1. Objetivo

Las políticas de seguridad de la información son un conjunto de reglas, procedimientos y normas que regulan la forma en que una organización previene, protege y maneja los riesgos inherentes al uso de las tecnologías de la información.

El presente documento no se trata de una documentación técnica con respecto de la seguridad de la información, sino que trata de definiciones con respecto del comportamiento esperado de los usuarios de los servicios informáticos provistos por el Instituto, tanto funcionarios como alumnado, así como del personal de empresas externas y entidades relacionadas que laboren en los ambientes tecnológicos provistos por AIEP. Del mismo modo, estas políticas determinarán la forma en que dichos servicios son prestados y las actividades que realizará la Dirección Nacional de TI para su provisión

Por lo indicado anteriormente, estas políticas han de ser aprobadas al máximo nivel dentro de la organización y posteriormente publicadas para el conocimiento de todo el personal y alumnado del Instituto.

Las políticas aquí descritas se aplican a todas las sedes y a sus respectivas áreas que hagan uso de los servicios informáticos, siendo responsabilidad de cada una de ellas, cumplir con lo establecido.

La responsabilidad de la actualización, mantención y publicación de este documento recae sobre el Oficial de Seguridad quién deberá realizar revisiones periódicas que permitan determinar la necesidad de adecuaciones producto de cambios en infraestructura, estructura organizacional, incorporación de nuevos elementos de seguridad o bien por necesidad de la empresa.

Es responsabilidad del Director Nacional de TI dar la aprobación y divulgación de éste al interior de AIEP, por medio de reuniones, presentaciones, u otro, así como también de velar por el cumplimiento de estas y aplicar las sanciones al no cumplimiento de las políticas.

Es importante destacar que las políticas aquí descritas deberán cumplirse a cabalidad, de lo contrario se aplicarán las sanciones correspondientes de acuerdo a lo estipulado en la Dirección Nacional de Recursos Humanos y el "Reglamento Interno de Orden, Higiene y Seguridad" en su capítulo XIII. En el caso del alumnado se regirá por el reglamento correspondiente.

Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

DIRECTOR NACIONAL DE CALIDAD

2. Definición

No aplica

3. Sobre la Política

Título 1: De la Seguridad de los Activo Tecnológicos

El objetivo de esta sección es establecer normas que permitan mantener un adecuado control sobre los activos tecnológicos que son de propiedad de la empresa.

Para un mejor entendimiento se entiende por activos tecnológicos a:

Información:
Bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida, información archivada.

Software:
Software de aplicaciones, software de sistemas, software de comunicación y telefonía, herramientas de desarrollo y utilitarios.

- Software desarrollado, a aquel construido por el área de Desarrollo de la Dirección Nacional de TI de acuerdo a los diferentes requerimientos institucionales
- Software de Escuela, a aquel adquirido exclusivamente para una escuela en particular, financiado con el centro de costo propio de ésta y de uso exclusivo
- Software Institucional que es adquirido para ser utilizado por más de una escuela. Los costos en cada caso particular, incluirán las licencias respectivas.

Hardware:
Equipamiento informático (servidores, computadores personales, procesadores, monitores, computadores portátiles, impresoras, mouse, teclados, discos, telefonía, entre otros), equipos de comunicaciones (módems, routers, switch, máquinas de fax, contestadores automáticos entre otros), medios magnéticos de almacenamiento (cintas, discos fijos o externos, pendrive), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento.

Bajo esta premisa la empresa ha definido las siguientes políticas de seguridad:

Título 2: De la compra e instalación de Activos Tecnológicos

a) Toda adquisición de activo tecnológico sea este Hardware o Software, deberá contar previamente con la evaluación y aprobación de la Dirección Nacional de TI, con el fin de que éstos cumplan con los estándares y normas de seguridad establecidos por la Institución.

b) Toda solicitud de compra de activos tecnológicos deberá contar con la aprobación de los estándares de y normas de seguridad por la Dirección Nacional de TI,

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

c) Toda adquisición de activo tecnológico sea este Hardware o Software, deberá ceñirse por el procedimiento de Compra establecido por la Institución y por los proveedores autorizados.

d) Toda adquisición de activo tecnológico sea este Hardware o Software, independiente de su ubicación, deberá tener un identificador único de Activo Fijo.

e) En el caso de la adquisición de servidores será la Dirección de Plataformas y Servicios TI quien decidirán sobre la ubicación física que este tendrá.

f) Todo activo tecnológico adquirido por AIEP deberá ser registrado y catastrado por el personal de Soporte Técnico sean estos de Nivel Central o de Sedes y centralizado en la Dirección de Operaciones.

g) Es responsabilidad del personal de Soporte Técnico el preparar e instalar el software estándar (so, antivirus, administrativos y de Información) de la compañía antes de ser entregados al usuario solicitante.

h) Todo activo tecnológico deberá ser probado en un ambiente de Test antes de adicionarlo a la red de AIEP.

i) Los encargados de Soporte Técnico en Sedes deberán mantener un control sobre el movimiento de la ubicación física de los equipos computacionales, así como de su notificación hacia el personal encargado de Soporte Técnico en Nivel Central

j) Toda instalación de equipamiento tecnológico en sedes Nuevas, se deberá regir por lo establecido en el "Manual de Apertura de Sede" existente en la Dirección de Operaciones.

k) Toda instalación de equipamiento tecnológico deberá ser revisado antes de que sean conectados a la red o pasen a producción a modo de evitar fallas, perdidas de equipamiento o mal funcionamiento de estos.

l) La entrega y retiro de equipamiento tecnológico hacia las unidades de Negocio deberá quedar debidamente respaldado a través de documento con la evidencia de la conformidad tanto de la entrega y recepción por ambas partes.

m) Todo el equipo computacional instalado y conectado en la Red deberá ser de propiedad de la institución, de lo contrario deberá contar con la debida revisión y autorización de la Dirección Nacional de TI para su instalación.

Título 3: De la instalación de software

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

n) Corresponde exclusivamente a la Dirección Nacional de TI el emitir las normas y procedimientos para la instalación y supervisión del software para cualquier tipo de equipo computacional.

o) En los equipos computacionales y de comunicaciones, únicamente se permitirá la instalación de software con licenciamiento apropiado, vigente y acorde a la propiedad intelectual.

p) La Dirección de Operaciones Sedes y Dirección de Plataformas y Servicios serán el único autorizado para la instalación de software en los equipos computacionales.

q) Toda instalación de software que desde el punto de vista de la Dirección Nacional de TI, pudiera poner en riesgo los recursos de la institución no será permitida y será comunicado a hacia la rectoría y vicerrectorías correspondientes.

r) Con el propósito de proteger la integridad de los sistemas informáticos y de comunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software y niveles de seguridad (antivirus, privilegios de acceso, y otros que se apliquen).

s) Queda expresamente prohibida la instalación de todo software y archivos que no sea coincidente con las labores propias del usuario (ej. Juegos, archivos personales, Snifers de red, Servidores virtuales, etc.)

t) La Dirección de Operaciones tiene la responsabilidad de mantener los software institucionales debidamente actualizados

Título 4: De la Administración del Activo Tecnológico.

a) Todos los equipos informáticos pertenecientes al Instituto Profesional AIEP y que residan en este, serán administrados por la Dirección de Plataformas y Servicios TI, perteneciente a la Dirección Nacional de TI, asegurando con ello un desarrollo tecnológico compatible y acorde con las necesidades de modernización en la gestión educativa.

b) En el caso de Servidores que se encuentran externalizados, será responsabilidad de la Dirección de Plataformas y Servicios TI perteneciente a la Dirección Nacional de TI, el definir la responsabilidad de la Administración de éstos.

c) En el caso de que la administración de servidores sea externalizada deberán existir contratos que indiquen dicha responsabilidad, mediante la definición de SLA's.

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

d) La Dirección Nacional de TI confeccionará anualmente un informe con el Análisis de Obsolescencia y renovación del equipamiento tecnológico existente, a modo de mantener los estándares de servicio entregados por todas sus Áreas.

e) Personal de Soporte Técnico (Sede o Nivel Central) será responsable de que todo equipamiento computacional mantenga en sus registros información actualizada acerca de su asignación, ubicación, composición y configuración.

f) Personal de Soporte Técnico estará autorizado para realizar visitas sorpresivas para validar la asignación y ubicación del equipamiento computacional y poder notificar cualquier cambio no autorizado y notificado a la Dirección de Plataformas y Servicios TI y/o a la Dirección de Soporte.

g) Todos los equipos informáticos asignados, serán registrados en el Área de Soporte de la Sede correspondiente.

h) Los activos tecnológicos, que sean asignados a Salas de Clases o Laboratorios para uso de alumnos, será responsabilidad del Jefe del Área de Soporte de dicha Sede, el mantener su control, cuidado y preservación.

i) Los asignatarios del equipamiento computacional de la institución deberán dar cabal cumplimiento con las notificaciones correspondientes de reubicación, reasignación, y todo aquello que implique movimientos en su ubicación física, de adjudicación, sistemas y nuevas labores.

j) El personal encargado de Soporte Técnico tiene la responsabilidad de mantener el equipamiento computacional, excluyendo servidores, bajo un estricto registro y regulación de versiones de software, parches, aplicativos, entre otros.

k) Es responsabilidad del Personal de Plataformas y Seguridad el mantener debidamente registrado y actualizado el software residente en los servidores que son propiedad de AIEP.

l) Las actualizaciones al software deberán ser coordinadas con la Dirección de Operaciones – Soporte Técnico, para que sean registradas y regularizadas en caso de necesitarse licencias adicionales.

Copia no controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

Título 5: Del mantenimiento del Activo Tecnológico

a) Todo servidor y equipos de comunicación deberán contar con una revisión preventiva cada seis meses con el objeto de minimizar los mantenimientos correctivos o fallas en los equipos.

b) El mantenimiento preventivo y correctivo de computadores al interior de AIEP es de exclusiva responsabilidad del personal de Soporte Técnico, dirigidos por la dirección de Plataformas y Servicios TI.

c) La utilización de proveedores de Servicio o Soporte Técnico solo aplicará cuando la Dirección de Operaciones y/o la Dirección de Plataforma y Servicios TI lo estime conveniente.

d) Se excluyen de los servicios de mantención otorgados por el personal de Soporte Técnico, a todo equipamiento computacional no perteneciente a la Institución.

e) Toda falla de funcionamiento en el equipo computacional, deberá ser comunicado vía e-mail exclusivamente al personal encargado de Soporte Técnico.

f) En el caso de requerir reemplazo o sustitución del equipamiento computacional, será el jefe inmediato del usuario quien solicitará por escrito al personal encargado de Soporte Técnico, quien decidirá, de acuerdo a disponibilidad de recursos el dar curso a dicha solicitud.

g) El personal de Soporte Técnico deberá registra todo equipamiento que presente fallas y no tenga reparación, del mismo modo deberá existir un comunicado formal y por escrito al Director Nacional de TI, Director de operaciones y al área contable para notificar su baja.

h) La actualización de software se llevará a cabo de acuerdo a la calendarización que anualmente sea propuesta por la Dirección Nacional de TI.

i) Corresponde a la Dirección Nacional de TI autorizar cualquier adquisición y actualización del software.

j) Las actualizaciones del software desarrollado, se llevarán a cabo de acuerdo a las políticas de desarrollo de aplicaciones de producción correspondientes la Dirección Nacional de TI.

Copia Controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

Título 6: Del Desuso de los Activos Tecnológicos.

a) Todo equipamiento Tecnológico para que sea dado de baja deberá contar con un informe técnico que indique el motivo del porque la máquina ya no puede seguir operando o bien porque está en la lista de donaciones.

b) Todo equipamiento que ha sido dado de baja deberá permanecer en las bodegas correspondientes a cada sede.

c) El área de Soporte Informático deberá mantener un registro actualizado de las bajas de equipamiento computacional de acuerdo a lo registrado en el Inventario de Activos tecnológicos.

d) El Área de Soporte Informático tiene la responsabilidad de comunicar al departamento de contabilidad y/o activo fijo todos aquellos equipos computacionales que han sido dados de baja, con su correspondiente informe de la baja.

e) La Dirección Nacional de TI deberá verificar e informar a la Alta Administración de la Institución de todo equipamiento que pase más de 6 meses guardado en las bodegas a objeto de que se analice una eventual donación a otras instituciones.

Título 7: De las Donaciones de Activos Tecnológicos

a) Será de responsabilidad de la dirección de cada sede la decisión de designar la institución que será beneficiada con la donación. Para esto la Dirección Nacional de TI deberá dar la información de los equipos a donar

b) Una vez acordado el proceso de donación, la Dirección Nacional de TI deberá realizar un inventario de los artículos donados y enviarlos al departamento de Contabilidad y/o Activo Fijo, para su registro y contabilización.

c) La Dirección Nacional de TI deberá informar a su área de Soporte informático de los bienes dados de baja, para que realicen la actualización del Inventario Tecnológico.

d) El traslado de los bienes donados será evaluado cada vez que se produzca el evento de donación.

Copia no controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

Título 8: De la Protección y Conservación de los Activos Tecnológicos.

f) Todo usuario que opere un equipamiento informático está obligado a familiarizarse con las Políticas y Directrices disponible en la Intranet de la Institución, con el objeto de no incurrir en faltas sujetas a sanción.

g) Todo equipo informático que no se encuentre en uso en las horas laborales, por ausentismo del usuario de su lugar de trabajo, deberá ser bloqueado por éste, para proteger el uso indebido del equipo por personas desconocidas.

h) Se prohíbe ingerir alimentos (sólidos o líquidos), en el mismo escritorio, mesa o módulo donde se encuentren ubicados los equipos computacionales, a fin de evitar que los residuos de los mismos al caer sobre cualquier parte del equipo (teclado, ranuras del CPU, monitor, entre otros) los deteriore o malogre.

i) El usuario no podrá agregar, modificar o manipular el equipamiento computacional proporcionado por AIEP o sacarlo de las oficinas sin la autorización expresa del área de Soporte correspondiente o por la Dirección de Plataformas y Servicios TI.

j) Todo medio de almacenamiento de información, que sea insertado en los equipos computacionales de propiedad del Instituto Profesional AIEP, tales como pendrive, discos duros externos, MP3, MP4, etc. deberá ser chequeado previamente a su uso con un antivirus recomendado por el personal Soporte Técnico correspondiente.

k) En el caso que el usuario no cuente con dicha aplicación en su equipo, deberá solicitar directamente al Área de Soporte correspondiente para su instalación

l) Los usuarios que tienen asignado equipamiento computacional son responsables directos de su resguardo y buen uso de los recursos asignados.

m) El usuario asignado será responsable de la pérdida, robo o daño al equipo y/o accesorios que están bajo su cargo, éste estará obligado a la reposición del equipo o a pagar su valor en aquellos casos en que se corrobore un mal manejo o descuido de su parte, en caso contrario las citadas falencias serán cubiertas por la garantía o seguros si es que hubiere.

n) La utilización del equipamiento computacional debe ser única y exclusivamente para el desarrollo propio de las funciones para las cuales fue solicitado, por tanto cualquier mal uso será sancionado.

m) Todo equipamiento computacional asignado y utilizado por más de una persona la responsabilidad recaerá sobre todos aquellos que lo utilizaron.

Copia no controlada

n) Todo equipamiento computacional deberá tener habilitado protectores de pantalla que impidan la visualización de información en las cuales se esta trabajando, en caso de que exista inactividad de 10 minutos.

o) Será de exclusiva responsabilidad del usuario restringir el acceso al equipo computacional asignado en caso de ausentarse, es decir, bloquear el equipo en caso de dejar de utilizarlo.

p) Todos los equipos asignados a un responsable dispondrán de una cuenta y clave de acceso, por lo que es de su competencia y responsabilidad, hacer buen uso de los mismos.

Título 9: De la Seguridad de la Información

Esta sección tiene por finalidad establecer e identificar diferentes niveles de información dentro de la institución, de acuerdo a su sensibilidad, importancia, distribución y propiedad entre otros.

Toda información debe tener una clasificación de acuerdo a los parámetros definidos en el párrafo anterior, así como también la documentación relacionada con estrategias del negocio.

Dado esto, se han definido lo siguiente:

- **De la administración de la información.**

a) Debido al carácter confidencial de la información, el personal que disponga de equipos computacional asignado, deberá de conducirse de acuerdo a los códigos de ética profesional y normas y procedimientos establecidos.

b) Toda aquella información que sea definida como crítica por la Institución deberá ser debidamente respaldada.

c) La propiedad de la información generada con motivo de la actividad normal de la institución es propiedad de éste, por lo que no podrá ser comercializada, distribuida o publicada sin el consentimiento de la rectoría.

d) La Dirección Nacional de TI podrá restringir el uso de dispositivos portables de almacenamiento de información para el equipamiento y por los periodos en que estime conveniente.

Copia Controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

Título 10: Resguardo y Custodia de la información

Información Electrónica

a) Es responsabilidad de la Dirección Nacional de TI el mantener debidamente custodiado todo el software de la Institución, así como también de los programas fuentes de los sistemas confeccionados internamente.

b) Los sistemas operativos de los servidores deberán ser respaldados cuando existan upgrade o actualizaciones de relevancia.

c) Las aplicaciones deberán ser respaldadas una vez puestas en producción y posteriormente respaldadas cada vez que existan modificaciones a los programas.

d) Los cierres financiero contable y de auxiliares de información deben ser respaldados en las fechas que indiquen los usuarios jefes responsables.

e) Los usuarios que posean información confidencial o crítica deberá dar aviso a la Dirección de Plataformas y Servicios TI para que les habilite espacio en el servidor de custodia de información, para que estas entren el proceso de respaldo.

f) Los medios utilizados para los respaldos de información electrónica deben ser protegidos de cualquier acción que atente contra su integridad.

g) Toda información que reside en medios magnéticos como son los respaldos, deberán ser custodiadas en un lugar distinto del departamento de informática.

h) Los medios utilizados para el respaldo de la información deberán ser transportadas hasta su lugar de custodia (interno o externo) en un medio adecuado, con el cual se acredite su máxima seguridad.

i) Los lugares físicos que serán utilizados como almacenaje de los medios magnéticos deberán contar con mecanismos de detección y prevención de incendios, como también mantener una seguridad física y de acceso acorde a lo custodiado.

Información Física

j) En las áreas físicas que conforman las Direcciones de TI no deberán residir reportes o informes con información residente en los sistemas de información o considerada critica para la institución.

Copia Controlada

k) El resguardo y custodia de los documentos, formularios y otros, serán de responsabilidad de cada área habilitar mecanismos para que ésta este disponible para revisiones de la gerencia, entidades fiscalizadoras o auditorías.

Título 11: De la Seguridad Física y Control de Acceso a las Dependencias de TI.

El objetivo de esta sección es asegurar la integridad de los componentes de hardware, software e instalaciones donde se resguardan o se acceden a los activos informáticos.

La protección física se llevará a cabo mediante la creación de diversas barreras físicas alrededor de los departamentos de la organización y de las instalaciones de procesamiento de la información. Donde cada barrera establece un perímetro de seguridad, y que en su conjunto incrementa la protección total de AIEP, tanto en sus sedes como a Nivel central.

Para la administración de las Áreas físicas que custodian los Activos tecnológicos AIEP ha definido áreas críticas que tendrán 3 niveles de acceso, las que se clasificarán de la siguiente manera:

Nivel Crítico Alto: Prohibido su ingreso, y sólo podrá hacerlo "personal autorizado"
Nivel Crítico Medio: Acceso restringido, y sólo podrá hacerlo "personal autorizado"
Nivel Crítico Bajo: Acceso controlado, con supervisión del Encargado del área.

Bajo este esquema la empresa ha definido las siguientes políticas de seguridad:

- **Del Control de Acceso Físico**

a) La Dirección Nacional de TI deberá tener establecido de cual será el perímetro de seguridad para aplicar normas de acceso.

b) El perímetro definido para instalaciones de procesamiento de información deberá ser en lo posible físicamente sólido de lo contrario deberá reforzar las medidas de monitoreo de la sala y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados.

c) El acceso a la sala de servidores existentes en AIEP en su nivel central, deberá contar con los medios de seguridad y protección para prohibir el acceso a ésta.

d) El acceso a la sala de servidores será por medio de la utilización de llaves las cuales deberán estar debidamente autorizadas por la Dirección de Plataformas y Servicios TI o por la Dirección de Operaciones TI (según corresponda).

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

e) La sala de servidores o de procesamiento deberá permanecer siempre cerrada, a modo de evitar accesos de personal no autorizado.

f) El acceso del personal a las zonas de disposición del equipamiento computacional y de comunicaciones crítico, así como el de disposición de respaldos de datos u otros considerados críticos se llevará un registro permanente del tráfico de personal, sin excepción.

g) Toda persona que requiera ingresar a la sala de servidores deberá solicitarlo por escrito al Director de Plataformas y Servicios TI o Director de Operaciones TI (según corresponda), quién determinará su Aceptación o Rechazo.

h) Toda persona que ingrese a la sala de Servidores deberá hacerlo en compañía del encargado de Plataformas y sólo por motivos estrictamente necesarios.

i) En el caso contar con servicios de hausing externalizado para servidores, será el Director de Plataformas y Servicios TI el responsable de mantener una lista con las personas que tendrá la autorización de ingreso al data center y el contacto con el proveedor del servicio.

j) Director de Plataformas y Servicios TI deberá hacer revisiones sorpresivas al registro de visitas, con el fin de validar los accesos y su correspondiente finalidad del acceso.

k) Bajo condiciones de emergencia o de situaciones de urgencia, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la institución.

- **De la Seguridad Física y Ambiental**

a) La sala de servidores y de suministro eléctrico deberá contar mecanismos alternativos de detección de humo y extinción de incendio, que sean adecuados a su propósito para que no produzcan daños a los componentes eléctricos y maquinaria existentes en el área.

b) Para garantizar la eficacia de los sistemas de extinción de incendios, la sala permanecerá sellada respecto al medio ambiente y con único acceso central que garantice la mínima dispersión de los agentes de extinción de incendio.

c) La sala de servidores deberá contar con mecanismos que regulen la temperatura ambiente a 18° C.

Copia no controlada

d) La sala de servidores deberá mantenerse libre de agentes contaminantes, como son polvo, humo, material inflamable y otros.

e) La sala de servidores deberá contar con piso falso y/o de material que esté libre de estática y de acumulación de polvo.

f) La sala de servidores deberá mantenerse cerrada y aislada de la sala de operaciones.

g) La sala de servidores deberá contar con mecanismos que permitan el suministro de electricidad de forma ininterrumpida.

h) Todos los servidores deberán residir en muebles especiales, como son los rack metálicos.

i) Todo el cableado de la red deberá adecuarse según la definición de políticas de Seguridad en Redes.

j) Queda estrictamente prohibido realizar las siguientes actividades dentro de la sala de servidores: comer, beber, fumar, uso de fósforos, encendedores y cualquier otro elemento que pueda provocar daño.

k) La Dirección de Plataformas y Servicios TI deberá realizar revisiones periódicas a los mecanismos de seguridad física y ambiental, con el fin de velar por su buen funcionamiento

l) El equipamiento (servidores, equipos de comunicación y telefonía) deberá mantenerse de acuerdo con las especificaciones recomendadas por los proveedores.

Copia no controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

Título 12: De la Identificación y Autentificación de Usuarios.

Esta sección define estándares mínimos necesarios para controlar que cada usuario que accede a los sistemas y a las Plataformas tecnológicas de la institución, están debidamente reglamentadas y controladas.

- **De la Identificación de Cuentas (UserID o Username)**

a) La Dirección Nacional de TI es responsable de proporcionar a los usuarios el acceso a los recursos informáticos (red y aplicaciones) mediante la creación de una UserID y una Password, previa validación de éste por la Dirección Nacional de Recursos Humanos.

b) Toda cuenta deberá ser creada mediante la utilización del Formulario "Solicitud de Creación y Modificación de Usuarios" (Anexo I).

c) Cada usuario, independiente de su categoría, debe contar con una identificación (UserID o Username) y una password única para acceder a los recursos de la red, base de datos, y sistemas de información.

d) En el caso del personal antiguo de la Institución y que están en cargos igual o superior a Director de Área, se podrá mantener la misma estructura de UserID con las que se crearon inicialmente.

e) Para todo usuario que haya ingresado a la Institución en forma posterior a la implantación de la política, independiente de su cargo su User-ID o Username deberá cumplir con la siguiente composición:

Cuentas de RED

- Personal de Planta
  - Primer nombre + apellido paterno; si se duplica quedará,
  - Primer nombre + apellido paterno + inicial apellido materno; si se volviera a duplicar quedará,
  - Primer nombre + inicial segundo nombre + apellido paterno + inicial del apellido materno.

- Personal Incremental
  - Primer nombre + apellido paterno; si se duplica quedará,
  - Primer nombre + apellido paterno + inicial apellido materno; si se volviera a duplicar quedará,

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

- Primer nombre + inicial segundo nombre + apellido paterno + inicial del apellido materno.

➢ Personal Externo (auditores, proveedores, consultores, etc.)
- Se construirá de forma idéntica al de personal de planta pero se le agregará al comienzo el distintivo de Externo "EXT"
(Ej. EXT+Primer nombre + apellido paterno)

➢ Username para los servidores de Laboratorio.
- Numero de RUT del Alumno (sin digito verificador)

Cuentas de Correo Electrónico

➢ Personal de Planta
- Primer nombre + apellido paterno + @aiep.cl
(ej. raul.parra@aiep.cl); si se duplica quedará,
- Primer nombre + apellido paterno + inicial apellido materno + @aiep.cl
(ej. raul.parra.t@aiep.cl); si se volviera a duplicar quedará,
- Primer nombre + inicial segundo nombre + apellido paterno + inicial del apellido materno + @aiep.cl
(ej.).

➢ Personal Incremental
- Primer nombre + apellido paterno+@adm+año de admisión
(ej. raul.parra@adm2010.aiep.cl); si se duplica quedará,
- Primer nombre + apellido paterno + inicial apellido materno+ @adm+año de admisión
(ej. raul.parra.t@adm2010.aiep.cl); si se volviera a duplicar quedará,
- Primer nombre + inicial segundo nombre + apellido paterno + inicial del apellido materno +@adm+año de admisión
(ej. raul.j.parra.t@adm2010.aiep.cl).

Cuentas de Aplicaciones
- Estas tendrán la misma nomenclatura que las cuentas de red, tanto para personal de planta, incremental y externo.

f) Toda cuenta creada ya sea en los servicios de la red o en Aplicativos y bases de datos deberá identificar claramente el nombre completo del usuario que la utilizará, esto implica nombres, apellidos paterno y materno.

Copia Controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

g) Esta prohibido el uso de User-ID y password de otras personas o facilitar su identificación y password a un tercero. De suceder, el titular de la password será responsable del uso que haga el tercero, haciéndose acreedor de una sanción de acuerdo a lo estipulado en el Reglamento Interno de la Institución.

h) Todo equipo portátil y estación de trabajo poseerá una cuenta de administrador y una cuenta de usuario, más una clave de acceso que será proporcionada por personal de TI. Siendo la cuenta de administrador para el personal de soporte y la otra será entregada al usuario.

i) Toda cuenta que se encuentre inactiva por más de 30 días será notificada

j) Las cuentas de Administrador para red y comunicaciones serán otorgadas bajo la supervisión del Director de Plataforma y Servicios TI y autorizadas por la Dirección Nacional de TI.

k) Las cuentas de Administrador para Aplicaciones y Bases de datos, deberán ser otorgadas bajo la supervisión y autorización del Director Nacional de TI y del Vicerrector o Director correspondiente al usuario catalogado como administrador.

l) Toda cuenta Administradora, deberá ser registrada y actualizada de acuerdo a las necesidades de la institución, indicando el motivo de su creación y su correspondiente evidencia de aprobación por cada una de las partes.

m) Se deberá restringir el uso de cuentas genéricas a lo más mínimo y estas deberán contar con la aprobación de la Dirección Nacional de TI y de la Vicerrectoría o Dirección de una Unidad de Negocio de la Institución.

n) Toda cuenta genérica además deberá tener asociado el nombre de la persona que se responsabilizará de su uso y administración.

o) Toda cuenta genérica deberá esta debidamente documentada, en cuanto a quién la solicita, descripción o justificación de uso y su correspondiente aprobación por las unidades correspondientes.

p) Toda cuenta que se encuentre bloqueada o deshabilitada, deberá contar con procesos de revisiones periódicas, con el fin de determinar su permanencia o eliminación.

q) Toda cuenta de usuario que ya no presta servicios a la institución y forman parte del Aplicativo CRM, No deberá ser borrada del servidor de dominio y deberá ser bloqueada o deshabilitadas por un periodo de 3 años.

Copia no controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

r) Toda cuenta solicitada por un proveedor que requiera tener acceso a una aplicación deberá contar con la aprobación de la unidad de negocio correspondiente a la cual el proveedor le esta dando el servicio.

s) Toda cuenta solicitada por un proveedor y que requiera el acceso a un servidor deberá contar con la autorización del Director de Plataformas y Servicios TI.

t) Toda cuenta solicitada por un proveedor deberá ser creada en forma individualizada con el nombre de la persona que la ocupara.

Copia no controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

a) De la Administración de las Contraseñas de Acceso o Password

i. Del largo mínimo y contenido de las password.

1. Toda contraseña de acceso o password debe ser construida bajo las normas establecidas por la institución, por lo que los servidores y aplicaciones deberán contar con mecanismos para forzar los cambios.

2. La contraseña de acceso o password es personal, intransferible y su uso es de responsabilidad exclusiva del asignatario de dicho equipamiento.

3. La contraseña de acceso o password sea esta de sistema operativo, comunicaciones, sistemas de información y/o bases de datos deberá permanecer siempre encriptada.

4. Las password o claves de acceso de usuarios deberán ser entregadas "expiradas", con el fin de que efectivamente éstas sean cambiadas bajo las normas establecidas.

5. La contraseña de acceso o password se debe crear en base a un conjunto de caracteres alfanuméricos (letras mayúsculas, minúsculas, números y símbolos), las que quedan a criterio del usuario.

6. La contraseña de acceso o password debe ser cambiada después de un periodo determinado de tiempo, y este debe aplicar para todos los que poseen una cuenta. Este tiempo queda establecido en :
   - 60 días para todos los que conforman la red de AIEP
   - 30 días para las cuentas administradoras
   - Número indefinido de días para los usuarios con acceso al dominio de servidores de laboratorio para apoyo a la docencia.

7. Las password para acceder a los recursos de la red y a los Sistemas de Información deberán tener un largo mínimo de 8 caracteres alfanuméricos.

8. Las contraseñas o password utilizadas para acceder a información confidencial y/o privilegiada deberán tener un largo de 9 caracteres alfanuméricos.

9. La contraseña de acceso o password no podrá repetirse hasta en 5 oportunidades de cambio, en el caso de los servidores de laboratorio se establece hasta los últimos 3 cambios.

10. La contraseña de acceso o password no debe estar escritas en cuadernos, tacos, libretas u otro documento que sea de uso común entre los empleados, ya que se pueden divulgar fácilmente.

Copia no controlada

11. La contraseña de acceso o password de administradores de sistemas operativos, equipos de comunicación, bases de datos o de sistemas de información deberán tener claves de acceso robustas y de largo en lo posible superior a las de un usuario normal.

12. Queda prohibido el cambio de contraseñas o password de acceso en los equipos portátiles y/o estaciones de trabajo, salvo que se trate de equipamiento propio del usuario.

ii. De los límite a intentos fallidos de ingreso de password.

a) Se limitará la cantidad de veces en que un usuario pueda ingresar consecutivamente su clave de acceso en forma errónea a la red, con el fin de evitar ingresos indebidos o no autorizados. Estos quedan establecidos en 5 intentos fallidos.

b) Las cuentas se deshabilitarán después de ocurridos el número máximo de intentos fallidos (5 veces), activando un bloqueo de la cuenta por 30 minutos.

c) El personal de soporte informático será el responsable de activar nuevamente la cuenta, previa verificación de la identidad del usuario.

d) En el caso de usuarios externos, sólo podrá ser reactivado el acceso por consentimiento del Director del Área que autorizó al momento de crear la cuenta.

iii. Del Almacenamiento de las Contraseñas o password.

a) Estas no deberán estar incorporadas en el o los códigos fuentes (programas fuentes, procedimientos y/o script) de los sistemas de información.

b) No se deberán mantener listados de password en archivos planos o cualquier otro tipo de archivo que sea de fácil acceso.

c) Las password de usuarios y administradores de sistemas de información (aplicaciones y/o bases de datos), deberán dejarlas en un sobre cerrado indicando en su interior la User Name, password y sistema o módulo a la cual da acceso. Ésta deberá ser entregada al Director Nacional de TI, quien será el responsable de mandarlas a la custodia de una bóveda o caja fuerte en caso de ser requeridos ante una contingencia.

d) Cada sobre en su parte externa deberá registrar el nombre del usuario, nombre de departamento, nombre del aplicativo o máquina más la fecha de entrega.

Copia no controlada

e) Cada vez que los administradores de sistemas de información (Aplicaciones y/o Bases de Datos) o de TI cambien sus password, deberán proceder a realizar la entrega del sobre a la Dirección Nacional de TI.

f) Será responsabilidad del Director Nacional de TI o quién él designe el hacer el reemplazo de los sobres de cuentas administradoras en la bóveda o caja fuerte de la institución.

iv. De las Password en dispositivos de Red.

a) Todos los dispositivos de red configurables (routers, firewalls, switch y otros elementos de conectividad administrables) deben tener password únicas como mecanismo de control de acceso.

b) Cada dispositivo debe tener su propia password de acceso para evitar el compromiso masivo en caso de ataque a los sistemas de comunicación. Si éstos no poseen password de acceso se debe impedir su administración remota, permitiendo la intervención sólo a personal autorizado y en forma directa (local).

c) El catastro de las password de red, debe ser creado y administrado por la Dirección de Plataformas y Servicios TI.

d) Además deberá existir una copia escrita de las password en un sobre cerrado y custodiado por el Director Nacional de TI.

b. Vulnerabilidades detectadas

a) Frente a la evidencia de un compromiso del sistema de uso indebido de las cuentas, todas las password deberán ser reemplazadas de forma inmediata.

b) Los usuarios o administradores deben informar cualquier evento anómalo o vulnerabilidad que detecten durante la operación de los sistemas a sus superiores y la administración del departamento de informática.

c) La completa eliminación de vulnerabilidades en este ámbito deberá ser prioritaria dentro de las funciones del personal encargado de la seguridad de la información.

Copia no controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

Título 13. Del Control de Acceso.

Esta sección define estándares mínimos necesarios para mantener un control eficaz del acceso a los datos y servicios de información y para cumplir con esto la Dirección Nacional de TI ha definido las siguientes políticas relacionadas con el control de acceso.

a) Del control de acceso local a la red

a. Dado el carácter unipersonal del acceso a la Red, la Dirección Nacional de TI, por medio del Oficial de Seguridad, verificará el uso responsable y seguro de la misma, cuando lo estime apropiado

b. El Oficial de Seguridad deberá notificar a la Dirección Nacional de TI cualquier anomalía detectada en el acceso a los servicios informáticos.

c. El Oficial de Seguridad realizará, en forma trimestral, revisiones de Seguridad a nivel de cuentas, tanto de aplicativos, bases de datos y red, en cuando a su contenido, considerando evaluación de cuentas genéricas o compartidas, cuentas administradoras, accesos remotos, inactividad de cuentas, bloqueo de cuentas y existencia de personal finiquitado y los niveles de aprobación que estas tuvieron. Esta revisión deberá quedar plasmada en un Informe.

d. Solo en los casos correspondientes a las Bibliotecas de la Institución, que prestan apoyo académico a los alumnos, se les estará permitido tener un equipo para dos usuarios, por motivos de turnos, debiendo cada uno de éstos ingresar a la red a través del Active Directory, con su username y pasword correspondiente, utilizando el menú "Cambiar de Usuario".

e. El acceso a las redes de datos, por parte del alumnado, será siempre para uso de actividades docentes y a través de accesos regulados y segregados de las redes de uso administrativo.

f. Es responsabilidad del personal de Plataformas la administración y registro de las personas que tienen autorización para el uso del administrador de tareas "job schudler" o tareas programadas en los servidores.

g. El personal del Área de Seguridad de TI o quienes las autoridades de la institución determinen, tendrán la facultad de acceder a cualquier equipo computacional, ya sea en forma presencial o en forma remota para auditar el cumplimiento de las

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

normas de seguridad internas, sin requerir autorización ni aviso previo al usuario asignado.

b) Del control de acceso remoto a la red

a. Todo acceso remoto debe ser solicitado por la Vicerrectoría o Dirección a la cual pertenece el usuario que requiere el acceso, por medio del Formulario de Solicitud de Creación y Modificación de Usuarios (Anexo I).

b. Para el caso especial de los servicios de conexión VPN (Virtual Private Network - Red privada virtual), éstos son restringidos, y su otorgamiento y uso deberán ser autorizados y documentados por el Director de Plataformas y Servicios TI exclusivamente, previa solicitud de la jefatura de quien la requiere.

c. El personal de Redes y Comunicaciones es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles, previa autorización del Director de Plataforma y Servicios TI y en su ausencia al Director Nacional de TI.

d. El usuario de Acceso Remoto deberá dar cumplimiento a las normas establecidas y en concordancia con los lineamientos generales de uso y restricciones de Internet.

e. Toda cuenta genérica con acceso remoto deberá estar asociada a una persona que se responsabilice de su uso.

c) Del acceso a los sistemas administrativos o de Información

a. Deberá restringirse el acceso a las identificaciones de usuario pre-configuradas en fábrica y suministradas con la aplicación, o a las que involucren súper usuarios. Para ello deberán desactivarse dichas identificaciones o se deberán cambiar las contraseñas.

b. Toda cuenta que tenga acceso a los sistemas administrativos o de información deberá estar autorizado por la correspondiente unidad de negocio a la cual pertenece o prestará servicios el usuario en creación.

c. El personal de Informática no deberá tener acceso a los aplicativos que se encuentran en ambiente productivo, salvo expresa autorización de la unidad de negocio correspondiente, y que sea exclusivamente por un acontecimiento de emergencia y por un plazo determinado de tiempo.

Copia no controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

d. La cuenta del administrador y sus accesos deberá ser aprobado por el titular del activo de información y por el titular del proceso, si es aplicable, y sólo deberá otorgarse a personas que estén conciente de estas políticas.

e. Los administradores deberán firmar un acuerdo por el que se comprometen a cumplir todas las políticas, los procedimientos y las normas aplicables, incluso cualquier ley o reglamento local, estatal y federal aplicable en nuestro país.

f. Las personas que tengan acceso privilegiado deberán tomar las precauciones necesarias para proteger la confidencialidad de la información usada en el ejercicio de sus funciones.

g. Los accesos directos a configuraciones y funciones de la base de datos deberán ser restringidas solo al DBA (interno o por proveedor del servicio).

h. Los accesos de los usuarios deberán otorgarse de acuerdo a la función realizada dentro de la institución, y deberá quedar establecida mediante una matriz de perfiles y autorizada por la unidad de negocio correspondiente al usuario.

i. Toda cuenta de usuario deberán estar restringidas de accesos directos a las bases de datos y a las tablas donde se almacenan las transacciones.

j. Los servidores de bases de datos son dedicados, por lo que se prohíben los accesos de cualquier usuario no certificado y validado por el administrador de base de datos y la unidad de negocio respectiva.

k. En caso que se requiera que usuarios de empresas externas requieran accesos a los sistemas administrativos o de información, se deberá aplicar el Procedimiento de Administración de Usuario, por tanto se deberá contar con la misma documentación de solicitud y de aprobación.

l. Los privilegios de acceso a las diferentes funcionalidades de los sistemas de información se asignarán a través de perfiles de usuario, no estando permitida la asignación de privilegios en forma directa a los usuarios.

m. Toda solicitud de creación, modificación y eliminación de usuarios, así como las solicitudes de creación o modificación de perfiles en los sistemas que abarca el presente instructivo deberán ser respaldadas con la documentación que se señala en cada uno de los procedimientos.

n. Semestralmente el Dueño de Procesos críticos y el Área de Seguridad de TI realizarán una revisión y validación de los accesos otorgados mediante perfiles.

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

Título 14. Monitoreo

El objetivo de esta sección es contar con herramientas que permitan medir la efectividad de los controles existentes, que sean de utilidad para la detección de vulnerabilidades o fallas en los controles implementados y en el registro de información de utilidad en investigaciones y/o análisis de situaciones particulares.

De acuerdo a lo anterior, el Área de Seguridad de TI, en conjunto con los dueños de los sistemas de AIEP, deberá implementar registros de actividad con el objeto de medir la efectividad de los controles implementados, considerando una adecuada protección de los sistemas y plataformas tecnológicas existentes.

Dado esto la Dirección Nacional de TI ha definido las siguientes políticas.

i. De las actividades de monitoreo

a) La Dirección Nacional de TI podrá realizar revisiones sorpresivas a las actividades realizadas en su área, con el fin de evaluar la efectividad y calidad de éstas.

b) La Dirección Nacional de TI, deberá monitorear los servicios de las Áreas de TI (Administración, Soporte, Plataformas/Seguridad, Comunicaciones y Redes), a modo de evaluar si éstos se realizan bajo las normas y políticas establecidas.

c) La Dirección Nacional de TI podrá realizar entrevistas al azar a los usuarios a modo de obtener el grado de satisfacción de los usuarios con respecto a cualquier servicio tecnológico.

d) La Dirección Nacional de TI deberá revisar cada uno de los informes de Auditoría (Externa/Interna) concerniente a sus áreas, a modo de evaluar y aplicar mejoras.

e) La Dirección Nacional de TI deberá exigir informes de monitoreo a sus proveedores cuando el servicio se encuentra externalizado.

f) La Dirección Nacional de TI podrá optar a contratar empresas externas para un monitoreo al azar de los actuales niveles de servicio.

g) Cada una de las áreas que componen la Dirección Nacional de TI deberá registrar y reportar de inmediato cualquier anomalía o vulnerabilidad a la seguridad de los servicios ofrecidos a la Dirección correspondiente y a la Dirección Nacional de TI.

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

h) Cada una de las áreas tienen la responsabilidad de tabular las anomalías o problemas detectados y clasificarlos para obtener estadísticas de fallas y/o problemas y poder aplicar mejoras a los servicios.

i) Cualquier solicitud de seguimiento de cuentas o de actividades realizadas por los usuarios deberá ser solicitada formalmente al Director Nacional de TI por la Vicerrectoría correspondiente al usuario en revisión.

ii. De la revisión de Log's

a) El personal de Plataformas y Seguridad, deberá revisar periódicamente los log's de auditoría de los servidores residentes en AIEP con el objeto de detectar anomalías y realizar un seguimiento de éstas.

b) En el caso de que se presentaran situaciones anormales o fuera de lo común en cualquiera de los log revisados, se deberá reportar a la Dirección de Plataformas y Servicios TI, al Área de Seguridad y a la Dirección Nacional de TI, a modo de determinar acciones a seguir.

c) Toda anomalía o falla detectada en los log deberá quedar registrada en la bitácora correspondiente.

Copia no controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

Título 15. De la Seguridad en Redes

El propósito de este módulo es señalar algunos requisitos de seguridad y control para la protección de las redes de comunicación y su interconexión con otras redes externas sean éstas de clientes, proveedores, entidades fiscalizadoras u otras.

Estas deben contemplar mecanismos de seguridad lógica y física que resguarden los activos de información de accesos no autorizados, tanto de la red interna, como de redes externas.

Las redes instaladas en AIEP deben contemplar un adecuado nivel de controles que garanticen los niveles de servicio definidos por la compañía y garanticen la disponibilidad, integridad y confidencialidad de la información que transporta.

Bajo este contexto la empresa ha definido las siguientes medidas de seguridad:

i. Principios de Seguridad en redes.

a) Todos los recursos físicos y lógicos de la red son de responsabilidad de la Dirección Nacional de TI, específicamente del Director de Plataformas y Servicios TI, así como también su custodia y protección.

b) Todos los recursos de la red deben estar protegidos y controlados adecuadamente por personal competente del ámbito informático o en su defecto por el o los proveedores contratados para estos efectos.

c) Sólo se utilizarán equipos aprobados y certificados por los proveedores.

d) Los proveedores de servicios de red deben estar aprobados desde el punto de vista de seguridad y niveles de servicios (SLA).

e) Los estándares y los controles básicos para asegurar los equipos de la red deben ser documentados e implementados formalmente.

f) Cada componente que forma parte de la red debe ser testeado antes de ingresar al ambiente de producción.

g) Cada diseño de red deberá quedar documentada por medio de planos, esquemas de comunicación y/o diagramas de red, claramente identificados.

h) Todos los componentes configurables de la red deberán contar con la documentación actualizada de su configuración.

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

i) Se realizarán o solicitarán a los proveedores las pruebas y revisiones de seguridad debidamente programadas, tales como:

- Búsqueda de equipos con su interfaz en modo promiscuo (técnicas usadas por los hackers para escuchar tráfico de red de terceros)
- Hacer un port scanning de todos los puertos de todas las IP's de los diferentes segmento de red utilizado por AIEP.

j) Todos los componentes de la red deben formar parte del inventario de Tecnología y estar debidamente rotulados.

k) Deberán estar identificados y documentados formalmente las responsabilidades que permitan implementar y cumplir con los principios de la seguridad de la red.

l) Se deberá garantizar y monitorear que por la red fluye sólo tráfico autorizado.

m) Se debe mantener un registro actualizado de los eventos de fallas o contingencias ocurridas.

n) Las actualizaciones o instalación de parches provistos por los proveedores deberá quedar configurado de modo tal que solo sea notificado, sin descargas ni instalaciones automáticas.

ii. Aseguramiento y protección contra amenazas externas e internas

a) Debe existir a lo menos un firewalls interno y externo para establecer un perímetro de defensa de seguridad sobre los recursos de la institución.

b) Debe existir a lo menos un IDS en la red LAN que permita detectar la intromisión de intrusos.

c) Las conexiones remotas y/o VPN se concederán de acuerdo a las políticas y procedimientos establecidos.

d) Todas las VPN deben estar encriptadas y autorizadas por el Jefe de Redes y Comunicaciones y una Vicerrectoría o Director como unidad usuaria.

e) La disponibilidad de la red, su rendimiento y capacidad estarán monitoreados para garantizar que la red proveerá un servicio adecuado al negocio.

Copia no controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

f) Cada componente de la red debe contar con medidas de seguridad tanto física como lógicas para su protección.

g) Todo el equipamiento de la red así como también el cableado existente debe estar debidamente rotulado y certificado.

h) Cada elemento crítico de la red debe contar con un plan de recuperación en caso de contingencia, el cual deberá estar debidamente documentado, revisado y probado periódicamente.

Copia no controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

Título 15: De los Servicios de Internet

El Objetivo principal de esta sección es establecer criterios básicos orientados a asegurar la disponibilidad, confiabilidad e integridad de la información existente o que viaja a través de Internet.

Regular el uso del Servicio para que sea utilizado de una manera apropiada y no pueda ser considerado como un uso prohibido, quedando afecto a sanciones por parte de la Institución.

i. Del World Wide Web (WWW)

a) La Dirección Nacional de TI es responsable de instalar y administrar el o los servidor(es) de Internet (WWW). Es decir, sólo se permiten servidores de páginas autorizados por la Dirección Nacional de TI y Autoridades Institucionales.

b) Los accesos a Internet serán otorgados en base a solicitudes por una vecerrectoría o director de una unidad de negocio.

c) La Intranet Institucional, así como las especificaciones para el acceso a este servicio, es responsabilidad exclusiva de la Dirección Nacional de TI.

ii. De las prohibiciones en los Sitios Web

a) Cometer o involucrarse en una violación de la ley, el orden o regulación (incluyendo el de un país extranjero), código de conducta obligatorio, o un código voluntario de conducta que han acordado cumplir

b) Utilizar este medio para causar daños a propiedades o personas mediante el acoso, amenazas o acecho.

c) Utilizar este servicio para incitar a la discriminación, el odio o la violencia hacia una persona o grupo, por ejemplo debido a su raza, religión, sexo o nacionalidad.

d) Esta prohibido el envío, la visualización, el acceso, la puesta a disposición, publicar, distribuir o estar involucrado con material que sea obsceno, pornográfico, difamatorio, o que podría ser considerado por otra persona como ofensivo o abusivos. Así como también su almacenamiento en cualquiera de los recursos informáticos existentes en AIEP.

Copia controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

e) Participar en cualquiera actividad engañosa o falsa, o realizar prácticas de comercialización o promoción de algún sistema de pirámide ilegal o juegos de azar ilegales.

f) Infringir sobre los derechos de cualquier persona, incluyendo pero no limitado a derechos de autor, marca registrada, secreto comercial, patente u otra propiedad u otros derechos de propiedad intelectual o derechos morales, o publicar información confidencial de cualquier persona, sea esta o no de la Institución.

g) Interferir con el correcto funcionamiento de la red, servicios o sistemas operados por AIEP o por un proveedor que da servicios a la Institución.

h) Utilizar los Servicios, o intentar de utilizar los Servicios o permitir que un tercero utilice los Servicios para enviar mensajeria del tipo SPAM.

i) Usar o tratar de usar los Servicios o permitir a un tercero utilizar los Servicios para el acceso a los Sistemas, Redes o datos (en particular mediante la retransmisión abierta, el sondeo de puertos y la utilización de analizadores de paquetes), sin consentimiento de la Dirección Nacional de TI.

j) Usar el servicio de suplantación de identidad en cualquier forma o tratar de usar los servicios o permitir a un tercero utilizar los Servicios para crear, enviar, recibir o alterar de cualquier forma y por cualquier medio (incluyendo suplantación de identidad, phishing y uso de la tercera parte de servidores de correo), el contenido de un mensaje electrónico con el propósito de esconder, ocultar o eliminar la fuente del mensaje.

k) Utilizar o de intentar utilizar el Servicio en relación con cualquier programa (incluyendo troyanos virus, gusano, cancelbot, Bomba de Tiempo, etc.), que este diseñado para proporcionar o permitir cualquier forma de control no autorizado a modo de resultar un efecto adverso en un sistema operativo, en la red de datos, o en los aplicativos. (El cancelbot automáticamente busca y elimina anuncios de masas).

l) Desfigurar sitios web sin el permiso del propietario; realizar sondeo de los dispositivos en Internet con la intención de buscar la identificación de las debilidades de seguridad en estos dispositivos.

m) Interferir con el servicio a cualquier usuario, host, sistema o red con bombardeo de correo, flooding, intentos deliberados de sobrecargar un sistema o red y los ataques de difusión y ataques de denegación de servicio.

n) Hacer descarga de software y/o archivos con restricciones de derechos de autor desde Internet.

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

iii. Del uso del correo electrónico

a) La Dirección Nacional de TI es la encargada de la creación de cuentas de correo electrónico institucionales

b) La Dirección Nacional de TI deberá contar con los dominios que sean necesarios para la administración de cuentas de correo del personal de la institución.

c) Las cuentas de correo deberán ser solicitadas por medio del formulario "Solicitud de Creación-Modificación de Usuarios" (Anexo I) y deberá seguir el mismo mecanismo de aprobación que la creación de una cuenta de usuario.

d) Todo e-mail enviado masivamente desde el servidor de correo de la institución deberá ser autorizado por el jefe del área que hace el envío, y su procesamiento será realizado por la Dirección Nacional de TI.

e) Todo comunicado, notificación o solicitud de servicios o requerimientos deberá realizarse mediante el servicio de mensajería que ha dispuesto la institución, por lo que no se permitirá el uso de correo electrónico personales.

Copia no controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

Título 16. De la Continuidad de la Operación

1. Cada una de las diferentes áreas de la institución deberán de emitir y documentar los planes de contingencia que correspondan a las actividades críticas que realicen.

2. La Dirección Nacional de TI deberá contar con planes de recuperación que permita levantar los servicios más críticos de la institución ante eventos de emergencia o catástrofe.

3. La Dirección Nacional de TI deberá solicitar a sus proveedores, por medio de contratos (SLA, niveles de servicio) el aseguramiento y la continuidad de sus servicios que se encuentran externalizados ante un evento de contingencia o catástrofe.

Título 17. Excepciones a la Política.

Cualquier excepción a las definiciones descritas en este documento, deberá contar con la aprobación explicita, a través de correo electrónico, del Director Nacional de TI, En este correo se especificará la política que se excepcionará, indicando además el alcance y tiempo de vigencia de esta.

4. Requisitos y documentación

- Reglamento Interno de Orden, Higiene y Seguridad

5. Control de Cambios.

Ver.	Modificaciones del Documento.	Fecha
1	Edición de Lanzamiento.	05/04/2010
2	Modificación y agregado de procesos en el presente procedimiento. Se insertaron nuevos párrafos, para corregir procesos, y palabras para complementar ideas en los textos.	15/09/2010
3	Se adecuan e insertan nuevas políticas, se cambia estructura del documento y se aplica nuevo formato.	07/12/2010
4	Se actualizan los cargos y se actualizan definiciones a partir de cambios tecnológicos.	24/04/2015

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.

5	Se incluye Titulo 17, que corresponde al tratamiento de las excepciones.	09/03/2016

Copia no controlada

El presente documento y referencias en el mismo (salvo que se indique lo contrario) se consideran como parte del Sistema de Gestión de Calidad únicamente en formato digital y disponible en la plataforma documental de ISOTools del Instituto Profesional AIEP. Toda copia que se genere adicional se considera "no controlada" y sólo para estudio ya que no será parte del SGC.