| 1  | Elaboración de planificación anual de mantenencias preventivas        | Se debe realizar anualmente, una planificación de mantenencias preventivas, calendarizando las actividades a lo largo del año. Esta planificación debe considerar cada área y tipo de equipamiento, además de que éstas se deben ejecutar fuera de horario laboral con el objetivo de no entorpecer las funciones de los colaboradores(as) de la Agencia y realizarlas con celeridad y mayor organización. | Encargado de Plataforma | 2                      |
| 2  | Identificación de equipamiento a realizar mantención                  | Se deben identificar los equipos o recursos a los cuales les corresponde la mantención preventiva según la planificación. Se pueden dar las siguientes alternativas:<br>- El mantenimiento se debe hacer mediante proveedor (3)<br>- El mantenimiento se realiza con personal interno (4)  | Encargado de Plataforma | 3 o 4                  |
| 3  | Coordinación con proveedor para mantención preventiva de equipamiento | Se debe coordinar con el proveedor apropiado, la ejecución de las mantenencias preventivas consideradas en el alcance según planificación. Éstas deben estar alineadas con las definiciones descritas en la actividad uno (1) de este flujo.<br><br><b>NOTA:</b> Las actividades de mantención del proveedores deben ser supervisadas por el Encargado de Soporte.   | Encargado de Plataforma | 4                      |

| <b>ID</b> | <b>ACTIVIDAD</b>  | <b>DESCRIPCIÓN</b>  | <b>RESPONSABLE</b>      | <b>ID ACTIVIDAD SIGUIENTE</b> |
|-----------|---|---|-------------------------|-------------------------------|
| 4         | Coordinación interna para mantención preventiva de equipamiento | <p>Se deben coordinar de forma interna, y al menos con 24 horas de anticipación, las actividades de mantención consideradas en el alcance de la planificación, se debe considerar:</p> <ul style="list-style-type: none"> <li>- Coordinación con Encargado de Soporte, quien ejecutará las actividades de mantención cuando estas se lleven a cabo de forma interna.</li> <li>- Comunicación, ya sea a la organización completa o a aquellos roles directamente involucrados en esta actividad, las medidas y consideraciones que deben tener de forma previa a la ejecución de éstas.</li> </ul> | Encargado de Plataforma | 5                             |
| 5         | Ejecución de actividades de mantención preventiva               | Se deben ejecutar las actividades de mantención preventiva consideradas en el alcance de la planificación.  | Encargado de Plataforma | 6                             |
| 6         | Generar reporte de mantención                                   | Se debe generar el reporte de mantención según lo indicado en el Anexo 1 de este documento.   | Encargado de Plataforma | 7                             |
| 7         | Actualización de Consolidado de Mantenciones                    | Se debe actualizar el consolidado de mantenciones preventivas según se indica en el Anexo 2 de este documento.  | Encargado de Plataforma | FIN                           |



### 7.3 Flujo de Procedimiento para Mantenciones Correctivas.



### 7.4 Matriz de Procedimientos para Mantenciones Correctivas.

| ID | ACTIVIDAD | DESCRIPCIÓN | RESPONSABLE | ID ACTIVIDAD SIGUIENTE |
|----|-----------|-------------|-------------|------------------------|
|----|-----------|-------------|-------------|------------------------|

| ID | ACTIVIDAD   | DESCRIPCIÓN  | RESPONSABLE             | ID ACTIVIDAD SIGUIENTE |
|----|---|--|-------------------------|------------------------|
| 1  | Detección de falla o intermitencia de funcionamiento en el equipamiento | <p>La detección de fallas en el equipamiento crítico se puede dar de las siguientes formas:</p> <ul style="list-style-type: none"> <li>- Indicadores de monitoreo, donde el mismo personal de la Unidad de TIC detecta la falla.</li> <li>- Mediante el sistema de tickets de la organización, donde un colaborador o colaboradora notifica fallas en el funcionamiento del equipamiento tecnológico.</li> </ul>                         | Encargado de Plataforma | 2                      |
| 2  | Identificación de equipamiento a realizar mantención correctiva         | <p>Si bien la notificación de la falla en el equipamiento puede llegar desde dos fuentes distintas, se debe identificar claramente qué elemento tecnológico presenta la falla para proceder a su mantención correctiva. Se pueden dar las siguientes alternativas:</p> <ul style="list-style-type: none"> <li>- El equipo cuenta con contrato con proveedor (3)</li> <li>- El equipo no cuenta con contrato con proveedor (4)</li> </ul> | Encargado de Plataforma | 3 o 4                  |
| 3  | Coordinación con proveedor para mantención correctiva de equipamiento   | <p>Se debe coordinar con el proveedor apropiado, la ejecución de las mantenciones correctivas asociadas a la falla presentada.</p> <p><b>NOTA:</b> Las actividades de mantención del proveedores deben ser supervisadas por el Encargado de Soporte.</p>   | Encargado de Plataforma | 4                      |

| ID | ACTIVIDAD   | DESCRIPCIÓN   | RESPONSABLE             | ID ACTIVIDAD SIGUIENTE |
|----|---|---|-------------------------|------------------------|
| 4  | Coordinación interna para mantención correctiva de equipamiento | Se deben coordinar de forma interna, y al menos con 24 horas de anticipación, las actividades de mantención consideradas en el alcance de la planificación, se debe considerar:<br>- Coordinación con Encargado de Soporte, quien ejecutará las actividades de mantención cuando estas se lleven a cabo de forma interna.<br>- Comunicación, ya sea a la organización completa o a aquellos roles directamente involucrados en esta actividad, las medidas y consideraciones que deben tener de forma previa a la ejecución de éstas. | Encargado de Plataforma | 5                      |
| 5  | Ejecución de actividades de mantención correctiva               | Se deben ejecutar las actividades de mantención preventiva consideradas en el alcance de la planificación. Se pueden dar las siguientes opciones:<br>- El equipo debe ser reemplazo (6).<br>- El equipo debe ser reparado (7)   | Encargado de Soporte    | 6 o 7                  |
| 6  | Sustitución y configuración del equipo                          | El equipo debe ser reemplazo por uno nuevo, el cual debe ser configurado, ya sea por el proveedor o por personal interno según corresponda.   | Encargado de Plataforma | 7                      |
| 7  | Generar reporte de mantención                                   | Se debe generar el reporte de mantención según lo indicado en el Anexo 1 de este documento.   | Encargado de Plataforma | 8                      |
| 8  | Actualización de Consolidado de Mantenciones                    | Se debe actualizar el consolidado de mantenciones preventivas según se indica en el Anexo 2 de este documento.  | Encargado de Plataforma | FIN                    |

### **7.5 Matriz de Responsabilidades.**

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

De esta forma, la matriz de responsabilidades para la mantención preventiva del equipamiento se estructura de la siguiente manera:

| ID | ACTIVIDAD   | ENC. SI | JEF E TIC | ENC. PLATAFORMA | ENC. SOPORTE |
|----|---|---------|-----------|-----------------|--------------|
| 1  | Elaboración de planificación anual de mantenciones preventivas        | I       | A         | R/E             | I            |
| 2  | Identificación de equipamiento a realizar mantención                  | I       | I         | R               | I            |
| 3  | Coordinación con proveedor para mantención preventiva de equipamiento | I       | A         | R/E             | I            |
| 4  | Coordinación interna para mantención preventiva de equipamiento       | I       | I         | R/E             | I            |
| 5  | Ejecución de actividades de mantención preventiva                     | I       | I         | R               | E            |
| 6  | Generar reporte de mantención   |         |           | A               | R            |
| 7  | Actualización de Consolidado de Mantenciones                          | I       | I         | R               | -            |

Así mismo, la matriz de responsabilidades para la mantención correctiva del equipamiento se estructura de la siguiente manera:

| ID | ACTIVIDAD   | ENC. SI | JEF E TIC | ENC. PLATAFORMA | ENC. SOPORTE |
|----|---|---------|-----------|-----------------|--------------|
| 1  | Detección de falla o intermitencia de funcionamiento en el equipamiento | I       | I         | R               | R            |
| 2  | Identificación de equipamiento a realizar mantención correctiva         | I       | I         | R/C             | E/C          |
| 3  | Coordinación con proveedor para mantención correctiva de equipamiento   | I       | A         | R/E             | I            |
| 4  | Coordinación interna para mantención preventiva de equipamiento         | I       | I         | R/E             | I            |
| 5  | Ejecución de actividades de mantención correctiva                       | I       | I         | R               | E            |
| 6  | Sustitución y configuración del equipo                                  | I       | A         | R               | E            |
| 7  | Generar reporte de mantención   | -       | -         | A               | R            |
| 8  | Actualización de Consolidado de Mantenciones                            | I       | I         | R               | -            |

#### 8. Registro de Operación.

| REGISTRO  | ID | RESPONSABLE/DUEÑO DEL REGISTRO | TIEMPO RETENCIÓN      | SOPORTE | LUGAR                      |
|---|----|--------------------------------|-----------------------|---------|----------------------------|
| Planificación anual de mantenciones preventivas | -  | Encargado de Plataforma        | 1 años / Archivo UTIC | Digital | PC Encargado de Plataforma |

| <b>REGISTRO</b>                                      | <b>ID</b> | <b>RESPONSABLE/D<br/>UEÑO DEL<br/>REGISTRO</b> | <b>TIEMPO<br/>RETENCIÓN</b>    | <b>SOPORTE</b> | <b>LUGAR</b>                        |
|--|-----------|--|--------------------------------|----------------|-------------------------------------|
| Consolidado<br>anual de<br>reportes de<br>mantención | -         | Encargado<br>Plataforma                        | de<br>1 años /<br>Archivo UTIC | Digital        | PC<br>Encargado<br>de<br>Plataforma |




**LISTA DE ASISTENCIA**  
**Comité de Seguridad de la Información**  
**Implementación PMG- Sistema de Seguridad de la Información**

- I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Estructura funcional del Sistema de Gestión de Seguridad de la Información y Ciberseguridad al interior de la Agencia de Calidad de la Educación
  2. Procedimiento de Contacto con Autoridades. Control A.6.1.3
  3. Procedimiento de Contacto con Grupos de Interés. Control A.6.1.4
  4. Política de Seguridad para Recursos Humanos. Control A.7.1.2
  5. Procedimiento de elaboración / Actualización de inventario de Activos. Control A.8.1.1 y su registro de operación.
  6. Procedimiento de Asignación y Devolución de Recursos. Control A.8.1.4
  7. Política de Control de Acceso físico y lógico. Control A.9.1.1 y A. 11.1.1
  8. Procedimiento de Inicio de Sesión Seguro. Control A.9.4.2
  9. Política de Ubicación y Protección del Equipamiento de la Agencia de Calidad de la Educación. Control A.11.2.1
  10. Procedimiento de Mantención de Equipos Críticos. Control A.11.02.04
  11. Procedimiento de eliminación o Reutilización de Equipamiento. Control A.11.2.7
  12. Procedimiento de Equipo de Usuario Desatendido. Control A.11.02.08
  13. Política de Escritorio y Pantalla limpios. Control A.11.2.9
  14. Procedimiento de Respaldo de Información. Control A.12.03.01

Fecha: 3 de julio de 2019

| N° | Nombre                   | Cargo                                    | Firma |
|----|--------------------------|--|-------|
| 1  | Juan Bravo               | Secretario Ejecutivo (S)                 |       |
| 2  | Gino Cortez              | Jefe de DEOD (S)                         |       |
| 3  | Cristóbal Alarcón        | Jefe de DIAC                             |       |
| 4  | Mariana Segura           | Jefa de DEIA(S) y DAG (S)                |       |
| 5  | María de la Luz González | Jefa de DIEST (S)                        |       |
| 6  | Andrea Soto Araya        | Encargada de SSI                         |       |
| 7  | Nicol Jeria              | Encargada de Ciberseguridad              |       |
| 8  | Sergio Hidalgo           | Jefe Departamento de Auditoría           |       |
| 9  | Gabriel Cáceres          | Encargado de Unidad de Planificación (s) |       |
| 10 | TATIANKA SOTO            | Jefe Unidad TIC                          |       |
| 11 | YERKO BRAGA              | Protección DIAC                          |       |
| 12 | CRISTÓBAL ALARCÓN        | Consultor Externo                        |       |

|  |   |                   |         |                          |
|--|---|-------------------|---------|--------------------------|
|  <p>Agencia de<br/>Calidad de la<br/>Educación</p> <p>Gobierno de Chile</p> | <b>Procedimiento de Respaldo de Información</b> |                   |         |                          |
|  | Nivel de Confidencialidad                       | -                 | Páginas | <b>1 de 10</b>           |
|  |   |                   | Versión | <b>1</b>                 |
|  | Fecha versión del documento                     | <b>31-05-2019</b> | Código  | <b>SGIC-PRO-A.12.3.1</b> |
| <b>Procedimiento de Respaldo de Información</b>  |   |                   |         |                          |

## Procedimiento de Respaldo de Información Control A.12.03.01

### Tabla de Contenidos

|            |   |          |
|------------|---|----------|
| <b>1</b>   | <b>Objetivo.....</b>  | <b>1</b> |
| <b>2</b>   | <b>Alcance.....</b>   | <b>2</b> |
| <b>3</b>   | <b>Normas y Referencias.....</b>  | <b>2</b> |
| <b>4</b>   | <b>Términos y Definiciones. ....</b>  | <b>2</b> |
| <b>5.</b>  | <b>Roles y Responsabilidades.....</b>                                       | <b>2</b> |
| <b>6.</b>  | <b>Directrices Generales para Respaldo de Información .....</b>             | <b>3</b> |
| <b>6.1</b> | <b>Directrices Generales para Respaldo de Servidores.....</b>               | <b>3</b> |
| <b>6.2</b> | <b>Directrices Generales para Respaldo de Estaciones de Trabajo .....</b>   | <b>3</b> |
| <b>7.</b>  | <b>Modo de Operación.....</b>   | <b>3</b> |
| <b>7.1</b> | <b>Flujo de Procedimiento para Respaldo de Servidores .....</b>             | <b>4</b> |
| <b>7.2</b> | <b>Matriz del Procedimiento para Respaldo de Servidores .....</b>           | <b>4</b> |
| <b>7.3</b> | <b>Flujo de Procedimiento para Respaldo de Estaciones de Trabajo.....</b>   | <b>6</b> |
| <b>7.4</b> | <b>Matriz del Procedimiento para Respaldo de Estaciones de Trabajo.....</b> | <b>7</b> |
| <b>7.5</b> | <b>Matriz de Responsabilidades. ....</b>                                    | <b>8</b> |
| <b>8.</b>  | <b>Registro de Operación. ....</b>  | <b>9</b> |

### REVISIONES DEL PROCEDIMIENTO

| Nº Versión | Fecha      | Motivo de la revisión | Páginas elaboradas o modificadas |
|------------|------------|-----------------------|----------------------------------|
| Uno (1)    | 31/05/2019 | Elaboración inicial   | Todas                            |

|   |                                 |   |                     |
|---|---------------------------------|---|---------------------|
| <b>ELABORADO POR</b>  | <b>VALIDACIÓN TÉCNICA</b>       | <b>APROBADO POR</b>   | <b>APROBADO POR</b> |
| Sistema de Gestión de Seguridad de Información y Ciberseguridad (SGSIC) | Patrick Soto<br>Jefe Unidad TIC | Andrea Soto Araya<br>Encargada de Seguridad de la Información | Comité de SGSIC     |

### 1. Objetivo.

En función de los objetivos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), declarado en la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, en adelante la Agencia, el presente documento tiene por objetivo establecer las actividades necesarias para respaldar la información contenida tanto en servidores como en estaciones de trabajo críticas de la Agencia, de modo de mantener el cumplimiento con los objetivos del SGSIC mencionados anteriormente.

## 2. Alcance.

Este procedimiento se debe aplicar a la totalidad de la información contenida en los servidores y estaciones de trabajo de la Agencia.

## 3. Normas y Referencias.

- Política General de Seguridad de la Información de la Agencia de Calidad de la Educación
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información.

## 4. Términos y Definiciones.

|  |   |
|--|---|
| <b>Copias de seguridad</b>               | Conjunto de archivos, carpetas y demás datos a los que se ha realizado copia de seguridad y se han almacenado en un archivo o en uno o varios medios (cintas, discos, DVD etc.).  |
| <b>Respaldo completo</b>                 | Es aquel que considera el respaldo de la totalidad de la información de interés para la Agencia. Incluye una copia de archivos de información de acuerdo a las extensiones de archivo que puedan contener información relevante para la Agencia, ofreciendo un respaldo por extensión de archivo sobre el perfil del usuario. |
| <b>Respaldo incremental</b>              | Copia los archivos creados o modificados desde la última copia de seguridad total (completa) o incremental.   |
| <b>Sistema de información</b>            | Aplicaciones, servicios, activos de tecnología de información, u otros componentes para el manejo de la información.  |
| <b>Usuario</b>                           | Persona que utiliza un activo de información, tales como: computador personal, notebook, Tablet, disco duro de la Agencia, ya sea que lo utilice en virtud de un empleo, sin importar la naturaleza jurídica de este o del estatuto que lo rija.  |
| <b>Periodo de retención del respaldo</b> | Es el tiempo indicado por el usuario o jefe directo que debe permanecer el respaldo activo.   |

## 5. Roles y Responsabilidades.

- Usuario:** Responsable de solicitar el respaldo de su equipo, así como de realizar los debidos respaldos en la nube mediante la utilización de las carpetas de Google.
- Encargada(o) de Seguridad de la Información:** Como líder del SGSIC, este rol será el encargado de velar por el cumplimiento de este procedimiento.
- Jefatura de Unidad de Tecnologías de Información y Comunicación:** Será responsable de garantizar la ejecución de este procedimiento, así como de entregar las directrices necesarias para su mejora continua en el tiempo.
- Analista de Soporte al Usuario:** Será éste el rol encargada de coordinar, preparar y ejecutar los respaldos de información asociados a las estaciones de trabajo de los colaboradores y colaboradoras de la Agencia.



- e) **Supervisor de Plataforma:** Será éste el rol responsable de coordinar, preparar, ejecutar y validar los respaldos, ya sean manuales o automáticos de los servidores de la Agencia.

## **6. Directrices Generales para Respaldo de Información**

A continuación, se entregan las directrices generales asociadas al respaldo de la información tanto en servidores como en estaciones de trabajo de la Agencia de Calidad de la Educación.

### **6.1 Directrices Generales para Respaldo de Servidores.**

De forma general, el respaldo de información almacenada en servidores de la Agencia, se debe realizar de forma diaria, y según las definiciones establecidas en el procedimiento asociado. Así mismo, la Agencia de Calidad de la Educación declara que toda información compartida para el trabajo diario, así como los archivos de producción personal que sean fruto del trabajo realizado para la Agencia, mediante sus divisiones, departamentos y unidades, debe residir en servidores de archivos (carpetas compartidas) especialmente habilitados por la Unidad de Tecnologías de Información y Comunicación a cada una de éstas, como contenedores de información productiva de la Agencia. Estos servidores de archivo serán respaldados según los lineamientos establecidos para el respaldo de servidores del servicio.

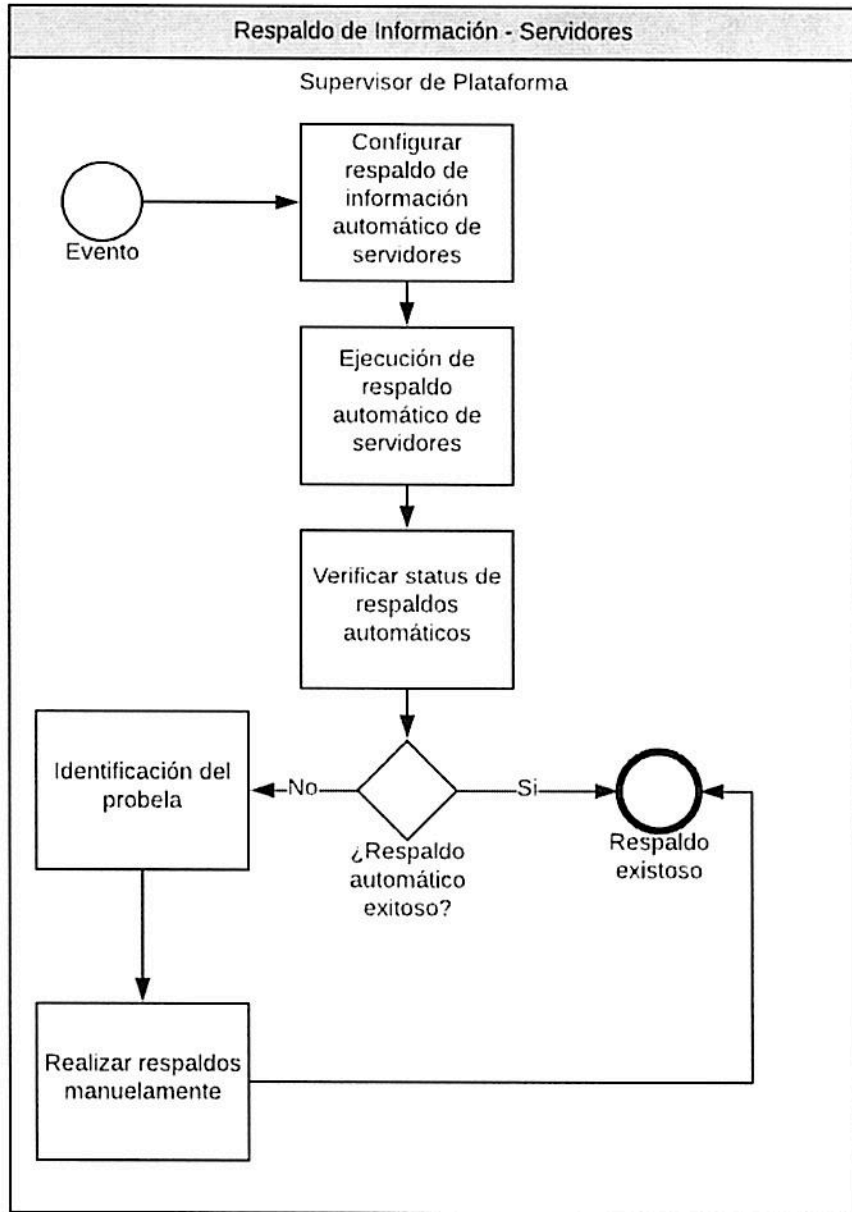
### **6.2 Directrices Generales para Respaldo de Estaciones de Trabajo.**

Dado lo especificado en el punto anterior, en donde se declara que la información compartida para el trabajo diario, así como la información producida bajo este mismo contexto debe ser almacenada en las carpetas compartidas disponibilizadas por la Unidad de TIC, es que el procedimiento de respaldo de información para estaciones de trabajo responde a la necesidad o solicitud específica de realizar un respaldo completo e íntegro de la información contenida en los computadores de los colaboradores y colaboradoras de la Agencia.

## **7. Modo de Operación.**

A continuación, se describen los flujos procedimentales para el respaldo de información contenida tanto en servidores como en estaciones de trabajo de la Agencia de Calidad de la Educación.

**7.1 Flujo de Procedimiento para Respaldo de Servidores.**



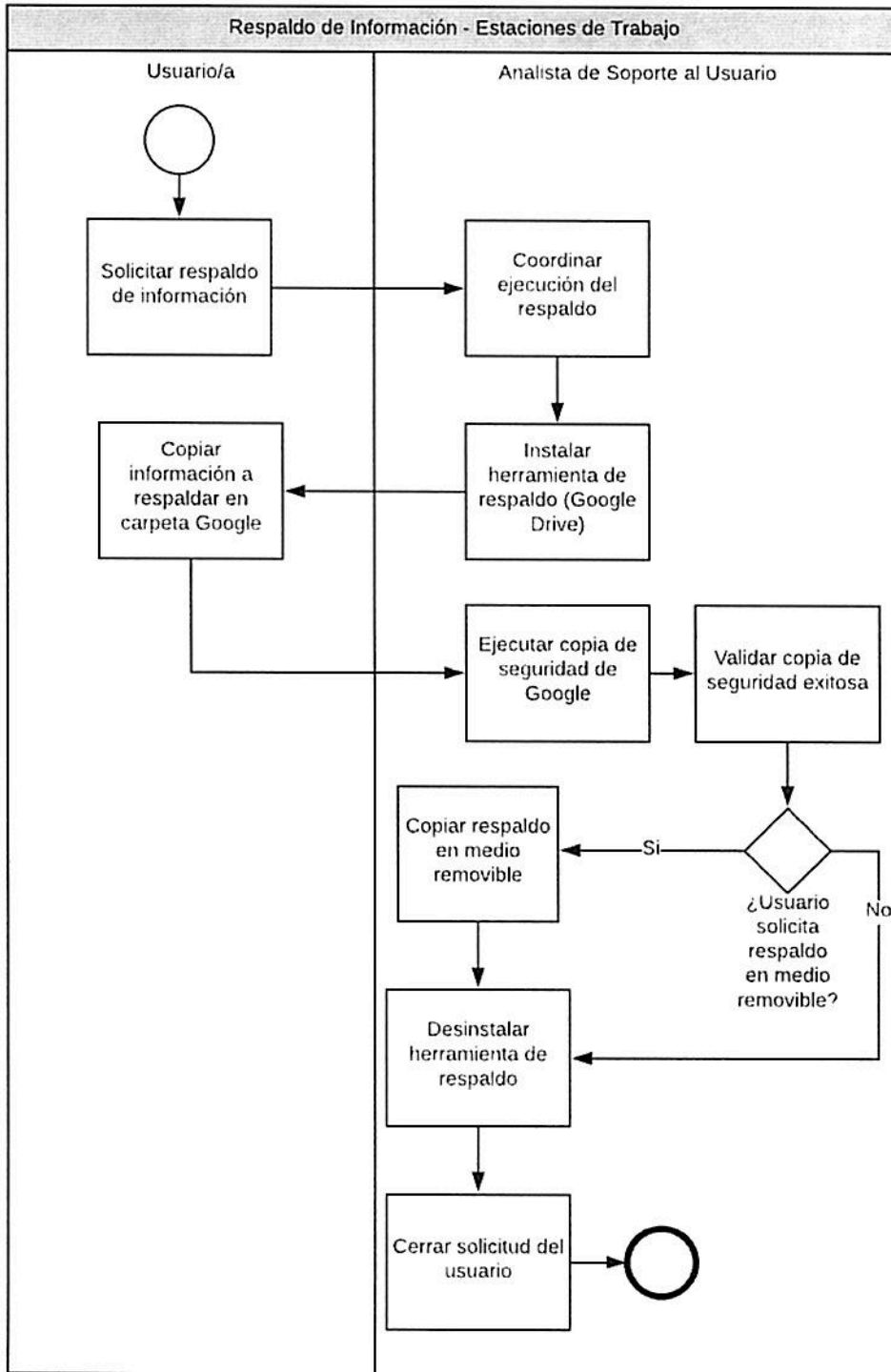
**7.2 Matriz del Procedimiento para Respaldo de Servidores.**

| ID | ACTIVIDAD | DESCRIPCIÓN | RESPONSABLE | ID ACTIVIDAD SIGUIENTE |
|----|-----------|-------------|-------------|------------------------|
|----|-----------|-------------|-------------|------------------------|

| ID | ACTIVIDAD   | DESCRIPCIÓN  | RESPONSABLE              | ID ACTIVIDAD SIGUIENTE |
|----|---|--|--------------------------|------------------------|
| 1  | Configurar respaldo de información automático de servidores | <p>Se debe establecer la configuración sobre el sistema de información respectivo que ejecute de forma automatizada los respaldos de información de los servidores de la Agencia bajo las siguientes condiciones:</p> <ul style="list-style-type: none"> <li>- Los respaldos se ejecutarán bajo una periodicidad diaria, al final de cada jornada.</li> <li>- Los respaldos se realizarán con una base incremental diaria de 15 días hábiles, o tres (3) semanas laborales de cinco (5) días corridos en horario de 5x8.</li> <li>- Se debe configurar el envío de un correo al Encargado de Plataforma, con copia a la Jefatura de Unidad de TIC, con el status de los respaldos una vez finalizada la ejecución de éstos, ya sea automática o manual.</li> </ul> | Supervisor de Plataforma | 2                      |
| 2  | Ejecución de respaldo automático de servidores              | El respaldo de los servidores debe realizarse automáticamente según lo establecido en la actividad uno (1) de este procedimiento.  | Supervisor de Plataforma | 3                      |
| 3  | Verificar status de respaldos automáticos                   | <p>Se debe revisar el reporte de status de respaldos entregado de forma automático según lo establecido en la actividad uno (1) de este procedimiento, para validar la correcta ejecución de éstos. Se pueden dar las siguientes alternativas:</p> <ul style="list-style-type: none"> <li>- Los respaldos no se realizaron de forma exitosa (4).</li> <li>- Los respaldos se ejecutaron de forma exitosa (FIN).</li> </ul>   | Supervisor de Plataforma | 4 o FIN                |
| 4  | Identificación del problema                                 | Se debe identificar el por qué no se realizaron con éxito los respaldos y solucionar el impedimento.   | Supervisor de Plataforma | 4A                     |

| ID | ACTIVIDAD                   | DESCRIPCIÓN  | RESPONSABLE              | ID ACTIVIDAD SIGUIENTE |
|----|-----------------------------|--|--------------------------|------------------------|
| 4A | Realizar respaldos manuales | Se debe realizar de forma manual el respaldo de el o los servidores sobre los cuales falló la ejecución del respaldo automático. | Supervisor de Plataforma | 3                      |

### 7.3 Flujo de Procedimiento para Respaldo de Estaciones de Trabajo.



**7.4 Matriz del Procedimiento para Respaldo de Estaciones de Trabajo.**

| ID | ACTIVIDAD                                       | DESCRIPCIÓN  | RESPONSABLE                    | ID ACTIVIDAD SIGUIENTE |
|----|---|--|--------------------------------|------------------------|
| 1  | Solicitar respaldo de información               | <p>Toda petición de respaldo de la información contenida en un computador personal o activo de información de un usuario, debe ser solicitada al <i>área de Soporte</i> mediante el sistema de tickets de la organización. En éste se deben especificar la información que necesita respaldar, así como las características y condiciones que se deben considerar en el momento de efectuar el respaldo.</p> <p><b>NOTA:</b> En caso de requerir una copia del respaldo en medio removible, la solicitud debe ir acompañada del visto bueno de la jefatura correspondiente mediante solicitud firmada o correo electrónico, y autorizada por la Encargada de Seguridad de la Información. En caso de información de carácter reservada, debe incluirse la autorización de la Jefatura de División.</p> | Usuario/a                      | 2                      |
| 2  | Coordinar ejecución del respaldo                | Se debe coordinar con el usuario solicitante, la realización del respaldo.   | Analista de Soporte al Usuario | 3                      |
| 3  | Instalar herramienta de respaldo (Google Drive) | <p>Se debe instalar en la estación de trabajo del usuario, la herramienta de sincronización y respaldos de Google.</p> <p><b>NOTA:</b> Al momento de la instalación se solicitará acceso a la cuenta google en donde se desea almacenar el respaldo. Ésta será la cuenta de Soporte al Usuaio.</p>   | Analista de Soporte al Usuario | 4                      |

| ID | ACTIVIDAD  | DESCRIPCIÓN   | RESPONSABLE                    | ID ACTIVIDAD SIGUIENTE |
|----|--|---|--------------------------------|------------------------|
| 4  | Copiar información a respaldar en carpeta Google | Se debe copiar toda la información a respaldar en la carpeta de Google.   | Usuario                        | 5                      |
| 5  | Ejecutar la copia de seguridad de Google         | Se debe ejecutar la acción de copia de seguridad de la herramienta de Copia de Seguridad y Respaldo de Goolge.  | Analista de Soporte al Usuario | 6                      |
| 6  | Validar copia de seguridad exitosa               | Se debe validar que la copia de seguridad se encuentre en la ubicación Google Drive de de la cuenta de Soporte al Usuario. Se pueden dar las siguientes opciones.<br>- El usuario solicitó copia del respaldo en medio removible (7).<br>- El usuario no solicitó copia de del respaldo en medio removible (8). | Analista de Soporte al Usuario | 7 O 8                  |
| 7  | Copiar respaldo en medio removible               | Previa validación de la existencia de las autorizaciones pertinentes, especificadas en la actividad uno (1) de este procedimiento, se procede a copiar el respaldo en un medio removible oficial de la institución.   | Analista de Soporte al Usuario | 8                      |
| 8  | Desinstalar herramienta de respaldo              | Una vez realizado el respaldo de forma exitosa, se debe desinstalar la herramienta de Copia de Seguridad y Sincronización de Google.  | Analista de Soporte al Usuario | 9                      |
| 9  | Cerrar solicitud del usuario                     | Se debe dar por cerrada la solicitud del usuario, con lo cual éste se dará por enterado de la ejecución exitosa de su solicitud.  | Analista de Soporte al Usuario | FIN                    |

### **7.5 Matriz de Responsabilidades.**

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

De esta forma, la matriz de responsabilidades para respaldo de información en servidores, se estructura de la siguiente manera:

| ID | ACTIVIDAD   | ENC. SI | JEF E TIC | ENC. PLATAFORMA |
|----|---|---------|-----------|-----------------|
| 1  | Configurar respaldo de información automático de servidores | I       | A         | R/E             |
| 2  | Ejecución de respaldo automático de servidores              | I       | I         | R               |
| 3  | Verificar status de respaldos automáticos                   | I       | A/C       | R/E             |
| 4  | Identificación del problema                                 | I       | I         | R               |
| 4A | Realizar respaldos manuales                                 | I       | I         | R               |

Así mismo, la matriz de responsabilidades para respaldos de estaciones de trabajo, se estructura de la siguiente manera:

| ID | ACTIVIDAD  | ENC. SI | JEFE/A | ENC. SOPORTE | USUARIO |
|----|--|---------|--------|--------------|---------|
| 1  | Solicitar respaldo de información                | I       | I      | I            | R/E     |
| 2  | Coordinar ejecución del respaldo                 | -       | -      | R/E          | R       |
| 3  | Instalar herramienta de respaldo (Google Drive)  | -       | -      | R/E          | R       |
| 4  | Copiar información a respaldar en carpeta Google | -       | -      | C            | R/E     |
| 5  | Ejecutar la copia de seguridad de Google         | -       | -      | R/E          | I       |
| 6  | Validar copia de seguridad exitosa               | -       | -      | R/E          | I       |
| 7  | Copiar respaldo en medio removible               | I       | I      | R/E          | -       |
| 8  | Desinstalar herramienta de respaldo              | -       | -      | R/E          | I       |
| 9  | Cerrar solicitud del usuario                     | I       | I      | R/E          | I       |

#### 8. Registro de Operación.

| REGISTRO  | ID | RESPONSABLE/DUEÑO DEL REGISTRO | TIEMPO RETENCIÓN      | SOPORTE | LUGAR                      |
|---|----|--------------------------------|-----------------------|---------|----------------------------|
| Reporte de ejecución exitosa de respaldos de servidores                     | -  | Encargado Plataforma de        | 4 años / Archivo UTIC | Digital | PC Encargado de Plataforma |
| Reporte de tickets cerrados asociados a respaldos de estaciones de trabajo. | -  | Encargado Soporte de           | 4 años / Archivo UTIC | Digital | PC Encargado de Soporte    |

Aprobado por:

**Firma:**

**Fecha de Actualización:**






**LISTA DE ASISTENCIA**  
**Comité de Seguridad de la Información**  
**Implementación PMG- Sistema de Seguridad de la Información**

- I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Estructura funcional del Sistema de Gestión de Seguridad de la Información y Ciberseguridad al interior de la Agencia de Calidad de la Educación
  2. Procedimiento de Contacto con Autoridades. Control A.6.1.3
  3. Procedimiento de Contacto con Grupos de Interés. Control A.6.1.4
  4. Política de Seguridad para Recursos Humanos. Control A.7.1.2
  5. Procedimiento de elaboración / Actualización de inventario de Activos. Control A.8.1.1 y su registro de operación.
  6. Procedimiento de Asignación y Devolución de Recursos. Control A.8.1.4
  7. Política de Control de Acceso físico y lógico. Control A.9.1.1 y A. 11.1.1
  8. Procedimiento de Inicio de Sesión Seguro. Control A.9.4.2
  9. Política de Ubicación y Protección del Equipamiento de la Agencia de Calidad de la Educación. Control A.11.2.1
  10. Procedimiento de Mantenimiento de Equipos Críticos. Control A.11.02.04
  11. Procedimiento de eliminación o Reutilización de Equipamiento. Control A.11.2.7
  12. Procedimiento de Equipo de Usuario Desatendido. Control A.11.02.08
  13. Política de Escritorio y Pantalla limpios. Control A.11.2.9
  14. Procedimiento de Respaldo de Información. Control A.12.03.01

Fecha: 3 de julio de 2019

| N° | Nombre                   | Cargo                                    | Firma |
|----|--------------------------|--|-------|
| 1  | Juan Bravo               | Secretario Ejecutivo (S)                 |       |
| 2  | Gino Cortez              | Jefe de DEOD (S)                         |       |
| 3  | Cristóbal Alarcón        | Jefe de DIAC                             |       |
| 4  | Mariana Segura           | Jefa de DEIA(S) y DAG (S)                |       |
| 5  | María de la Luz González | Jefa de DIEST (S)                        |       |
| 6  | Andrea Soto Araya        | Encargada de SSI                         |       |
| 7  | Nicol Jeria              | Encargada de Ciberseguridad              |       |
| 8  | Sergio Hidalgo           | Jefe Departamento de Auditoría           |       |
| 9  | Gabriel Cáceres          | Encargado de Unidad de Planificación (s) |       |
| 10 | YATINCK SOTO S.          | Jefe Unidad TIC                          |       |
| 11 | Yerko Barra              | Protección DIAC                          |       |
| 12 | Claudio Corado           | Consultor Externo                        |       |

|   |   |                   |         |                         |
|---|---|-------------------|---------|-------------------------|
| <br><b>Agencia de<br/>Calidad de la<br/>Educación</b><br><br>Gobierno de Chile | <b>Procedimiento de Inicio de Sesión Seguro</b> |                   |         |                         |
|   | Nivel de Confidencialidad                       | -                 | Páginas | <b>1 de 5</b>           |
|   |   |                   | Versión | <b>0</b>                |
|   | Fecha versión del documento                     | <b>31-05-2019</b> | Código  | <b>SGIC-PRO-A.9.4.2</b> |
| <b>Procedimiento de Inicio de Sesión Seguro</b>   |   |                   |         |                         |

## Procedimiento de Inicio de Sesión Seguro Control A.09.04.02

Tabla de Contenidos

|            |  |          |
|------------|--|----------|
| <b>1</b>   | <b>Objetivo.....</b>   | <b>2</b> |
| <b>2</b>   | <b>Alcance.....</b>  | <b>2</b> |
| <b>3</b>   | <b>Normas y Referencias.....</b>                                   | <b>2</b> |
| <b>4</b>   | <b>Términos y Definiciones. ....</b>                               | <b>2</b> |
| <b>5.</b>  | <b>Roles y Responsabilidades.....</b>                              | <b>3</b> |
| <b>6.</b>  | <b>Directrices Generales para el inicio de sesión seguro .....</b> | <b>3</b> |
| <b>7.</b>  | <b>Modo de Operación .....</b>                                     | <b>3</b> |
| <b>7.1</b> | <b>Flujo de Procedimiento para Inicio de Sesión Seguro .....</b>   | <b>4</b> |
| <b>7.2</b> | <b>Matriz del Procedimiento para Inicio de Sesión Seguro .....</b> | <b>4</b> |
| <b>7.3</b> | <b>Matriz de Responsabilidades. ....</b>                           | <b>5</b> |
| <b>8.</b>  | <b>Registro de Operación. ....</b>                                 | <b>5</b> |

| REVISIONES DEL PROCEDIMIENTO |            |                       |                                  |
|------------------------------|------------|-----------------------|----------------------------------|
| Nº<br>Versión                | Fecha      | Motivo de la revisión | Páginas elaboradas o modificadas |
| Cero (0)                     | 31/05/2019 | Elaboración inicial   | Todas                            |

|  |                                |   |                     |
|--|--------------------------------|---|---------------------|
| <b>ELABORADO POR</b>   | <b>VALIDACIÓN TÉCNICA</b>      | <b>APROBADO POR</b>   | <b>APROBADO POR</b> |
| Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC) | Patrik Soto<br>Jefe Unidad TIC | Andrea Soto Araya<br>Encargada de Seguridad de la Información | Comité de SGSIC     |



## 1. Objetivo.

En función de los objetivos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), declarado en la Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, en adelante la Agencia, el presente documento tiene por objetivo establecer y definir las actividades necesarias que permitan aplicar las reglas de acceso a las estaciones de trabajo de propiedad del servicio.

## 2. Alcance.

Este procedimiento deberá ser aplicado por todos(as) los(as) funcionarios(as) de planta y contrata, personal a honorarios y toda aquella persona natural o jurídica que preste servicios (terceros y proveedores) y que, a raíz de ello, tengan acceso a estaciones de trabajo de la Agencia y por consiguiente, tenga acceso a información del servicio.

## 3. Normas y Referencias.

- Política General de Seguridad de la Información de la Agencia de Calidad de la Educación
- Política de Gestión de usuarios y Contraseñas
- Procedimiento de Entrega de Acceso a los Usuarios
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información

## 4. Términos y Definiciones.

|                                       |   |
|---------------------------------------|---|
| <b>Contraseña:</b>                    | Autenticación del usuario que utiliza información   |
| <b>Active Directory (AD)</b>          | Es el sistema de Directorio que posee la Agencia y que gestiona la Unidad TIC para identificar a todos los usuarios con el objetivo de administrar los inicios de sesión de los equipos en red.   |
| <b>Sistemas Informáticos</b>          | Sistemas que permiten almacenar y procesar información.   |
| <b>Acceso a la información</b>        | Derecho que tiene un usuario para buscar, recibir y difundir información del Servicio.  |
| <b>Restringir el acceso</b>           | Delimitar el acceso de los funcionarios (as), servidores públicos a honorarios y terceras partes a determinados recursos.   |
| <b>Estación de Trabajo</b>            | Es un computador que facilita a los usuarios (as) el acceso a los servidores y periféricos de la red.   |
| <b>Autenticación</b>                  | Proceso de confirmación de la identidad del (de la) usuario (a) que utiliza un sistema informático.   |
| <b>Identificador de autenticación</b> | Mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos.  |
| <b>Autenticar (o autenticar)</b>      | Se refiere a comprobar que esa persona es quien dice ser. Ello se logra cuando se cotejan uno o más datos en dicha identificación oficial contra (i) los datos en alguna otra identificación, documento, certificado digital (como el de la firma electrónica) o dispositivo que tenga la persona, (ii) los datos que sepa o tenga memorizados (su firma autógrafa o su contraseña, por ejemplo) o (iii) una o más características que coincidan con lo que es dicha persona (fotografía o huella dactilar, por ejemplo). |
| <b>Autorizar</b>                      | Se refiere al acceso que se le permite a la persona que se ha identificado y autenticado apropiadamente.  |
| <b>Identificador Único Global</b>     | Abreviado bajo la sigla Guid es una implementación del sistema Active Directory que permite que cada usuario sea único e irrepetible.   |

## **5. Roles y Responsabilidades**

- a) **Encargada(o) de Seguridad de la Información:** Como líder del SGSIC, este rol será el encargado de velar por el cumplimiento de este procedimiento.
- b) **Usuario:** Responsable de recordar e ingresar sus credenciales de inicio de sesión con éxito.
- c) **Jefatura de Unidad de Tecnologías de Información y Comunicación:** Será responsable de garantizar la ejecución de este procedimiento, así como de determinar el método técnico de protección adecuado para el acceso a la información. Además, será el encargado de entregar las directrices necesarias para su mejora continua en el tiempo.
- d) **Encargado de Plataforma y Operaciones TI:** Será éste el rol responsable de implementar, administrar y mantener las medidas de seguridad técnicas para proveer control de acceso a las estaciones de trabajo de la Agencia.

## **6. Directrices Generales para el inicio de sesión seguro.**

Se debe tener en cuenta, que si bien, de forma previa a la ejecución de este procedimiento, el perfilamiento de privilegios de acceso a la información se efectúa basado en roles según lo indicado en la Política de Gestión de Usuarios y Contraseñas, se pueden solicitar accesos específicos según las necesidades de la División, Departamento o Unidad a la que pertenezca el usuario o usuaria que requiere el acceso, según lo detallado en el Procedimiento de Entrega de Acceso a los Usuarios.

Para la autenticación e identificación de todos los usuarios de la agencia, se definió la utilización de un sistema de Directorio, específicamente MS Active Directory, en adelante AD, el cual permite localizar el acceso a la red del servicio, con el fin de facilitar su localización y administración.

Así mismo, con respecto al acceso a los sistemas, el personal para ingresar a un computador o a la red de Trabajo de la Agencia, deberá autenticarse e ingresar su usuario y contraseña de AD, con ello es reconocido (al ser identificador único) por los Sistemas Informáticos de la Agencia. Este acceso es la única puerta de entrada a todos los sistemas e información de la institución.

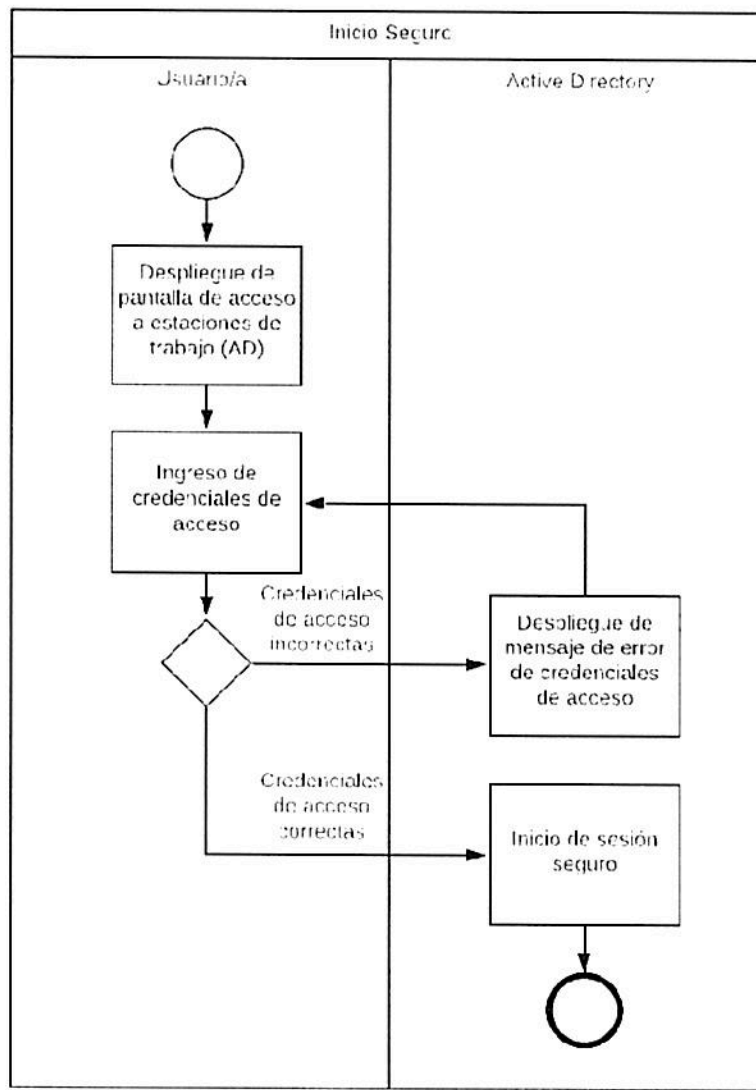
El sistema AD cumple una serie de requisitos que permiten respaldar la generación de identificadores de usuarios, considerando que todas las acciones parten de la base del identificador único global, siendo éste irreplicable. Este identificador se genera cuando un usuario es creado por la Unidad de Tecnologías de la Información en el AD. De esta forma, si el equipo de un usuario se encuentra en red, la Unidad TIC mediante controladores de dominio asignará una IP para identificar sus actividades.

El sistema AD permite que un usuario pueda ingresar al sistema independiente del punto físico donde se encuentre, accediendo ya sea desde Nivel Central o Macrozonas, como también permite ingresar por diversos equipos computacionales a los sistemas de la Agencia.

## **7. Modo de Operación.**

A continuación, se describen los flujos procedimentales para el inicio de sesión seguro en estaciones de trabajo de la Agencia de Calidad de la Educación.

## 7.1 Flujo de Procedimiento para Inicio de Sesión Seguro.



## 7.2 Matriz del Procedimiento para Inicio de Sesión Seguro.

| ID | ACTIVIDAD   | DESCRIPCIÓN  | RESPONSABLE | ID ACTIVIDAD SIGUIENTE |
|----|---|--|-------------|------------------------|
| 1  | Despliegue de pantalla de acceso a estaciones de trabajo (AD) | Al momento de encender una estación de trabajo el sistema AD mostrará una pantalla con las indicaciones para desplegar la solicitud de credenciales de acceso para inicio de sesión seguro, como se muestra en el Anexo I.<br><br><b>NOTA:</b> Se debe presionar simultáneamente las teclas Ctrl+Alt+Suprimir. | Usuario/a   | 2                      |

| ID | ACTIVIDAD  | DESCRIPCIÓN  | RESPONSABLE      | ID ACTIVIDAD SIGUIENTE |
|----|--|--|------------------|------------------------|
| 2  | Ingreso de credenciales de acceso                        | El usuario ingresa sus credenciales de acceso en la pantalla desplegada, como se muestra en el Anexo I. Se pueden dar las siguientes alternativas:<br>- Credenciales de acceso incorrectas (3)<br>- Credenciales de acceso correctas (4) | Usuario/a        | 3 o 4                  |
| 3  | Despliegue de mensaje de error de credenciales de acceso | El sistema AD despliega un mensaje indicando que las credenciales de acceso son incorrectas.   | Active Directory | 2                      |
| 4  | Inicio de sesión seguro                                  | El sistema AD concede acceso a los sistemas de la institución  | Active Directory | FIN                    |

### 7.3 Matriz de Responsabilidades.

No Aplica.

### 8. Registro de Operación.

| REGISTRO  | ID | RESPONSABLE/DUEÑO DEL REGISTRO | TIEMPO RETENCIÓN      | SOPORTE | LUGAR                                   |
|---|----|--------------------------------|-----------------------|---------|---|
| Evidencia de la configuración adecuada del sistema Active Directory para inicio de sesión seguro. | -  | Encargado de Plataforma        | 4 años / Archivo UTIC | Digital | Panel de configuración Active Directory |

**Aprobado por:**

**Firma:**

**Fecha de Actualización:**



**LISTA DE ASISTENCIA**  
**Comité de Seguridad de la Información**  
**Implementación PMG- Sistema de Seguridad de la Información**

- I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Estructura funcional del Sistema de Gestión de Seguridad de la Información y Ciberseguridad al interior de la Agencia de Calidad de la Educación
  2. Procedimiento de Contacto con Autoridades. Control A.6.1.3
  3. Procedimiento de Contacto con Grupos de Interés. Control A.6.1.4
  4. Política de Seguridad para Recursos Humanos. Control A.7.1.2
  5. Procedimiento de elaboración / Actualización de inventario de Activos. Control A.8.1.1 y su registro de operación.
  6. Procedimiento de Asignación y Devolución de Recursos. Control A.8.1.4
  7. Política de Control de Acceso físico y lógico. Control A.9.1.1 y A. 11.1.1
  8. Procedimiento de Inicio de Sesión Seguro. Control A.9.4.2
  9. Política de Ubicación y Protección del Equipamiento de la Agencia de Calidad de la Educación. Control A.11.2.1
  10. Procedimiento de Mantenimiento de Equipos Críticos. Control A.11.02.04
  11. Procedimiento de eliminación o Reutilización de Equipamiento. Control A.11.2.7
  12. Procedimiento de Equipo de Usuario Desatendido. Control A.11.02.08
  13. Política de Escritorio y Pantalla limpios. Control A.11.2.9
  14. Procedimiento de Respaldo de Información. Control A.12.03.01

Fecha: 3 de julio de 2019

| N° | Nombre                   | Cargo                                    | Firma |
|----|--------------------------|--|-------|
| 1  | Juan Bravo               | Secretario Ejecutivo (S)                 |       |
| 2  | Gino Cortez              | Jefe de DEOD (S)                         |       |
| 3  | Cristóbal Alarcón        | Jefe de DIAC                             |       |
| 4  | Mariana Segura           | Jefa de DEIA(S) y DAG (S)                |       |
| 5  | María de la Luz González | Jefa de DIEST (S)                        |       |
| 6  | Andrea Soto Araya        | Encargada de SSI                         |       |
| 7  | Nicol Jeria              | Encargada de Ciberseguridad              |       |
| 8  | Sergio Hidalgo           | Jefe Departamento de Auditoría           |       |
| 9  | Gabriel Cáceres          | Encargado de Unidad de Planificación (s) |       |
| 10 | <i>YATINCK SOTO</i>      | <i>Jefe Unidad TIC</i>                   |       |
| 11 | <i>Yerko Brera</i>       | <i>Protección DIAC</i>                   |       |
| 12 | <i>Claudio Conado</i>    | <i>Consultas Externas</i>                |       |

|  |   |          |         |                          |
|--|---|----------|---------|--------------------------|
|  <p>Agencia de<br/>Calidad de la<br/>Educación</p> <p>Gobierno de Chile</p> | <b>Procedimiento de Asignación y Devolución de Recursos</b> |          |         |                          |
|  | Nivel de Confidencialidad                                   | -        | Páginas | 7                        |
|  |   |          | Versión | 1                        |
|  | Fecha versión del documento                                 | 28-06-19 | Código  | <b>SGSIC-PRO-A.8.1.4</b> |
| <b>Procedimiento de Asignación y Devolución de Recursos</b>  |   |          |         |                          |

## Procedimiento de Asignación y Devolución de Recursos

### Control A.08.01.04

#### Tabla de Contenidos

|            |  |          |
|------------|--|----------|
| <b>1</b>   | <b>Objetivo.....</b>   | <b>1</b> |
| <b>2</b>   | <b>Alcance.....</b>  | <b>2</b> |
| <b>3</b>   | <b>Normas y Referencias.....</b>   | <b>2</b> |
| <b>4</b>   | <b>Términos y Definiciones. ....</b>   | <b>2</b> |
| <b>5.</b>  | <b>Roles y Responsabilidades.....</b>  | <b>3</b> |
| <b>6.</b>  | <b>Directrices Generales para la Entrega y Devolución de Recursos.....</b>                   | <b>3</b> |
| <b>7.</b>  | <b>Modo de Operación.....</b>  | <b>4</b> |
| <b>7.1</b> | <b>Flujo de Procedimiento.....</b>   | <b>4</b> |
| <b>7.2</b> | <b>Matriz del Proceso de Entrega de Activos en caso de Ingreso de Nuevo Personal.....</b>    | <b>4</b> |
| <b>7.3</b> | <b>Flujo de Procedimiento.....</b>   | <b>5</b> |
| <b>7.4</b> | <b>Matriz del Proceso de Recepción de Activos en caso de Desvinculación de Personal.....</b> | <b>6</b> |
| <b>7.5</b> | <b>Flujo de Procedimiento.....</b>   | <b>6</b> |
| <b>7.6</b> | <b>Matriz del Proceso de Entrega de Activos en caso de Solicitud.....</b>                    | <b>7</b> |
| <b>7.7</b> | <b>Matriz de Responsabilidades. ....</b>   | <b>7</b> |
| <b>8.</b>  | <b>Registro de Operación. ....</b>   | <b>8</b> |

#### REVISIONES DEL PROCEDIMIENTO

| Nº Versión | Fecha    | Motivo de la revisión | Páginas elaboradas o modificadas |
|------------|----------|-----------------------|----------------------------------|
| Uno (1)    | 28-06-19 | Elaboración inicial   | Todas                            |

|   |                           |   |                     |
|---|---------------------------|---|---------------------|
| <b>ELABORADO POR</b>  | <b>VALIDACIÓN TÉCNICA</b> | <b>APROBADO POR</b>   | <b>APROBADO POR</b> |
| Sistema de Gestión de Seguridad de Información y Ciberseguridad | Patrick Soto<br>Jefe TIC  | Andrea Soto Araya<br>Encargada de Seguridad de la Información | Comité de SGSIC     |

#### 1. Objetivo.

El presente procedimiento tiene por objetivo establecer y definir las actividades a realizar para solicitar y controlar tanto la entrega como la devolución de los recursos tecnológicos pertenecientes a la Agencia de Calidad de la Educación, en adelante la Agencia. El procedimiento en cuestión está particularmente diseñado para dejar constancia de la entrega o recepción de los recursos cuando se produce un ingreso, una desvinculación o algún otro cambio en las funciones del personal de la Agencia.



## 2. Alcance.

Este procedimiento deberá ser aplicado sobre todos los recursos tecnológicos de propiedad de la Agencia que deban ser asignados a funcionarios(as) tanto internos de planta, contrata u honorarios, como externos, terceros y proveedores, que de forma directa o indirecta requieran de estos recursos para el cumplimiento de sus responsabilidades.

## 3. Normas y Referencias.

- Ley N° 20.529, Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su Fiscalización.
- DFL N° 29, del año 2004 que fija el Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo.
- Ley N° 19.880, Establece Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la administración del Estado.
- Ley N° 20.285, sobre acceso a la Información Pública.
- Decreto Supremo N° 83, Norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información - Requisitos.
- Norma NCh-ISO 27002:2013, Código de Prácticas para la Gestión de la Seguridad de la Información.
- Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, vigente.

## 4. Términos y Definiciones.

|   |   |
|---|---|
| <b>Activo de Información</b>                  | La Información es un activo fundamental para el desarrollo, operativa, control y gestión de la Institución, se considera como la información propiamente tal, así como todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.   |
| <b>Acceso a la información</b>                | El acceso a la información es el derecho que tiene toda persona de buscar, recibir y difundir información en poder del Servicio, y que justifique el quehacer para el cual fue contratado.  |
| <b>Derechos de accesos</b>                    | Conjunto de permisos dados a un usuario, de acuerdo con sus funciones, para acceder a un determinado recurso.   |
| <b>Restringir el acceso</b>                   | Delimitar el acceso de los usuarios, servidores públicos a honorarios y terceras partes a determinados recursos.  |
| <b>Sistema de información</b>                 | Aplicaciones, servicios, activos de tecnología de información, u otros componentes para el manejo de la información.  |
| <b>Medios de procesamiento de información</b> | Los dispositivos internos y/o externos que tenga la capacidad de procesar información, almacenarla y que se encuentren disponibles para ser manipulados por el usuario. Como ejemplos de medios de procesamiento de información, podemos enumerar: <ul style="list-style-type: none"><li>• Servidores de aplicaciones: de correo, de impresión, aplicaciones web.</li><li>• Servidores de Almacenamientos.</li><li>• Computadores personales.</li><li>• Discos duros externos</li><li>• Pendrives.</li><li>• Teléfonos móviles.</li></ul> |

|                   |  |
|-------------------|--|
| <b>Usuario(a)</b> | Persona que utiliza un activo de información, tales como: computador personal, notebook, tablet, disco duro, teléfonos de la Agencia en virtud de su empleo, sin importar la naturaleza jurídica de este o del estatuto que lo rija. |
|-------------------|--|

## **5. Roles y Responsabilidades.**

- a) **Analista Departamento de Gestión y Desarrollo de las Personas:** Como miembro del Departamento de Gestión y Desarrollo de Personas, colabora de forma directa con los procesos de vinculación y desvinculación de la organización. En función de lo anterior, es también responsable de dar inicio al proceso de entrega/devolución de recursos de la Agencia, mediante el llenado tanto del formulario de vinculación, indicando los recursos que deberán ser asignados al trabajador que se incorpora a la organización, como del de desvinculación.
- b) **Encargado(a) de Seguridad de la Información:** Como rol líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), tiene la responsabilidad de monitorear el cumplimiento de este procedimiento, así como de atender cualquier complicación asociada a la entrega o recepción de recursos que son propiedad de la organización.
- c) **Analista de Soporte al Usuario:** Como rol a cargo del inventario de los recursos tecnológicos pertenecientes a la organización, es responsabilidad de éste verificar la disponibilidad de los recursos solicitados, así como de hacer entrega de estos. Adicionalmente, debe de hacer recepción de los recursos que son devueltos por los trabajadores que han sido desvinculados de la organización. Dado lo anterior, este rol deberá también garantizar la constante mantención actualizada del inventario de recursos tecnológicos.
- d) **Jefatura Directa:** Como superior inmediato del usuario que recibe uno a varios recursos tecnológicos, es la labor de éste determinar correctamente los recursos que deberán ser facilitados al usuario en cuestión, con el objetivo de que este pueda realizar sus funciones correctamente. Adicionalmente, deberá aprobar o rechazar las solicitudes de recursos adicionales elevadas por los usuarios que se encuentren bajo su ámbito de gestión.
- e) **Usuario:** Hace referencia a todo colaborador, tanto interno como externo, a quien se le han asignado recursos para la realización de sus tareas.

## **6. Directrices Generales para la Entrega y Devolución de Recursos.**

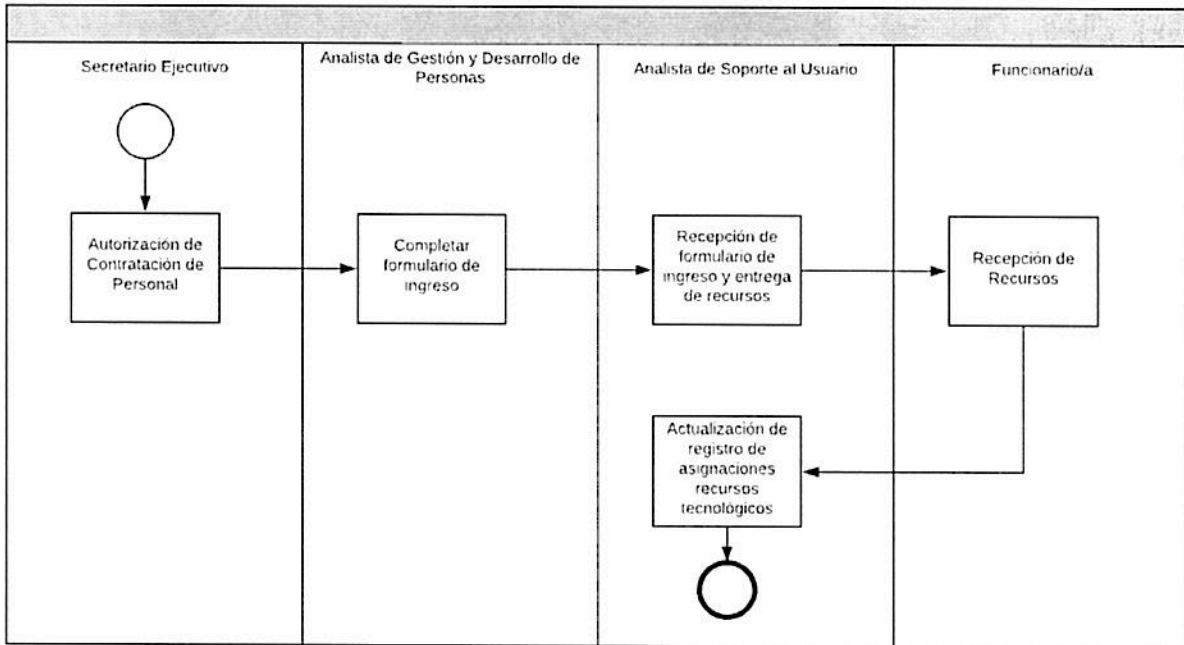
Teniendo en cuenta que todos los colaboradores y colaboradoras de la organización necesitan de recursos tecnológicos para la realización de sus tareas, es necesaria la existencia de instancias formales para hacer entrega/recepción de éstos, así como de mecanismos definidos para dejar constancia de estos movimientos. En este contexto, a continuación, se detallan los principales insumos utilizados por la organización con el objetivo de la realización ordenada del procedimiento en cuestión:

| <b>TIPO DE EVENTO</b>             | <b>INSUMO</b>                                       |
|-----------------------------------|---|
| <b>Vinculación de Personal</b>    | <b>Anexo I: Formulario de Solicitud de Recursos</b> |
| <b>Desvinculación de Personal</b> | <b>Anexo II: Formulario de Entrega de Recursos</b>  |

## 7. Modo de Operación.

De acuerdo con los eventos descritos anteriormente, se establece un flujo comunicacional específico, en donde, de acuerdo con el tipo de evento, se definen las tareas pertinentes, así como los roles responsables de la realización de estas.

### 7.1 Flujo de Procedimiento para Asignación de Recursos por Ingreso de Personal.

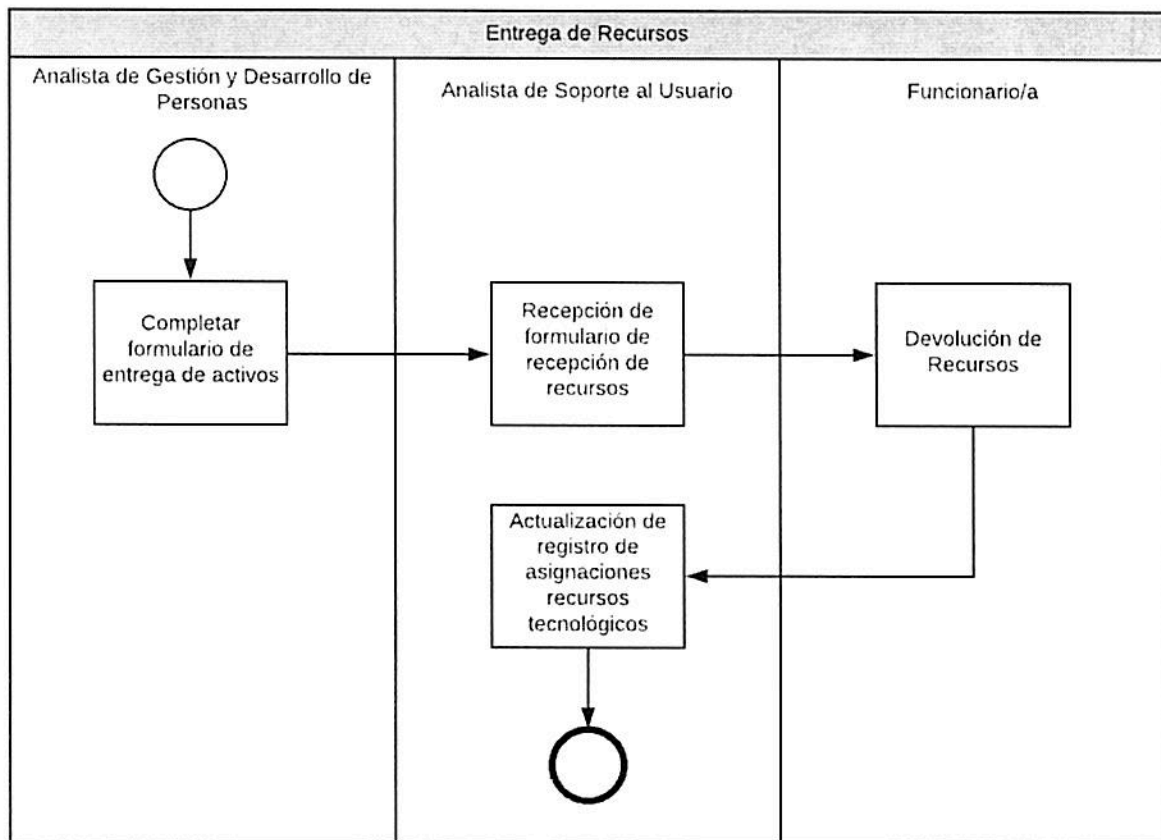


### 7.2 Matriz del Proceso de Entrega de Recursos en caso de Ingreso de Nuevo Personal.

| ID | ACTIVIDAD                                 | DESCRIPCIÓN  | RESPONSABLE                               | ID ACTIVIDAD SIGUIENTE |
|----|---|--|---|------------------------|
| 1  | Autorización de contratación del personal | Una vez es autorizada la incorporación del personal a la organización por parte del Secretario Ejecutivo, se notifica de ésta al Departamento de Gestión y Desarrollo de las Personas, con la finalidad de hacer oficial la vinculación del personal en cuestión.  | Secretario Ejecutivo                      | 2                      |
| 2  | Completar formulario de ingreso           | En virtud de la autorización recibida, se procede a completar el formulario de ingreso dispuesto para solicitar recursos, en el cual se deberán especificar los recursos que serán asignados al rol que se incorpora, en función de las especificaciones entregadas en la descripción del cargo y por su Jefe Directo según corresponda. | Analista de Gestión y Desarrollo Personas | 3                      |

| ID | ACTIVIDAD   | DESCRIPCIÓN  | RESPONSABLE                     | ID ACTIVIDAD SIGUIENTE |
|----|---|--|---------------------------------|------------------------|
| 3  | Recepción de formulario de ingreso y entrega de recursos        | Se hace recepción del formulario de ingreso, en el cual se encuentran especificados los recursos que deberán ser entregados al rol que se incorpora a la organización.<br>El Analista de Soporte al Usuario deberá revisar la disponibilidad del material solicitado, y hacer entrega al trabajador de lo requerido. | Analista de Soporte al Usuario  | 4                      |
| 4  | Recepción de recursos   | El trabajador/a que se incorpora a la organización hace recepción de los recursos y revisa que estos correspondan a lo señalado en el formulario de ingreso. Adicionalmente, deberá firmar el acta de recepción.   | Colaborador(a) de nuevo ingreso | 5                      |
| 5  | Actualización de Registro de Asignaciones Recursos Tecnológicos | Una vez realizada la recepción de el o los recursos tecnológicos, se debe actualizar el estado de éste/éstos en la CMDB mediante su asignación al código del usuario.  | Analista de Soporte al Usuario  | FIN                    |

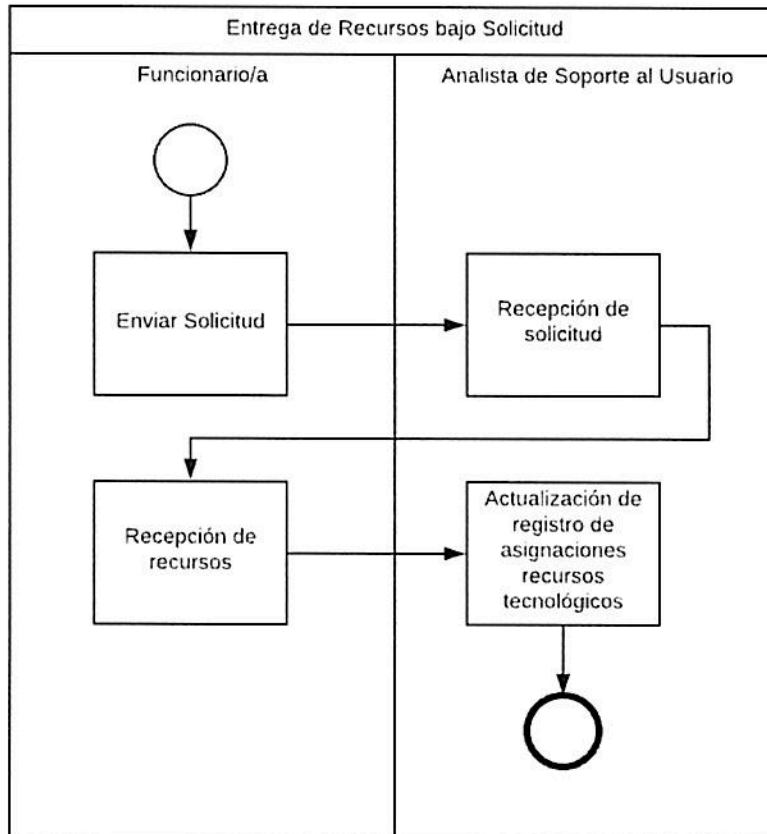
### 7.3 Flujo de Procedimiento para Devolución de Recursos por Desvinculación.



**7.4 Matriz del Proceso de Recepción de Recursos en caso de Desvinculación de Personal.**

| ID | ACTIVIDAD   | DESCRIPCIÓN   | RESPONSABLE                               | ID ACTIVIDAD SIGUIENTE |
|----|---|---|---|------------------------|
| 1  | Completar formulario de Entrega de Activos                      | Se procede a llenar el formulario de Entrega de Activos.  | Analista de Gestión y Desarrollo Personas | 2                      |
| 2  | Recepción de formularios de Entrega de Activos                  | Se hace recepción del formulario de Entrega de Activos. El Analista de Soporte al Usuario deberá revisar que el trabajador tenga recursos asignados, si es así, procede a realizar la recepción de estos. | Analista de Soporte al Usuario            | 3                      |
| 3  | Devolución de recursos  | El trabajador que ha dejado de formar parte de la organización procede a devolver los recursos que le han sido entregados y firma el acta de retiro de estos.   | Trabajador                                | 4                      |
| 4  | Actualización de Registro de Asignaciones Recursos Tecnológicos | Una vez realizada la recepción de el o los recursos tecnológicos, se debe actualizar el estado de éste/éstos en la CMDB como "disponible(s)".   | Analista de Soporte al Usuario            | FIN                    |

**7.5 Flujo de Procedimiento para Entrega de Recursos por Solicitud.**



## 7.6 Matriz del Proceso de Entrega de Recursos en caso de Solicitud.

| ID | ACTIVIDAD   | DESCRIPCIÓN  | RESPONSABLE                    | ID ACTIVIDAD SIGUIENTE |
|----|---|--|--------------------------------|------------------------|
| 1  | Elevar solicitud  | El trabajador en cuestión procede a elevar una solicitud a su Jefe Directo para la obtención de recursos esenciales para la realización de sus funciones.  | Trabajador                     | 2                      |
| 2  | Recepción de solicitud  | Se hace recepción de la solicitud aprobada por el Jefe Directo del trabajador, a continuación, se procede a verificar la disponibilidad del activo solicitado. En caso de tener stock del activo especificado, deberá ser facilitado al rol en cuestión. | Analista de Soporte al Usuario | 3                      |
| 3  | Recepción de recursos   | El trabajador hace recepción de los recursos y revisa que estos se encuentren en buen estado. Adicionalmente, deberá firmar el acta de recepción.  | Trabajador                     | 4                      |
| 4  | Actualización de Registro de Asignaciones Recursos Tecnológicos | Una vez realizada la recepción de el o los recursos tecnológicos, se debe actualizar el estado de éste/éstos en la CMDB como "disponible(s)".  | Analista de Soporte al Usuario | FIN                    |

## 7.7 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

De esta forma, la matriz de responsabilidades para el proceso de ingreso de nuevo personal es la siguiente:

| ID | ACTIVIDAD                                       | TRABAJADOR | JEFATURA DIRECTA | ENCARGADA SI | ANALISTA SOPORTE USUARIO | ANALISTA GESTIÓN | SECRETARIO EJECUTIVO |
|----|---|------------|------------------|--------------|--------------------------|------------------|----------------------|
| 1  | Autorización de contratación del personal       | I          | I                | I            | -                        | -                | R/E                  |
| 2  | Completar formulario de ingreso                 | C          | I                | -            | I                        | R/E              | -                    |
| 3  | Recepción de formulario de ingreso y entrega de | I          | I                | -            | R/A                      | -                | -                    |

|   |   |     |   |   |     |   |   |
|---|---|-----|---|---|-----|---|---|
|   | <b>recursos</b>   |     |   |   |     |   |   |
| 4 | Recepción de recursos   | R/E | - | I | R/A | - | - |
| 5 | Actualización de Registro de Asignaciones Recursos Tecnológicos | -   | - | - | R/E | - | - |

De esta forma, la matriz de responsabilidades para e proceso de desvinculación es la siguiente:

| ID | ACTIVIDAD   | TRABAJADOR | JEFATURA DIRECTA | ENCARGADA SI | ANALISTA SOPORTE USUARIO | ANALISTA GESTIÓN |
|----|---|------------|------------------|--------------|--------------------------|------------------|
| 1  | Completar formulario de Entrega de Activos                      | C          | I                | -            | I                        | R/E              |
| 2  | Recepción de formularios de Entrega de Activos                  | I          | I                | -            | R/A                      | -                |
| 3  | Devolución de recursos  | R/E        | -                | I            | R/A                      | -                |
| 4  | Actualización de Registro de Asignaciones Recursos Tecnológicos | -          | -                | -            | R/E                      | -                |

De esta forma, la matriz de responsabilidades para e proceso de solicitud de recursos es la siguiente:

| ID | ACTIVIDAD   | TRABAJADOR | JEFATURA DIRECTA | ENCARGADA SI | ANALISTA SOPORTE USUARIO |
|----|---|------------|------------------|--------------|--------------------------|
| 1  | Elevar solicitud  | R/E        | A                | I            | -                        |
| 2  | Recepción de solicitud  | C          | I                | -            | R/E                      |
| 3  | Recepción de recursos   | E/A        | I                | -            | R                        |
| 4  | Actualización de Registro de Asignaciones Recursos Tecnológicos | -          | -                | -            | R/E                      |

### 8. Registro de Operación.

| REGISTRO                                     | ID | RESPONSABLE/DUEÑO DEL REGISTRO | TIEMPO RETENCIÓN      | SOPORTE | LUGAR |
|--|----|--------------------------------|-----------------------|---------|-------|
| Registro de asignaciones actualizado en CMDB | -  | Analista de Soporte al Usuario | 4 años / Archivo UTIC | Digital | CMDB  |




**LISTA DE ASISTENCIA**  
**Comité de Seguridad de la Información**  
**Implementación PMG- Sistema de Seguridad de la Información**

- I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Estructura funcional del Sistema de Gestión de Seguridad de la Información y Ciberseguridad al interior de la Agencia de Calidad de la Educación
  2. Procedimiento de Contacto con Autoridades. Control A.6.1.3
  3. Procedimiento de Contacto con Grupos de Interés. Control A.6.1.4
  4. Política de Seguridad para Recursos Humanos. Control A.7.1.2
  5. Procedimiento de elaboración / Actualización de inventario de Activos. Control A.8.1.1 y su registro de operación.
  6. Procedimiento de Asignación y Devolución de Recursos. Control A.8.1.4
  7. Política de Control de Acceso físico y lógico. Control A.9.1.1 y A. 11.1.1
  8. Procedimiento de Inicio de Sesión Seguro. Control A.9.4.2
  9. Política de Ubicación y Protección del Equipamiento de la Agencia de Calidad de la Educación. Control A.11.2.1
  10. Procedimiento de Mantenimiento de Equipos Críticos. Control A.11.02.04
  11. Procedimiento de eliminación o Reutilización de Equipamiento. Control A.11.2.7
  12. Procedimiento de Equipo de Usuario Desatendido. Control A.11.02.08
  13. Política de Escritorio y Pantalla limpios. Control A.11.2.9
  14. Procedimiento de Respaldo de Información. Control A.12.03.01

Fecha: 3 de julio de 2019

| N° | Nombre                   | Cargo                                    | Firma |
|----|--------------------------|--|-------|
| 1  | Juan Bravo               | Secretario Ejecutivo (S)                 |       |
| 2  | Gino Cortez              | Jefe de DEOD (S)                         |       |
| 3  | Cristóbal Alarcón        | Jefe de DIAC                             |       |
| 4  | Mariana Segura           | Jefa de DEIA(S) y DAG (S)                |       |
| 5  | María de la Luz González | Jefa de DIEST (S)                        |       |
| 6  | Andrea Soto Araya        | Encargada de SSI                         |       |
| 7  | Nicol Jeria              | Encargada de Ciberseguridad              |       |
| 8  | Sergio Hidalgo           | Jefe Departamento de Auditoría           |       |
| 9  | Gabriel Cáceres          | Encargado de Unidad de Planificación (s) |       |
| 10 | Patrick Soto             | Jefe Unidad TIC                          |       |
| 11 | Yerko Braun              | Protección DIAC                          |       |
| 12 | Carlo Conado             | Comisión Externa                         |       |



|  |   |                 |                                  |
|--|---|-----------------|----------------------------------|
|  <p>Agencia de<br/>Calidad de la<br/>Educación</p> <p>Gobierno de Chile</p> | <b>Procedimiento de Eliminación o Reutilización de Equipamiento</b> |                 |                                  |
|  | Nivel de Confidencialidad   | -               | Páginas <b>1-5</b>               |
|  | Fecha versión del documento   | <b>28-06-19</b> | Versión <b>0</b>                 |
|  |   |                 | Código <b>SGSIC-PRO-A.11.2.7</b> |
| <b>Procedimiento de Eliminación o Reutilización de Equipamiento</b>  |   |                 |                                  |

## Procedimiento de Eliminación o Reutilización de Equipamiento

### Control A.11.02.07

#### Tabla de Contenidos

|            |   |          |
|------------|---|----------|
| <b>1</b>   | <b>Objetivo.....</b>  | <b>1</b> |
| <b>2</b>   | <b>Alcance.....</b>   | <b>1</b> |
| <b>3</b>   | <b>Normas y Referencias.....</b>  | <b>2</b> |
| <b>4</b>   | <b>Términos y Definiciones. ....</b>  | <b>2</b> |
| <b>5.</b>  | <b>Roles y Responsabilidades.....</b>   | <b>2</b> |
| <b>6.</b>  | <b>Directrices Generales para la Entrega y Devolución de Recursos.....</b>                | <b>2</b> |
| <b>7.</b>  | <b>Modo de Operación.....</b>   | <b>3</b> |
| <b>7.1</b> | <b>Flujo de Procedimiento.....</b>  | <b>3</b> |
| <b>7.2</b> | <b>Matriz del Proceso de Entrega de Activos en caso de Ingreso de Nuevo Personal.....</b> | <b>3</b> |
| <b>7.7</b> | <b>Matriz de Responsabilidades. ....</b>  | <b>5</b> |
| <b>8.</b>  | <b>Registro de Operación. ....</b>  | <b>5</b> |

#### REVISIONES DEL PROCEDIMIENTO

| Nº Versión | Fecha    | Motivo de la revisión | Páginas elaboradas o modificadas |
|------------|----------|-----------------------|----------------------------------|
| Cero (0)   | 28-06-19 | Elaboración inicial   | Todas                            |

| ELABORADO POR   | VALIDACIÓN TÉCNICA       | APROBADO POR  | APROBADO POR    |
|---|--------------------------|---|-----------------|
| Sistema de Gestión de Seguridad de Información y Ciberseguridad | Patrick Soto<br>Jefe TIC | Andrea Soto Araya<br>Encargada de Seguridad de la Información | Comité de SGSIC |

#### 1. Objetivo.

Este procedimiento tiene por finalidad tanto determinar el mecanismo de verificación del equipamiento por eliminar o reutilizar, para asegurar que estos no contengan información confidencial, como especificar los mecanismos de destrucción de información sensible, o que cuente con derechos de autor, de la Agencia de Calidad de la Educación

#### 2. Alcance.

Todos los equipos institucionales inventariados, cuya adquisición haya significado la inversión de recursos par la Institución como, por ejemplo, computadores personales, teléfonos celulares, dispositivos portátiles y otros que se pongan a disposición del personal o de funcionarios(as) en particular, y que por el término de la vida útil de este, deberá ser eliminado para destrucción o reutilización.

### 3. Normas y Referencias.

- Ley N° 19.223, sobre Figuras Penales relativas a la Informática.
- Ley N° 20.285, sobre Acceso a la Información Pública.
- DS N° 83/2005, del Ministerio Secretaría General de la Presidencia, Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
- Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información - Requisitos.
- Norma NCh-ISO 27002:2013, Código de Prácticas para la Gestión de la Seguridad de la Información.
- Política General de Seguridad de la Información de la Agencia de Calidad de la Educación, vigente.
- Política de Uso de Celulares Corporativos de la Agencia de Calidad de la Educación, vigente.

### 4 Términos y Definiciones.

|  |   |
|--|---|
| <b>Borrado Seguro (Wiping)</b>             | Proceso mediante el cual se sobrescribe varias veces cada segmento de la superficie del disco del equipo en cuestión con cadenas aleatorias de ceros y unos.      |
| <b>Distro Linux (System Rescue 6.0.2.)</b> | Proceso de borrado seguro, cuyo objetivo es específicamente el que la información que una vez fue contenida por el equipo no pueda ser recuperada posteriormente. |

### 5. Roles y Responsabilidades.

- Unidad de Tecnologías de Información y Comunicación:** Es responsabilidad de la Unidad eliminar correctamente la información contenida en los equipos que serán eliminados, reutilizados o devueltos a los proveedores. Una vez se determine que la información que contiene un equipo será eliminada, la Unidad deberá comunicar de esto al Encargado(a) de Seguridad de la Información, mediante la utilización del "Registro de Eliminación de Información o Equipamiento". En caso de que un equipo deba ser formateado para su posterior reutilización, la Unidad deberá solicitar la autorización de la Jefatura de la División de Administración General.
- Encargado(a) de Seguridad de la Información:** Como rol líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), tiene la responsabilidad de monitorear el cumplimiento de este procedimiento. Adicionalmente debe ser notificado del acta de eliminación que entrega la Unidad TIC.
- Jefatura de División de Administración General:** Como supervisores de las acciones realizadas por la Unidad TIC, deberá autorizar el formateo de los equipos que serán reutilizados posteriormente por personal de la organización.

### 6. Directrices Generales para la Entrega y Devolución de Recursos.

Teniendo en cuenta la importancia de la información manipulada dentro de la institución, particularmente en relación con la privacidad y confidencialidad de esta, es necesario tomar las precauciones pertinentes para la protegerla. En función de lo anterior la organización ha definido los siguientes tipos de eliminación de información para los diferentes escenarios presentados a continuación:

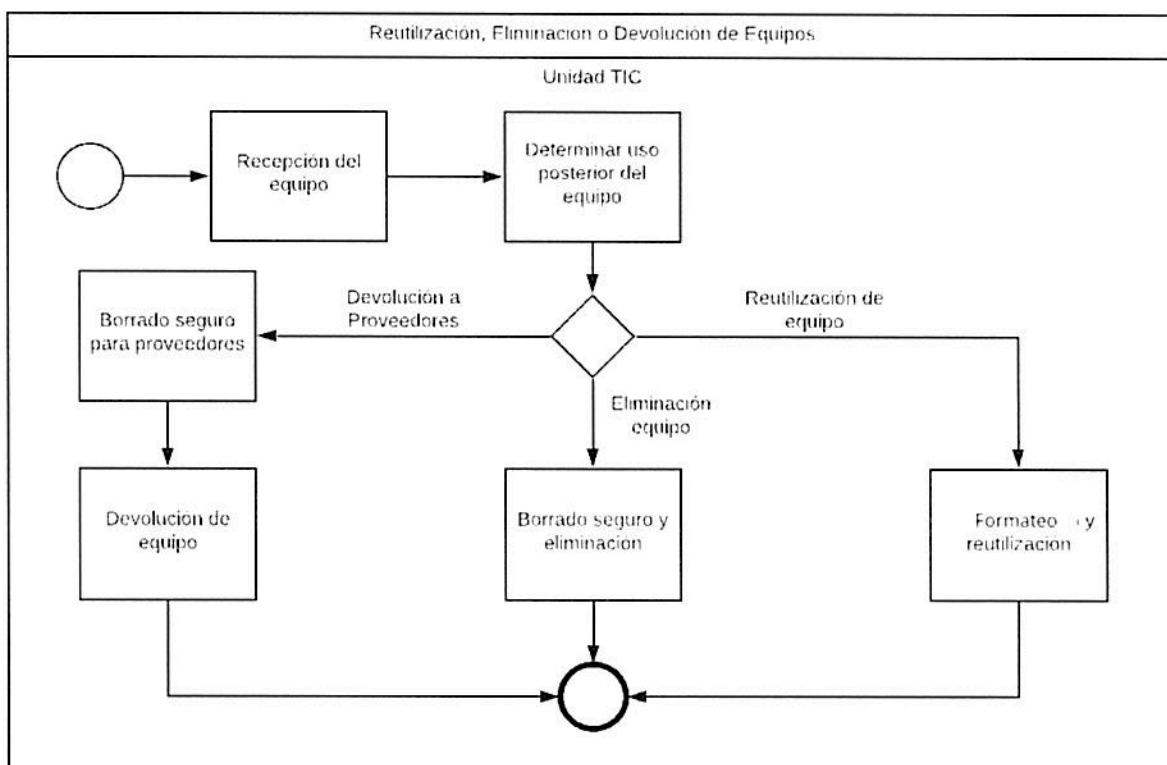
| TIPO DE EVENTO                  | FORMA DE ELIMINACIÓN DE INFORMACIÓN   |
|---------------------------------|---|
| <b>Eliminación del Equipo</b>   | Borrado Seguro (Wiping)   |
| <b>Reutilización del Equipo</b> | Borrado Seguro (Wiping)<br>Actualización del ID del equipo en la CMDB, quedando con estado "Disponible" |
| <b>Devolución del Equipo</b>    | Borrado Seguro (Wiping)<br>Distro Linux, system rescue 6.0.2  |

Es importante detallar que una vez sea realizada cualquiera de estas formas de eliminación, deberá ser llenado el "Registro de Eliminación de Información o Equipamiento", el cual deberá ser visado por el Encargado(a) de Seguridad de la Información.

### 7. Modo de Operación.

De acuerdo con los eventos descritos anteriormente, se establece un flujo comunicacional específico, en donde, de acuerdo con el tipo de evento, se definen las tareas pertinentes, así como los roles responsables de la realización de estas.

#### 7.1 Flujo de Procedimiento.



#### 7.2 Matriz del Proceso de Entrega de Activos en caso de Ingreso de Nuevo Personal.

| ID | ACTIVIDAD | DESCRIPCIÓN | RESPONSABLE | ID ACTIVIDAD SIGUIENTE |
|----|-----------|-------------|-------------|------------------------|
|----|-----------|-------------|-------------|------------------------|

| ID | ACTIVIDAD                           | DESCRIPCIÓN  | RESPONSABLE | ID ACTIVIDAD SIGUIENTE |
|----|-------------------------------------|--|-------------|------------------------|
| 1  | Recepción del equipo                | Una vez que el equipo ha cumplido su vida útil dentro de la organización y es necesario que este sea eliminado, debe ser entregado a Unidad TIC para asegurar que la información almacenada dentro de estos equipos sea correctamente eliminada.   | Unidad TIC  | 2                      |
| 2  | Determinar uso posterior del equipo | Con el objetivo de hacer un borrado seguro de la información contenida en el equipo, es necesario determinar correctamente el uso posterior que se le dará al equipo en cuestión, este puede ser: <ul style="list-style-type: none"> <li>- Equipo será devuelto a los proveedores (3)</li> <li>- Equipo será eliminado (4)</li> <li>- Equipo será reutilizado (5)</li> </ul> | Unidad TIC  | 3, 4, o 5              |
| 3  | Borrado seguro para proveedores     | Se deberá efectuar un borrado seguro (Wiping). Adicionalmente se deberá correr Distro Linux (System rescue 6.0.2) con el objetivo de que la información no pueda ser recuperada por los proveedores  | Unidad TIC  | 3A                     |
| 3A | Devolución de equipo                | Una vez se ha asegurado que la información que el equipo contenía no puede ser recuperada, se puede efectuar la devolución del equipo al proveedor.  | Unidad TIC  | FIN                    |
| 4  | Borrado seguro y eliminación        | Se procederá a efectuar un borrado seguro sobre el equipo (Wiping), haciendo utilización también de Distro Linux (System rescue 6.0.2). Una vez este sea realizado, se procederá a eliminar el equipo según lo establecido en el Procedimiento de Eliminación de Medios.   | Unidad TIC  | FIN                    |

| ID | ACTIVIDAD                      | DESCRIPCIÓN   | RESPONSABLE | ID ACTIVIDAD SIGUIENTE |
|----|--------------------------------|---|-------------|------------------------|
| 5  | Borrado seguro y reutilización | <p>Se efectuará el borrado seguro del equipo. Posteriormente se deberá actualizar el ID del equipo en la CMDB, quedando este como "disponible". Cuando el equipo sea asignado para su reutilización, se deberá asignar el ID cambiado al trabajador a quien fue asignado el equipo.</p> <p><b>Nota:</b> Es importante detallar que en caso de que un equipo deba ser reutilizado posteriormente, es la Jefatura de la División de Administración General quien debe autorizar el formateo del equipo en cuestión.</p> | Unidad TIC  | FIN                    |

### 7.3 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

De esta forma, la matriz de responsabilidades para el proceso es:

| ID | ACTIVIDAD                           | UNIDAD TIC | ENCARGADA SI | JEFATURA DAG |
|----|-------------------------------------|------------|--------------|--------------|
| 1  | Recepción del equipo                | R/E        | I            | I            |
| 2  | Determinar uso posterior del equipo | R/E        | -            | -            |
| 3  | Borrado seguro para proveedores     | R/E        | A            | I            |
| 3A | Devolución de equipo                | R/E        | -            | -            |
| 4  | Borrado seguro y eliminación        | R/E        | A            | -            |
| 5  | Borrado seguro y reutilización      | R/E        | A            | A            |

### 8. Registro de Operación.

| REGISTRO | ID | RESPONSABLE/D<br>UEÑO DEL<br>REGISTRO | TIEMPO<br>RETENCIÓN | SOPORTE | LUGAR |
|----------|----|---------------------------------------|---------------------|---------|-------|
|----------|----|---------------------------------------|---------------------|---------|-------|

| <b>REGISTRO</b>                             | <b>ID</b> | <b>RESPONSABLE/DUEÑO DEL REGISTRO</b> | <b>TIEMPO RETENCIÓN</b> | <b>SOPORTE</b> | <b>LUGAR</b> |
|---|-----------|---------------------------------------|-------------------------|----------------|--------------|
| Inventario de recursos tecnológicos en CMDB | -         | Analista de Soporte al Usuario        | 4 años / Archivo UTIC   | Digital        | CMDB         |

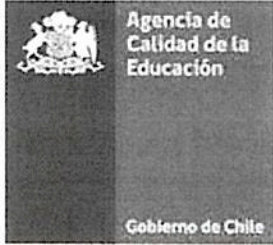


**LISTA DE ASISTENCIA**  
**Comité de Seguridad de la Información**  
**Implementación PMG- Sistema de Seguridad de la Información**

- I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Estructura funcional del Sistema de Gestión de Seguridad de la Información y Ciberseguridad al interior de la Agencia de Calidad de la Educación
  2. Procedimiento de Contacto con Autoridades. Control A.6.1.3
  3. Procedimiento de Contacto con Grupos de Interés. Control A.6.1.4
  4. Política de Seguridad para Recursos Humanos. Control A.7.1.2
  5. Procedimiento de elaboración / Actualización de inventario de Activos. Control A.8.1.1 y su registro de operación.
  6. Procedimiento de Asignación y Devolución de Recursos. Control A.8.1.4
  7. Política de Control de Acceso físico y lógico. Control A.9.1.1 y A. 11.1.1
  8. Procedimiento de Inicio de Sesión Seguro. Control A.9.4.2
  9. Política de Ubicación y Protección del Equipamiento de la Agencia de Calidad de la Educación. Control A.11.2.1
  10. Procedimiento de Mantenimiento de Equipos Críticos. Control A.11.02.04
  11. Procedimiento de eliminación o Reutilización de Equipamiento. Control A.11.2.7
  12. Procedimiento de Equipo de Usuario Desatendido. Control A.11.02.08
  13. Política de Escritorio y Pantalla limpios. Control A.11.2.9
  14. Procedimiento de Respaldo de Información. Control A.12.03.01

Fecha: 3 de julio de 2019

| N° | Nombre                   | Cargo                                    | Firma |
|----|--------------------------|--|-------|
| 1  | Juan Bravo               | Secretario Ejecutivo (S)                 |       |
| 2  | Gino Cortez              | Jefe de DEOD (S)                         |       |
| 3  | Cristóbal Alarcón        | Jefe de DIAC                             |       |
| 4  | Mariana Segura           | Jefa de DEIA(S) y DAG (S)                |       |
| 5  | María de la Luz González | Jefa de DIEST (S)                        |       |
| 6  | Andrea Soto Araya        | Encargada de SSI                         |       |
| 7  | Nicol Jeria              | Encargada de Ciberseguridad              |       |
| 8  | Sergio Hidalgo           | Jefe Departamento de Auditoría           |       |
| 9  | Gabriel Cáceres          | Encargado de Unidad de Planificación (s) |       |
| 10 | YATMICK SOTO             | Jefe Unidad TIC                          |       |
| 11 | Yerlin Barea             | Profesional DIAC                         |       |
| 12 | Claudio Corado           | Consultor Externo                        |       |



**Procedimiento de Equipo de Usuario Desatendido**

|                             |          |         |                    |
|-----------------------------|----------|---------|--------------------|
| Nivel de Confidencialidad   | -        | Páginas | 1-5                |
| Fecha versión del documento | 28-06-19 | Versión | 0                  |
|                             |          | Código  | SGSIC-PRO-A.11.2.8 |

**Procedimiento de Equipo de Usuario Desatendido**

**Procedimiento de Equipo de Usuario Desatendido**  
**Control A.11.02.08**

Tabla de Contenidos

|            |   |          |
|------------|---|----------|
| <b>1</b>   | <b>Objetivo.....</b>  | <b>2</b> |
| <b>2</b>   | <b>Alcance.....</b>   | <b>2</b> |
| <b>3</b>   | <b>Normas y Referencias.....</b>  | <b>2</b> |
| <b>4</b>   | <b>Términos y Definiciones.....</b>   | <b>2</b> |
| <b>5</b>   | <b>Roles y Responsabilidades.....</b>   | <b>2</b> |
| <b>6</b>   | <b>Directrices Generales para la Entrega y Devolución de Recursos.....</b>    | <b>3</b> |
| <b>7</b>   | <b>Modo de Operación.....</b>   | <b>3</b> |
| <b>7.1</b> | <b>Flujo de Procedimiento.....</b>  | <b>3</b> |
| <b>7.2</b> | <b>Matriz del Proceso de Protección de Equipo de Usuario Desatendido.....</b> | <b>4</b> |
| <b>7.3</b> | <b>Matriz de Responsabilidades.....</b>                                       | <b>5</b> |
| <b>8</b>   | <b>Registro de Operación.....</b>   | <b>5</b> |

**REVISIONES DEL PROCEDIMIENTO**

| Nº Versión | Fecha    | Motivo de la revisión | Páginas elaboradas o modificadas |
|------------|----------|-----------------------|----------------------------------|
| Cero (0)   | 28-06-19 | Elaboración inicial   | Todas                            |

|   |                           |   |                     |
|---|---------------------------|---|---------------------|
| <b>ELABORADO POR</b>  | <b>VALIDACIÓN TÉCNICA</b> | <b>APROBADO POR</b>   | <b>APROBADO POR</b> |
| Sistema de Gestión de Seguridad de Información y Ciberseguridad | Patrick Soto<br>Jefe TIC  | Andrea Soto Araya<br>Encargada de Seguridad de la Información | Comité de SGSIC     |





## 1. Objetivo.

El presente procedimiento tiene por finalidad establecer las actividades y paso a paso para promover e instaurar el bloqueo del computador por parte del usuario una vez que éste ha desocupado su estación de trabajo, a modo de proteger los Activos de Información que se encuentran almacenados en el computador o en la nube a la que el usuario tiene acceso mediante su equipo.

## 2. Alcance.

El procedimiento debe ser aplicado por todos los computadores que estén en funcionamiento, tanto dentro como fuera de la Agencia de Calidad de la Educación, que contengan información relacionada con la institución.

## 3. Normas y Referencias.

- Decreto Supremo N° 83, Norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Resolución Exenta N° 1440, Política General de Seguridad de la Información.
- Norma NCh-ISO 27001:2009, Sistemas de Gestión de la Seguridad de la Información - Requisitos. Anexo A, A.10.5.1
- Norma NCh-ISO 27002:2009, Código de prácticas para la gestión de la seguridad de la información, Control 10.5.1.

## 4. Términos y Definiciones.

|                              |   |
|------------------------------|---|
| <b>Proteger Documentos</b>   | Acción de bloquear el computador, con la finalidad de proteger los activos de información contenidos en este. Esta acción se lleva a cabo mediante la combinación de teclas: Ctrl + Alt+ Supr<br>Esta acción es también realizada por la Unidad TIC mediante la utilización de Active Directory para bloquear el computador luego de que han pasado cinco (5) minutos de inactividad. |
| <b>Usuario</b>               | Hace referencia al responsable del bloqueo de su computador, el cual contiene información sensible para la institución.   |
| <b>Activo de Información</b> | La información es un activo fundamental para el desarrollo, operativa, control y gestión de la institución. Esta es considerada como información propiamente tal, abstrayéndola del medio en el que se encuentra almacenada.  |
| <b>Restricción de Acceso</b> | Delimitar el acceso de los usuarios, servidores públicos a honorarios y terceras partes a determinados recursos de la organización.   |
| <b>Estación de Trabajo</b>   | Un computador que facilita a los usuarios(as) el acceso a los servidores y periféricos de la organización.  |
| <b>Active Directory</b>      | Es el termino usado por Microsoft para referirse a la implementación de un servicio de directorio en una red distribuida de computadores. En la Agencia de Calidad de la Educación, es el sistema implementado para acceder a cada equipo computacional.  |
| <b>Contraseña</b>            | Forma de autenticación que utiliza información secreta para controlar el acceso a cierto recurso.   |

## 5. Roles y Responsabilidades.

- a) **Unidad de Tecnologías de Información y Comunicación:** Es responsabilidad de la Unidad el proteger los computadores de la organización mediante la activación del

bloqueo automático en cada uno de los equipos de los funcionarios, cumplido cierto espacio de tiempo determinado, mediante la utilización de la herramienta Active Directory.

- b) **Encargado(a) de Seguridad de la Información:** Como rol líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), tiene la responsabilidad de monitorear el cumplimiento de este procedimiento.
- c) **Usuario:** Es responsabilidad del trabajador perteneciente a la Agencia de Calidad de la Educación, bloquear su estación de trabajo una vez ha dejado de utilizarla.

## **6. Directrices Generales para la Protección del Usuario Desatendido.**

Teniendo en consideración la importancia de la protección de la información manipulada dentro de la organización, es necesario tomar precauciones pertinentes para que agentes externos no tengan acceso a esta mediante la utilización del equipo desatendido de alguno de los trabajadores de la institución. En función de lo anterior, se especifican a continuación las posibles formas de protección de información y bloqueo del equipo:

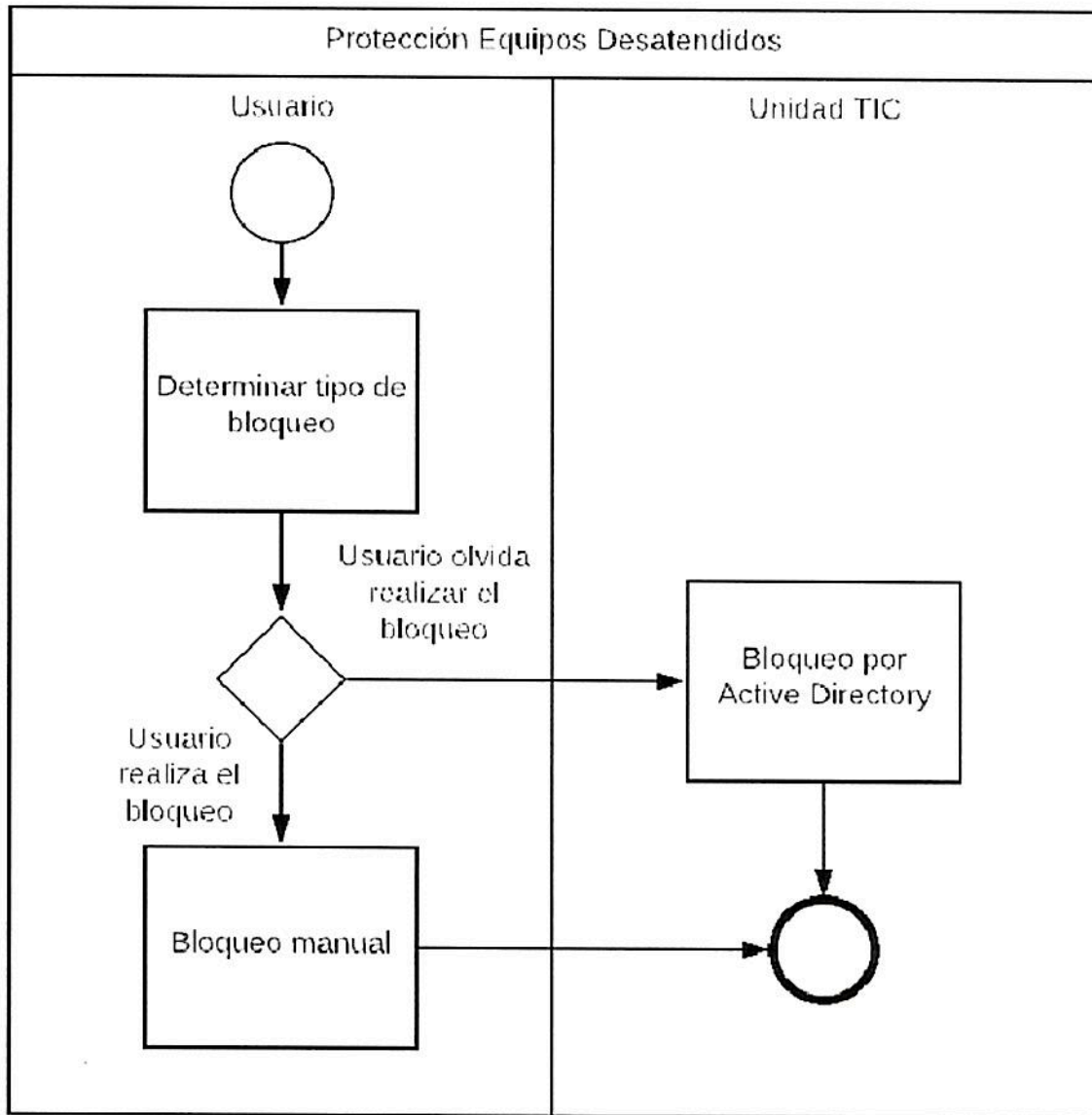
| <b>TIPO DE BLOQUEO</b>              | <b>EJECUTOR</b> | <b>FORMA DE PROTECCIÓN DE INFORMACIÓN</b>   |
|-------------------------------------|-----------------|---|
| <b>Bloqueo Manual</b>               | Usuario         | Hace referencia al bloqueo del equipo que realiza el usuario a quien pertenece este, el cual es realizado mediante la combinación de las teclas: Ctrl + Alt + Spr   |
| <b>Bloqueo por Active Directory</b> | Unidad TIC      | Bloqueo remoto efectuado por la Unidad TIC sobre todos los computadores de la institución mediante Active Directory. Este bloqueo se activa sobre el equipo en cuestión una vez que ha estado desatendido por un periodo de cinco (5) minutos. Se pueden encontrar los detalles de esta configuración en el Anexo I: Configuración Active Directory para bloqueo automático de estaciones de trabajo. |

Es importante detallar que cada uno de los usuarios tiene la responsabilidad de bloquear su equipo una vez que ha dejado de utilizarlo.

## **7. Modo de Operación.**

De acuerdo con los tipos de bloqueo descritos anteriormente, se establece un flujo de actividades específico, en donde, de acuerdo con el tipo de evento, se definen las tareas pertinentes, así como los roles responsables de la realización de estas.

### **7.1 Flujo de Procedimiento.**



**7.2 Matriz del Proceso de Protección de Equipo de Usuario Desatendido.**

| ID | ACTIVIDAD                  | DESCRIPCIÓN   | RESPONSABLE | ID ACTIVIDAD SIGUIENTE |
|----|----------------------------|---|-------------|------------------------|
| 1  | Determinar tipo de bloqueo | <p>Una vez que el usuario ha terminado de utilizar el equipo, se deberá determinar el tipo de bloqueo que tendrá efecto:</p> <ul style="list-style-type: none"> <li>- Bloqueo Manual (2)</li> <li>- Bloqueo por Active Directory (3)</li> </ul> <p><b>Nota:</b> Es importante especificar que es responsabilidad del usuario realizar el bloqueo de su equipo, por lo que el bloqueo por Active Directory está implementado como una medida preventiva en caso de que el usuario olvide realizar el bloqueo manual.</p> | Usuario     | 2, 3                   |

| ID | ACTIVIDAD                    | DESCRIPCIÓN   | RESPONSABLE      | ID ACTIVIDAD SIGUIENTE |
|----|------------------------------|---|------------------|------------------------|
| 2  | Bloqueo Manual               | El usuario deberá realizar el bloqueo manual del equipo mediante la utilización de la combinación de teclas: Ctrl + Alt+ Supr | Usuario          | FIN                    |
| 3  | Bloqueo por Active Directory | Una vez que el computador este ha estado desatendido por cinco (5) minutos o más, se bloqueará automáticamente.               | Active Directory | FIN                    |

### 7.3 Matriz de Responsabilidades.

En este punto se presenta una matriz de responsabilidades tipo RACIE bajo la siguiente nomenclatura:

- R: Responsable
- A: Aprobador
- C: Consultado
- I: Informado
- E: Ejecutor

De esta forma, la matriz de responsabilidades para el proceso es:

| ID | ACTIVIDAD                    | UNIDAD TIC | USUARIO |
|----|------------------------------|------------|---------|
| 1  | Determinar tipo de bloqueo   | -          | E/R     |
| 2  | Bloqueo Manual               | -          | E/R     |
| 3  | Bloqueo por Active Directory | R/E        | -       |

### 8. Registro de Operación.

| REGISTRO                            | ID | RESPONSABLE/DUEÑO DEL REGISTRO | TIEMPO RETENCIÓN      | SOPORTE | LUGAR                       |
|-------------------------------------|----|--------------------------------|-----------------------|---------|-----------------------------|
| Pantalla de AD con la configuración | -  | Unidad TIC                     | 4 años / Archivo UTIC | Digital | PC Responsable del Registro |



**LISTA DE ASISTENCIA**  
**Comité de Seguridad de la Información**  
**Implementación PMG- Sistema de Seguridad de la Información**

- I. Aprobación de los siguientes procedimientos y políticas de seguridad de la información:
1. Estructura funcional del Sistema de Gestión de Seguridad de la Información y Ciberseguridad al interior de la Agencia de Calidad de la Educación
  2. Procedimiento de Contacto con Autoridades. Control A.6.1.3
  3. Procedimiento de Contacto con Grupos de Interés. Control A.6.1.4
  4. Política de Seguridad para Recursos Humanos. Control A.7.1.2
  5. Procedimiento de elaboración / Actualización de inventario de Activos. Control A.8.1.1 y su registro de operación.
  6. Procedimiento de Asignación y Devolución de Recursos. Control A.8.1.4
  7. Política de Control de Acceso físico y lógico. Control A.9.1.1 y A. 11.1.1
  8. Procedimiento de Inicio de Sesión Seguro. Control A.9.4.2
  9. Política de Ubicación y Protección del Equipamiento de la Agencia de Calidad de la Educación. Control A.11.2.1
  10. Procedimiento de Mantenimiento de Equipos Críticos. Control A.11.02.04
  11. Procedimiento de eliminación o Reutilización de Equipamiento. Control A.11.2.7
  12. Procedimiento de Equipo de Usuario Desatendido. Control A.11.02.08
  13. Política de Escritorio y Pantalla limpios. Control A.11.2.9
  14. Procedimiento de Respaldo de Información. Control A.12.03.01

Fecha: 3 de julio de 2019

| N° | Nombre                   | Cargo                                    | Firma |
|----|--------------------------|--|-------|
| 1  | Juan Bravo               | Secretario Ejecutivo (S)                 |       |
| 2  | Gino Cortez              | Jefe de DEOD (S)                         |       |
| 3  | Cristóbal Alarcón        | Jefe de DIAC                             |       |
| 4  | Mariana Segura           | Jefa de DEIA(S) y DAG (S)                |       |
| 5  | María de la Luz González | Jefa de DIEST (S)                        |       |
| 6  | Andrea Soto Araya        | Encargada de SSI                         |       |
| 7  | Nicol Jeria              | Encargada de Ciberseguridad              |       |
| 8  | Sergio Hidalgo           | Jefe Departamento de Auditoría           |       |
| 9  | Gabriel Cáceres          | Encargado de Unidad de Planificación (s) |       |
| 10 | TATNICK SOTO             | Jefe Unidad TIC                          |       |
| 11 | Yerko Bruna              | Profesional DIAC                         |       |
| 12 | Claudio Conado           | Consultor Externo                        |       |