Política de Seguridad de la Información

AGTEC

Pol01

Soluciones informáticas

Control de Cambios

Historia del documento			
Nombre del documento	Política de Seguridad de la Información.doc		
Preparado por	Marcelo González		
Responsable del documento	Vanessa Martínez	Fecha de Creación	10-08-2022
Aprobado por	Álvaro García	Fecha de Aprobación	17-08-2022

Control de Versiones			
Versión	Fecha de Creación	Preparada por	Descripción
V1.0	10-08-2022	Marcelo González	Políticas de seguridad

INDICE

1. Introducción

Las políticas incluidas en este documento se constituyen como parte fundamental del sistema de gestión de seguridad de Agtec Servicios Informáticos Limitada y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos. La seguridad de la información es una prioridad para las entidades y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

Para la elaboración de este documento, se tomaron como base las leyes y demás regulaciones aplicables, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

2. Objetivo

Las Políticas de Seguridad de la Información de AGtec Servicios Informáticos Ltda. tiene por fin dar a conocer las directrices de seguridad para el resguardo de los activos de información y de la infraestructura tecnológica que soporta las operaciones de AGtec Servicios Informáticos Ltda., a fin de aplicar y dar cumplimiento a las normas y leyes estipuladas que rigen la materia, emplear las mejores prácticas y los marcos referenciales como fundamento para la Gestión de la Seguridad de la Información de la empresa.

3. Alcance

Esta política debe emplearse para servir de dirección en la protección de los activos de información de la empresa. Las políticas aquí enmarcadas, deben ser cumplidas por todos los empleados y terceros relacionados que acceden a la información de AGtec Servicios Informáticos Ltda.

4. Definiciones

Para los efectos del presente documento se entienden por:

Amenaza: Es una situación o acontecimiento que pueda causar daño a los bienes informáticos; puede ser una persona, un programa malicioso o un suceso natural o de otra índole y representan los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema.

Análisis de riesgo: el proceso dirigido a determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos e implica la identificación de los bienes a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que puedan causar

Bienes informáticos: Los elementos componentes del sistema informático que deben ser protegidos en evitación de que como resultado de la materialización de una amenaza sufran algún tipo de daño.

Impacto: Es el daño producido por la materialización de una amenaza.

Riesgo: Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto negativo en la organización.

Riesgo residual: Es el riesgo remanente después de aplicados controles de seguridad para minimizarlo

Seguridad: Es usado en el sentido de minimizar los riesgos a que están sometidos los bienes informáticos hasta llevarlos a niveles adecuados.

Sistema informático: Es el conjunto de bienes informáticos de que dispone una entidad para su correcto funcionamiento y la consecución de los objetivos.

Vulnerabilidad: En un sistema informático es un punto o aspecto susceptible de ser atacado o de dañar su seguridad; representan las debilidades o aspectos falibles o atacables en el sistema informático y califican el nivel de riesgo del mismo.

5. Responsabilidades y Cumplimiento

5.1 Responsabilidades

La Gerencia de AGTEC es responsable de apoyar el proceso de implementación de las Políticas de Seguridad de la Información y asignar los recursos necesarios para su cumplimiento.

El Encargado de Seguridad de la Información es responsable durante el proceso de revisión y asesoría de cualquier actividad o asunto relacionado a la Seguridad de la Información.

El Encargado de Seguridad de la Información es responsable de verificar periódicamente el cumplimiento de las Políticas de Seguridad de la Información.

Es responsabilidad de la Gerencia, la revisión anual del presente manual, tanto por actualización y mejoras del mismo. De igual forma se debe revisar en caso que se produzcan cambios significativos en la organización.

La Gerencia es responsable de la implementación y administración de los controles técnicos aplicables a las Políticas de Seguridad de la Información.

Es responsabilidad de la unidad administrativa, dar a conocer el contenido del presente manual entre los colaboradores, así como exigirles su firma en señal de haberse efectuado la lectura y entendimiento correspondiente.

5.2 Cumplimiento

El Encargado de Seguridad de la Información es responsable de verificar periódicamente el cumplimiento de las Políticas de Seguridad de la Información.

El Encargado de Seguridad de la Información es responsable de supervisar la implementación de las Políticas de Seguridad de la Información, velar porque el personal de AGTEC dé cumplimiento y apoyar a la Gerencia cuando se requiera.

6. Política

6.1 De la Información Interna:

No Aplica para proveedor de acuerdo a los servicios efectuados.

6.2 De la Información de usuarios externos:

No Aplica para proveedor de acuerdo a los servicios efectuados.

7. Deberes del personal

Todas las personas que trabajen por y para AGTEC tendrán como deber de conocer las políticas de seguridad que se han definido.

De manera periódica se les hará recordatorios que es de su responsabilidad leer las políticas y utilizar las recomendaciones definidas.

Todas las personas podrán acceder a la última versión de este documento y descargarla de la página web de AGTEC.

8. Difusión de la política

Esta Política será difundida por el Encargado de Seguridad de la Información a través de correo o bien a través de la actualización en la web institucional.

9. Formato y mantención de las políticas

9.1 Formato de las políticas

Toda política debe tener el siguiente formato

- Introducción
- Objetivo
- Alcance
- Definiciones
- Responsabilidades y cumplimiento
- Deberes del personal
- Difusión de la política
- Formato y mantención de las políticas

Formato Texto: todo el documento debe tener el tipo de letra Arial

Tamaño:

- Para títulos debe ser tamaño 28 en la portada y los subtítulos de la portada tamaño 16
- Para los ítems de la política debe tener del tipo título 16
- Para subtitulo debe tener tipo título tamaño 14
- Texto en general tamaño 12

9.2 Mantención de la política

La mantención de la política de seguridad definida por AGTEC será revisada anualmente por el Encargado de Seguridad.

Todas las modificaciones serán presentadas a la Gerencia.

Una vez presentadas las modificaciones, la Gerencia autorizará el cambio.

El Encargado de Seguridad procederá a actualizar el documento de Política de Seguridad de la Información.

Se procederá a enviar un comunicado por correo a todos los colaboradores con la modificación realizada.

10. Políticas de Seguridad de la información

Conjunto de normas declaradas y aplicadas, cuyo objetivo es disminuir el nivel de riesgo y garantizar la revisión periódica.

10.1 Políticas y normas de seguridad de la información modelo y gestión formal de seguridad de la Información

La política de Seguridad de la Información es la forma en que AGTEC ha decidido implementar y mantener procedimientos que permitan gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información basado en la norma chilena NCH ISO 27001:2013. La implementación de esta política contribuirá significativamente a mitigar el impacto de los riesgos generados que están sometidos los activos de información tales como: documentos en papel y digitales; bases de datos; enlaces de terceros; datacenter; soporte de almacenamientos; elementos de infraestructura; procesos y personas.

10.2 Registro de aceptación y/o conformidad de Políticas de Seguridad

Esta política se encarga de velar por el mantenimiento de las evidencias de las acciones y actividades que puedan afectar los activos de información

AGTEC ha acordado que la política deberá contener:

- Responsabilidad: Definir quién y cuando llevará a cabo las auditorías a los sistemas y actividades relacionadas a la gestión de activos de información, así como informar los resultados de las auditorías.

- Almacenamiento de registros: La política debe incluir el almacenamiento de los registros de las copias de seguridad.

- Normatividad: La política de auditoría debe velar porque las mismas sean realizadas acorde a la norma vigente.

- Garantía cumplimiento: La política debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la AGTEC; así como recomendar las deficiencias detectadas.

- Periodicidad: La política debe determinar la revisión periódica de los niveles de riesgos a los cuales está expuesta AGTEC,

10.3 Periodo de aplicación y alcance de Ethical Hacking y alcance

No Aplica para proveedor de acuerdo a los servicios efectuados.

10.4 Políticas de ciberseguridad o lineamiento de ciberseguridad

AGTEC considera que la información y los sistemas asociados son activos críticos que deben ser protegidos para asegurar el correcto funcionamiento de la empresa.

La Política de Ciberseguridad está orientada a gestionar eficazmente la seguridad de la información tratada por los sistemas informáticos de la empresa, así como los activos que participan en sus procesos.

Esta Política tiene como objetivo garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, y cumplir con las Leyes y Reglamentaciones vigentes en cada momento, manteniendo un equilibrio entre los niveles de riesgo y un uso eficiente de los recursos, con criterios de proporcionalidad.

Esta política de ciberseguridad es de aplicación a todos los colaboradores, administrativos y gerentes de AGTEC.

10.5 Métodos o herramientas para las pruebas de ciberseguridad

AGTEC ha definido al menos el uso de algunas herramientas tendientes a disminuir alguna posible pérdida de información.

1. Software antivirus.

Se instalará un antivirus gratuito y confiable en todos los computadores conectados a la red, personales y corporativos deben contar con un antivirus gratuito y confiable.

Estos programas permitirán contar con medidas de protección efectivas ante la detección de malware u otros elementos maliciosos, por medio de ofrecer la posibilidad de eliminar las posibles amenazas o poner al dispositivo en estado de “cuarentena”.

2. Firewall perimetral de red.

Adicionalmente, se proveerá de firewall perimetral de red lo que permitirá: escanear los paquetes que se transmite por la red, permitiéndoles o bloquearlos según las reglas definidas por un administrador.

3. Servidor proxy.

Se dispondrá de un servidor proxy para bloquear sitios web que se estimen como peligrosos o prohibidos dentro del ambiente laboral.

Por otro lado, permite establecer un sistema de autentificación, el cual limita el acceso a la red externa, permitiendo contar con registros sobre sitios, visitas, entre otros datos.

4. Escáner de vulnerabilidades.

Se instalará un software para el escaneo de vulnerabilidades que se encargará de detectar, analizar y gestionar los puntos débiles del sistema.

Gracias a esta plataforma, se puede mantener controlada la exposición de los recursos empresariales a las amenazas de ciberseguridad y sus posibles consecuencias. Además, permite alertar en tiempo real, lo que ayuda a la solución de problemas de forma oportuna y sin comprometer la continuidad del negocio.

10.6 En el organigrama de cargos existe organismo o encargado de la seguridad de información

AGTEC ha definido un Encargado de Seguridad que será el responsable de la seguridad de la información de la empresa y velar por el cumplimiento de las mismas.

10.7 Certificación en seguridad de la información u otra

No Aplica para proveedor de acuerdo a los servicios efectuados.

10.8 Informar tipos de versiones de la política, autorizaciones y creaciones de estas mismas.

AGTEC anualmente actualizará este documento de políticas de seguridad de ser necesario. El Encargado de Seguridad será el responsable de la aprobación para la introducción de nuevos sistemas informáticos, actualizaciones y nuevas versiones, previa verificación de su correspondencia con el sistema de seguridad establecido y el cumplimiento de los criterios de seguridad apropiados.

11. Capacitación y Sensibilización en Seguridad

Ámbito alineado con las políticas de seguridad de la información y la participación activa de colaboradores de la organización con el fin de lograr el nivel de cumplimiento adecuado de los lineamientos y requisitos de seguridad de la información.

11.1 Métodos de difusión, educación o formalización en seguridad de la información

El personal de AGTEC deberá recibir información y herramientas que les permitan mejorar su conocimiento y entendimiento respecto a la Seguridad de la Información, así como a las posibles vulnerabilidades, medidas de resguardo y prevención contempladas por la empresa.

Objetivo:

Capacitar y desarrollar el nivel de conciencia del personal de la empresa sobre cuáles son los riesgos de seguridad de la información, así como las acciones preventivas sean parte de las actividades laborales regulares.

Criterios para la implementación de la política:

- La información confidencial puede ser ilegalmente adquirida, dañada o modificada debido a desconocimiento en materia de Seguridad de la Información.

- La información confidencial puede ser comprometida por el personal si asume sus responsabilidades sin haber recibido entrenamiento específico sobre Seguridad de la Información.

Responsabilidades:

- La Gerencia de AGTEC serán los responsables de establecer los requerimientos y planificar las actividades correspondientes.

Referencias

- ISO 27002: 7.2.2 Concientización, educación y capacitación en seguridad de la información.

11.2 Plan de capacitación, difusión en materias de seguridad y frecuencia de esta según rotación de colaboradores

AGTEC también asegurará que el personal tome conciencia de la necesidad e importancia de las actividades de seguridad informática que le corresponde realizar, mediante un plan de capacitación.

Las actividades de formación y sensibilización incluirán:

1. Concientizar a los colaboradores de la importancia de la información que estén utilizando tanto de la empresa como de sus clientes.
2. Dar a conocer de manera periódica la divulgación, conocimiento y comprensión de las políticas de seguridad que se implementen en AGTEC.
3. Capacitar a los colaboradores en las medidas y procedimientos que se vayan a implantar dentro de AGTEC.

El cumplimiento de este plan contribuirá al proceso de mejora continua de AGTEC y será actualizado según se vaya ejecutando. Algunos aspectos que se consideran son los siguientes:

1. La implementación de mediano y largo plazo de aquellos aspectos que así lo exijan para alcanzar un mayor nivel de seguridad, como por ejemplo la introducción de medios técnicos de seguridad, modificación de locales, etc.

2. La preparación y capacitación del personal en materia de seguridad informática, según su participación en el sistema diseñado, ya sea a través de cursos específicos, mediante la impartición de materias relacionadas con el tema y con acciones de divulgación.

11.3 Resumen o reporte de efectividad de capacitaciones de seguridad

AGTEC publicará anualmente un resumen de las actividades de capacitación realizadas en el año, en relación a las políticas de seguridad que se ha fijado. La idea es poder llevar un registro de cuántos de los colaboradores han realizado el curso que se dispondrá para dar a conocer las políticas y cuáles fueron los resultados obtenidos. Este reporte resumirá inicialmente el cumplimiento de divulgación de las mismas.

11.4 Plan de capacitación formal para el personal clave de la organización respecto de la política, modelo de continuidad de negocio, y los planes de continuidad/recuperación implementados

AGTEC realizará una capacitación a su equipo clave respecto de las políticas de seguridad definidas para el resguardo de la información, así como también de los procedimientos que serán realizados para dar continuidad al negocio en caso de pérdida de información sensible para el negocio y como a través de los procedimientos, la información será recuperada.

Esta capacitación estará basada en el documento y la versión vigente de Política de Seguridad de AGTEC. A través de la capacitación, será una instancia que permitirá validar la política definida y de ser necesaria, actualizarla con nuevos mecanismos o considerandos que a la fecha hayan sido incorporados.

11.5 Instrucción especial (capacitación) a colaboradores externos que trabajen en dependencias del Banco y utilicen permisos especiales en plataformas o sistemas banco

No Aplica para proveedor de acuerdo a los servicios efectuados.

11.6 Plan anual sobre reforzamiento orientado a los incidentes de seguridad como capacitación inicial y conocimiento continuo

AGTEC considera no sólo realizar una capacitación anual para evitar incidentes de seguridad, sino se compromete a estar enviando información (vía email) de como deberían actuar nuestros colaboradores para recordar que cosas deben realizar en términos de seguridad, que abarcará desde cambios de contraseña, hasta guardar información sensible en las rutas definidas en la nube de Google.

12. Gestión de Activos:

Este ítem de revisión permite obtener información respecto a la trayectoria física y lógica de los bienes del proveedor.

12.1 Políticas de clasificación de la Información

Objetivo: asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.

Control: Los dueños de la información deben clasificar los niveles de sensibilidad de la misma, de acuerdo con los siguientes criterios: Crítica o Relevante. Se entenderá por “Activo Crítico” o relevante, todo aquel cuyo análisis de impacto en la integridad, disponibilidad o confidencialidad sea clasificado cómo medio o alto.

La clasificación de seguridad asignada a la información debe ser respetada por todos los colaboradores que producen, compilan o modifican información, quienes deberán cumplir con los controles y medidas de seguridad que se definan.

12.2 Procedimiento para el manejo y protección de activos

Objetivo: establecer procedimientos eficaces para el manejo de los soportes de almacenamiento, de acuerdo con la clasificación de la información.

Permanentemente se debe efectuar copia de respaldo de toda la información considerada confidencial o sensible y que se encuentre contenida en los equipos del personal de AGTEC.

En especial se debe asegurar el respaldo de información cuando termine el vínculo laboral del funcionario o contractual del proveedor responsable de su generación, edición y manejo, así como cuando se vaya a dar de baja un activo tecnológico (por pérdida, daño, devolución, enajenación o donación, entre otros).

12.3 Políticas de respaldo y recuperación de la información

No Aplica para proveedor de acuerdo a los servicios efectuados.

12.4 Políticas de respaldo contempla la generación de un backup interno y externo de seguridad

La experiencia nos indica que, si bien se pueden aplicar las mejores medidas preventivas y defensivas para evitar incidentes destructivos, de la información considerada crítica o relevante para AGTEC o bien para nuestros clientes.

Para este caso, contar con una adecuada estrategia de respaldo de la información relevante será un factor clave para una recuperación rápida y sin pérdida de información.

El respaldo de información es la copia de los datos importantes de un dispositivo primario en uno o varios dispositivos secundarios, ello para que en caso de que el primer dispositivo sufra una avería electromecánica o un error en su estructura lógica, sea posible contar con la mayor parte de la información necesaria para continuar con las actividades rutinarias y evitar la pérdida generalizada de datos.

Por lo tanto, existirán medios de backup internos en discos definidos para este propósito o bien en un medio externo como la nube de Google.

12.5 Indique medidas de protección y de seguridad con las que cuentan los recintos donde se resguardan los respaldos.

Se definirán más de un mecanismo de respaldo para evitar pérdidas de información debido a fallos en los dispositivos secundarios, robos o actos maliciosos, para existirán varios medios de backup internos como externos como la nube de Google, con usuarios y claves asignadas para estos fines.

13. Control de Acceso:

Está relacionado principalmente con el acceso de los usuarios a la red interna de nuestro proveedor y la información a la que podría acceder de acuerdo los controles de acceso.

13.1 Políticas de control de acceso

A cada empleado se le otorgará un usuario con su respectiva contraseña, para poder acceder a sus correos y la red, o bien de cualquier otra forma de acceso autorizado, siendo cado uno el responsable de su uso y protección. Cada usuario será único e intransferible.

Criterios:

- Al momento del ingreso de cada nuevo colaborador se la indicará su responsabilidad sobre su usuario y clave y los criterios que deberá utilizar al momento de crear una contraseña.
- De forma periódica AGTEC enviará comunicados de concientización para la no divulgación de las credenciales de conexión a la Empresa y recordarles que deben cambiar sus claves.

13.2 Políticas sobre el uso de los servicios de red

Para poder realizar un acceso remoto a la red y/o a los recursos de AGTEC será mediante usuarios autorizados, encriptada a través de la red y con privilegios restringidos.

AGTEC permitirá el acceso a la red, por medios de acceso seguros desde y hacia fuentes externas acordes con el valor de la información que estará expuesta a través de la red. Para ello, de ser necesarios, se dispondrá de mecanismos, tales como la Red Privada Virtual o Virtual Private Network.

Criterios para la implementación de la política:

- Asegurar el acceso a la red interna de AGTEC al personal autorizado y autenticado por los mecanismos de control.
- Asegurar la confidencialidad de la información mediante técnicas de cifrado entre los usuarios remotos y la red interna.

Responsabilidades:

- Todos los Gerentes y/o Supervisores de AGTEC, deberán asegurar que el personal bajo su cargo, reciba la debida autorización de acceso remoto a la red de la empresa y darle a conocer la política, así como instruirlos en el cumplimiento de ella.
- Todos los usuarios que tengan asignado un equipo de computación tendrán que respetar la política de seguridad.
- Será de responsabilidad de la Gerencia proporcionar canales de comunicación seguros.

13.3 Procesos de altas, bajas y modificaciones (ABM) de cuentas en sistemas y/o aplicativos.

Con el fin de poder llevar la administración usuarios y control de accesos a los sistemas y/o red de AGTEC hemos definido una serie de pautas:

Objetivos:

- Evitar duplicación de usuarios.
- Mantener una nomenclatura única para designar los ID de cada usuario/colaborador perteneciente a AGTEC.

Criterio de Alta:

1. El usuario se creará con la primera letra del primer y segundo nombre concatenando el apellido y en caso que contenga un segundo apellido se deberá colocar la primera letra del mismo para finalizar.

Ejemplo:

Un Colaborador que posee el siguiente nombre "Juan Carlos Pérez García"

El usuario debería crearse de la siguiente manera: "JCPEREZG".

2. En el caso de que ya exista el ID de un usuario, se considera agregar la segunda letra del primer nombre.

Ejemplo:

Un Colaborador que posee el siguiente nombre "Juan Carlos Pérez García"

El usuario debería crearse de la siguiente manera: "JUCPEREZG".

3. En el caso de que ya exista el ID de usuario que se configura, se debe continuar agregando letras del primer nombre hasta que se complete el mismo.

Ejemplo de cómo agregar letras para crear ID de usuario:

a. Un Colaborador que posee el siguiente nombre "Juan Carlos Pérez García

JCPEREZG JUCPEREZG JUACPEREZG JUANCPEREZG

4. Una vez que se agoten las posibilidades con las letras del primer nombre y validando como resultado que ya existe un usuario con el mismo ID, se deberá continuar utilizando las letras consecutivas a la primera del segundo nombre hasta completarlo.

5. En caso que las posibilidades de ID ya hayan sido utilizadas, se procederá a completar con letras del segundo apellido.

6. En caso que todas las posibilidades de ID de usuarios anteriormente conformados ya existan, se utilizará primero el nombre completo y luego ir agregando letras del segundo nombre.

7. Así y todo, si el ID de usuarios anteriormente conformados ya exista, es decir, que se haya utilizado el primer nombre completo y el segundo nombre también, se procederá a utilizar el

primer y segundo nombre completo concatenado con el apellido e ir agregando letras del segundo apellido.

8. Finalmente, una vez creado el ID Usuario se otorgará el o los privilegios al o los sistemas de AGTEC.

Restricciones de configuración de usuarios:

- Todos los ID de usuarios se harán en mayúsculas.
- Se permitirán combinaciones con valores alfanuméricos, guion bajo y punto.
- No se podrán crear ID de usuario con espacios (ni adelante, ni atrás o en el centro).
- El largo de los ID de usuario no podrá ser mayor o igual a 3 caracteres y tendrá un máximo de hasta 30.
- Sólo se permitirá usar hasta 1 número en los ID de usuario.
- Los ID de usuario sólo podrán comenzar con letras, no con número, ni rayas, ni otro carácter.
- No permitirá dar de alta un ID de usuario que ya exista.
- Se prohibirá, que existen ID de usuario, que contengan palabras tales como: CONSULTA, CAPACITACION, PRUEBA, TEST

Baja de Usuarios

La baja de usuarios se producirá toda vez que un colaborador renuncie o sea desvinculado de AGTEC para evitar que pueda acceder al o los sistemas de empresa. Lo anterior podrá ser solicitado mediante un email enviado por el jefe directo, o bien por algún miembro de la Gerencia para darlo de baja de las distintas plataformas.

En caso de querer dar la baja de accesos, el Jefe directo deberá solicitar mediante un correo electrónico dirigido a la Gerencia o al Service Desk (service_desk@agtec.cl) la Baja de usuario en el o los Sistemas o Base Datos según corresponda, indicando la Identificación Usuario, Base de Datos o Requerimiento Usuario necesarios.

Modificación de Usuarios

En la eventualidad de requerir modificar accesos de usuarios, el jefe directo deberá solicitar mediante un correo electrónico dirigido a la Gerencia o al Service Desk (service_desk@agtec.cl) la Modificación de usuario en el o los Sistemas o Base Datos según corresponda, indicando la Identificación Usuario, Base de Datos o Requerimiento Usuario necesarios.

13.4 Controles de acceso a sistemas y aplicaciones

De acuerdo a la política definida por AGTEC se ha definido una serie de pasos tendientes a mantener y controlar el acceso a los sistemas y aplicaciones de la empresa, con el fin de proteger los activos y evitar que puedan ser accedidos por terceros.

Criterios:

Según corresponda, se definirán perfiles de usuarios sobre los distintos sistemas y aplicativos, autorizando accesos, sólo aquellos que su perfil permita.

El jefe Directo o la Gerencia, definirá el perfil de cada usuario

Si AGTEC tuviere que utilizar algún personal externo, se creará un usuario que lo determine, y se le asignará un perfil distinto a un colaborador normal para acceder a él o los sistemas y base datos.

Adicionalmente lo anterior, existirá un estricto control para aquellas cuentas genéricas y/o privilegiadas, tales como “Admin”, “Root”, entre otras.

Evidencias requeridas para validar cumplimiento

Se mantendrá un listado de perfiles de usuarios por sistema (formato Excel y en base datos de los distintos perfiles y usuarios de AGTEC).

Para efectos de auditoría y control, se llevará un registro que evidencie la fecha, quien autoriza y actualización del o los perfiles.

Se llevará el control de la eliminación de accesos para el personal desvinculado, bloqueo de cuentas para casos con licencias prolongadas, así como también información de cuentas de personal externo.

Existirá un control de todas las cuentas privilegiadas, de quien y cuando se han utilizado.

13.5 Control de ingreso seguro

Según la situación actual país, y de acuerdo a la emergencia sanitaria decretada por el Ministerio de Salud, con ocasión de la Pandemia de Coronavirus (Covid-19), AGTEC, ha preparado una

serie de recomendaciones, para aplicar en el ingreso de personas a la oficina, como una forma de seguir las indicaciones de la autoridad sanitaria, respecto del cuidado de la vida y salud de las personas.

Por políticas de la empresa, se ha definido que todos los colaboradores trabajen de manera remota, esto con el fin de disminuir al máximo la probabilidad de contagio de Covid-19, sin embargo, en caso de ser necesario que algún colaborador asista de manera presencial a las dependencias de AGTEC se han definido una serie de normas al ingreso, las que se detallan a continuación.

Normas de ingreso:

Toda vez que ingrese una persona a las dependencias de AGTEC, se deberá respetar la distancia de seguridad (física) mínima de 1,5 metros entre personas.

Todos los colaboradores o personas que ingresen a AGTEC deberán hacer uso de mascarilla, en caso de no contar con este elemento, no se le permitirá su ingreso.

Cada persona que haga ingreso a las oficinas de AGTEC será sometida a un test de control de temperatura y alcohol gel.

Toda persona externa a AGTEC que se le permita su ingreso, deberá ser controlado al ingresar, además se registrarán sus datos personales, así como registrar con quien tendrá contacto.

Control de Temperatura para el ingreso seguro a AGTEC

Caso 1

Si la persona se presentase sin mascarilla, se prohibirá el ingreso

Si la temperatura es igual o mayor a 37,8 °, presenta dificultad para respirar, se prohibirá el ingreso Y se le indicará como recomendación concurrir a servicio de urgencia para evaluación.

Caso 2

Si la persona se presentara con mascarilla y control de temperatura positivo, se permitirá el

ingreso. El control de temperatura debe ser menor a 37,8°, con lo cual se les permitirá el ingreso a las dependencias AGTEC.

La persona deberá ingresar al baño que esté disponible para el lavado de manos con agua y jabón y/o aplicación de alcohol gel.

13.6 Uso de programas utilitarios privilegiados

Entendemos que es muy importante que los colaboradores y/o cuentas de usuarios no tengan acceso a funciones privilegiadas desde sus cuentas de usuario normales, lo anterior con el fin de evitar un perjuicio para la empresa, así como también a nuestros clientes. Es por esta razón, que hemos definido como política que las cuentas de administrador tengan acceso a software de microinformática o de propósito general, como el correo electrónico, u otra aplicación definida por la organización.

Los administradores sólo tendrán cuentas estándar para correo electrónico / oficina / etc. y solo usar cuentas con privilegios cuando sean realmente necesarias, para ello deberán cumplir y acatar las políticas de seguridad de la información.

Definición de políticas:

- Controlar estricto para el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y/o controles de las aplicaciones.
- Uso limitado de programas utilitarios a sólo un número mínimo práctico de usuarios confiables y autorizados.
- Acceso limitado por tiempo para el uso de programas utilitarios
- Mantener un registrar el uso de los programas utilitarios.
- Definir, mantener y documentar los niveles de autorización para los programas utilitarios.
- Mantener actualizado o deshabilitados aquellos programas utilitarios innecesarios.
- No disponer de programas utilitarios a usuarios que tengan acceso a aplicaciones en sistemas en donde se requiera la separación de funciones y responsabilidades.

14. Seguridad Física y Ambiental:

Ámbito relacionado principalmente con las evidencias que indiquen los métodos de controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. Adicionalmente evidencias de métodos o procedimientos de protección física contra los desastres naturales, ataque maliciosos o accidentes.

14.1 Controles físicos de entrada en la organización

AGTEC ha definido una política de controles físicos tanto de los colaboradores, así como de los equipos que puedan utilizar sus colaboradores y evitar al máximo posible, perdidas de información sensible de la empresa, como la de sus clientes.

14.2 Políticas o Controles físicos de entrada en las dependencias de la organización

AGTEC cuenta con un ingreso controlado a su oficina, al que pueden acceder los colaboradores, administrativos y gerentes de la empresa.

14.3 Protección contra las amenazas externas y ambientales

AGTEC cuenta con equipos protegidos con software antivirus, firewall, entre otros mecanismos que permiten evitar amenazas y resguardar la información crítica relevante de la empresa.

14.4 Políticas de seguridad de los equipos y activos fuera de las instalaciones

Control

Deberían aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.

Guía de implantación

Todo uso fuera de las instalaciones de la organización de cualquier equipo que almacene o trate información debería ser autorizado por la dirección. Esto aplica a los equipos propiedad de la organización y a los equipos propiedad del usuario, pero utilizado en nombre de la organización.

Se deberían considerar las siguientes directrices para la protección de los equipos fuera de las instalaciones de la organización:

a) los equipos y soportes sacados de las instalaciones no se deberían dejar desatendidos en lugares públicos;

b) se deberían respetar en todo momento las instrucciones del fabricante relativas a la protección de los equipos, por ejemplo, sobre la protección contra exposiciones a campos electromagnéticos intensos;

c) se deberían determinar los controles para emplazamientos fuera de las instalaciones de la organización incluyendo el trabajo en el domicilio personal, teletrabajo y lugares de trabajo temporales, mediante una evaluación del riesgo y, cuando corresponda, aplicarse los controles convenientes, por ejemplo, archivadores que se puedan cerrar, una política de puesto de trabajo despejado, controles de acceso a los ordenadores y comunicación segura con la oficina

d) cuando el equipo fuera de las instalaciones se transfiere entre diferentes individuos o entidades externas, se debería mantener un registro que defina la cadena de custodia de los equipos incluyendo, al menos, los nombres y las organizaciones de aquellos responsables de los equipos.

Los riesgos de seguridad, por ejemplo, de daño, robo o escucha, pueden variar considerablemente según la ubicación y deberían tenerse en cuenta al determinar los controles que sean más adecuados.

Información adicional

Los equipos de tratamiento y de almacenamiento de la información comprenden todo tipo de ordenadores personales, organizadores, teléfonos móviles, tarjetas inteligentes, documentos en formato papel o en otros formatos, que se lleven al domicilio personal o fuera del lugar habitual de trabajo.

Política de dispositivos móviles

Control

Se debería adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.

Guía de implantación

Cuando se utilicen dispositivos móviles, se debería tener un cuidado especial para asegurar que no se compromete la información del negocio. La política de dispositivos móviles debería tener en cuenta los riesgos de trabajar con dispositivos móviles en entornos desprotegidos.

La política de dispositivos móviles debería considerar:

a) el registro de dispositivos móviles;

b) los requisitos para la protección física;

c) las restricciones de instalación de software;

d) los requisitos para las versiones de software de dispositivos móviles y para la aplicación de los parches y actualizaciones del software.

e) las restricciones de conexión a servicios de información;

f) los controles de acceso;

g) las técnicas criptográficas;

h) la protección ante el software malicioso (malware);

i) la inhabilitación, el borrado y bloqueo remotos;

j) las copias de respaldo;

k) la utilización de servicios y aplicaciones web.

Se debería tener cuidado con el uso de dispositivos móviles en zonas públicas, salas de reunión y otras áreas desprotegidas fuera de las instalaciones de la organización. Se debería implantar algún tipo de protección para evitar el acceso no autorizado o la revelación de la información almacenada y procesada por estos dispositivos, por ejemplo, utilizando técnicas criptográficas.

14.5 Políticas de puesto de trabajo despejado y bloqueo de pantallas

Control

Debería adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.

Guía de implantación

La política de puesto de trabajo despejado y pantalla limpia debería tener en cuenta las clasificaciones de la información, los requisitos legales y contractuales y los correspondientes riesgos y aspectos culturales de la organización. Se consideran las siguientes directrices:

a) la información de negocio sensible o crítica, por ejemplo, en papel o en soportes de almacenamiento electrónico, debería estar guardada (idealmente en una caja fuerte, armario u otro tipo de mueble de seguridad), cuando no se necesite, especialmente cuando la oficina esté vacía;

b) los ordenadores y terminales deberían quedarse apagados o protegidos mediante un mecanismo de bloqueo de pantalla y teclado controlado mediante una contraseña, dispositivo hardware o mecanismo similar de autenticación de usuario cuando estén desatendidos y deberían estar protegidos mediante claves de bloqueo, contraseñas u otros controles cuando no están en uso;

c) debería prevenirse el uso por usuarios no autorizados de fotocopias y otros dispositivos de reproducción (por ejemplo, escáneres, cámaras digitales);

d) los soportes que contengan información sensible o clasificada deberían retirarse de manera inmediata de las impresoras.

Información adicional

Una política de puesto de trabajo despejado y pantalla limpia reduce los riesgos de accesos no autorizados, pérdida o daño de la información tanto durante las horas normales de trabajo como fuera de ellas. Las cajas fuertes u otras formas de almacenamiento seguro pueden proteger la información almacenada también contra desastres tales como el fuego, un terremoto, una inundación o una explosión.

Considerar el uso de impresoras con función de código PIN, de esta manera los autores son los únicos que pueden obtener sus impresiones, y además hacerlo únicamente cuando estén delante de la impresora.

14.6 Políticas de seguridad de trabajo remoto

El acceso remoto a la red y a los recursos de la empresa será permitido sólo cuando los usuarios autorizados son autenticados, la información viaje encriptada a través de la red y los privilegios sobre la misma sean restringidos.

Objetivo:

Proporcionar medios de acceso seguros desde y hacia fuentes externas acordes con el valor de la información que estará expuesta a través de la red. Utilizando medios seguros, tales como la Red Privada Virtual o Virtual Private Network, el cual proporciona el acceso a través de las redes públicas.

Criterios para la implementación de la política:

- Asegurar el acceso a la red interna de AGTEC al personal autorizado y autenticado por los mecanismos de control.

- Asegurar la confidencialidad de los datos e información transmitidos entre los usuarios remotos y la red interna a través de técnicas de cifrado.

Alcance:

Esta política va dirigida a todos los usuarios que reciben autorización para tener acceso remoto a la red de AGTEC.

Responsabilidades:

- Todos y cada uno de los Gerentes, Coordinadores y/o Supervisores de AGTEC, deben asegurar que el personal bajo su cargo, que reciba autorización de acceso remoto a la red de la empresa, conozca y le dé cumplimiento a esta política.

- Todo usuario que tenga asignado un equipo de computación tiene responsabilidad directa en el cumplimiento de las políticas de seguridad.

- Es Responsabilidad de la Gerencia de Tecnología de la Información proporcionar canales de comunicación seguros.

14.7 Certificaciones de Datacenter, cuáles son los datacenter

No Aplica para proveedor de acuerdo a los servicios efectuados.

14.8 Ubicación o distancia que se encuentra ubicado el sitio de recuperación en relación al sitio primario de su organización

No Aplica para proveedor de acuerdo a los servicios efectuados.

14.9 Utilización de medios de almacenamiento de larga duración para el almacenamiento a largo plazo

No Aplica para proveedor de acuerdo a los servicios efectuados.

DRP Continuidad de Negocio:

Refiere a procesos de mantención y actualización periódica de pruebas DRP y las evidencias o planillas donde se demuestre el calendario anual de las pruebas DRP. Posteriormente, las planillas o registros de resultados de las ejecuciones de las pruebas DRP ejecutadas con 1 (uno), año de antelación.

14.10 Políticas, modelo o gestión formal de continuidad de negocio implementada

Política: "La información será guardada en discos con la periodicidad requerida en cada caso a fin de garantizar su restablecimiento en caso de incidentes de seguridad".

Medidas:

1. La información que se comparte en los servidores de la red se salvará en los discos habilitados al efecto, diariamente en dos versiones.

2. Las bases de datos serán salvadas en discos reescribirles en dos versiones. Diariamente se salvarán las modificaciones realizadas y mensualmente toda la información.

Procedimientos:

a) En las oficinas de AGTEC.

1. Realizar la recuperación de la información que se comparte en los servidores en dos discos numerados, alternándolos diariamente, una hora antes de concluir la jornada de trabajo. Utilizar el disco marcado con el No. 1 los días impares y con el No. 2 los días pares.

Responsable: Encargado de Seguridad

2. Anotar en el modelo de registro la fecha, la hora y el disco utilizado.

Responsable: Encargado de Seguridad

3. Verificar integridad de la información salvada.

Responsable: Encargado de Seguridad

4. Guardar el respaldo bajo llave en el archivo metálico ubicado en la oficina del Gerente General.

Responsable: Gerente General.

14.11 Estructura funcional que soporta, genere la política y el modelo de continuidad de negocio de la empresa

La estructura funcional que soportará la política para el modelo de continuidad del negocio, será el equipo definido para estos efectos, partiendo por comunicar al Encargado de Seguridad para que analice y evalúe el impacto de la situación y coordine las actividades a realizar en las dependencias de AGTEC. El Encargado de Seguridad se pondrá en contacto con la gerencia a fin de comunicar los pasos a realizar e informará si requiere de algún apoyo adicional a sus capacidades.

14.12 ¿El modelo de continuidad de negocio contempla distintos escenarios de interrupción? (Ejemplo: desastres tecnológicos, daño e infraestructura física, contingencia que afecten a las personas, contingencia que afecten a proveedores críticos)

Dado el tipo de empresa y tamaño de AGTEC, entendemos que, en el caso de haber un desastre tecnológico, toda la documentación sensible o clasificada como importante, se encuentra resguardada el algún dispositivo de respaldo físico o bien en la nube de Google. En caso que la contingencia afecte a alguno de nuestros colaboradores, en el peor escenario, se recuperará la información desde alguno de los mecanismos definidos para estos fines o bien, se reemplazará el computador con la mayor cantidad de información recuperada.

14.13 Registro y control de incidentes producidos en la ejecución de las pruebas de continuidad de negocio y de las acciones correctivas definidas para su pronta solución

No Aplica para proveedor de acuerdo a los servicios efectuados.

14.14 ¿El plan de continuidad de negocio y/o de recuperación es capaz de restablecer los servicios proporcionados al banco?¿En cuánto tiempo?

No Aplica para proveedor de acuerdo a los servicios efectuados.

14.15 Documento formal de ejecución pruebas DRP. Proceso de mantención y actualización periódica

No Aplica para proveedor de acuerdo a los servicios efectuados.

14.16 Redundancia de instalaciones de procesamiento

No Aplica para proveedor de acuerdo a los servicios efectuados.

14.17 Plan y Calendario anual de pruebas DRP

No Aplica para proveedor de acuerdo a los servicios efectuados.

14.18 Informe de resultados asociados a la ejecución de pruebas DRP, brechas o desviaciones identificados de acuerdo a la criticidad

No Aplica para proveedor de acuerdo a los servicios efectuados.

14.19 En caso de que exista hallazgos, proceso de seguimiento de hallazgos

No Aplica para proveedor de acuerdo a los servicios efectuados.

15. Seguridad Operativa

Menciona procedimientos que aseguren las operaciones correctas y seguras de las instalaciones de procesamiento de la información, también las políticas que describan el control de cambios en la organización, procesos de negocios e instalaciones en los sistemas de procesamientos de información que afecten la seguridad de la información.

15.1 Procedimientos Operacionales y Responsabilidades

15.2 Políticas de Gestión de Cambio

La gestión del cambio busca facilitar y conseguir la implementación exitosa de los procesos de transformación, esto lo que implica trabajar con y para las personas en la aceptación y asimilación de los cambios y en la reducción de la resistencia; facilitando el éxito de los cambios, producto de una nueva forma de operación.

La norma ISO9001 de Sistemas de Gestión de calidad establece en su apartado de Planificación de los cambios “Cuando la organización determine la necesidad de cambios en el sistema de gestión de la calidad, estos cambios se deben llevar a cabo de manera planificada.

La organización debe considerar:

a) el propósito de los cambios y sus consecuencias potenciales;
b) la integridad del sistema de gestión de la calidad;
c) la disponibilidad de recursos;
d) la asignación o reasignación de responsabilidades y autoridades.”

Por otro lado, la norma ISO20000 de Gestión de Servicios establece en su apartado de Gestión de cambios, establece las directrices generales para la adaptación al cambio en Servicios: Hardware, Software, equipos de comunicaciones, sistemas de información, aplicaciones en producción y toda la documentación y procedimientos asociados con la ejecución, soporte y mantenimiento de los sistemas de producción.

15.3 ¿Se separan ambientes de desarrollo, prueba y producción? Describa proceso de intercambio de un ambiente a otro

No Aplica para proveedor de acuerdo a los servicios efectuados.

15.4 Controles de detección y prevención para proteger contra códigos maliciosos

No Aplica para proveedor de acuerdo a los servicios efectuados.

15.5 Registro de incidentes de seguridad de la información que contengan actividades de usuario, excepciones, fallas e incidentes.

No Aplica para proveedor de acuerdo a los servicios efectuados.

15.6 Registro de actividades del administrador u operador del sistema

No Aplica para proveedor de acuerdo a los servicios efectuados.

15.7 Control o procedimientos de instalaciones de software en sistemas operativos

No Aplica para proveedor de acuerdo a los servicios efectuados.

15.8 Controles de auditoría interna de sistemas de información

No Aplica para proveedor de acuerdo a los servicios efectuados.

15.9 Procedimientos de control de cambios en sistema, aplicaciones e infraestructura. Explique aplicación de procedimientos

No Aplica para proveedor de acuerdo a los servicios efectuados.

16. Seguridad en las Comunicaciones:

Este ítem de revisión tiene como objetivo revisar el conjunto de políticas procedimientos y controles para proteger la transferencia de la información. Como también el control o mecanismo que proteja adecuadamente la información contenida en la mensajería electrónica.

16.1 Políticas y procedimientos de transferencia de información

No Aplica para proveedor de acuerdo a los servicios efectuados.

16.2 Detallar tipo de análisis de navegación y correo electrónico, por ejemplo: filtro de contenido y correo electrónico.

No Aplica para proveedor de acuerdo a los servicios efectuados.

17. Adquisición, desarrollo y mantenimiento de los sistemas de Información

El objetivo asegurar los controles y herramientas que estén dirigidas a la seguridad de la información, dentro del ciclo de vida de desarrollo de los sistemas de la información.

17.1 Control de seguridad en los procesos de desarrollo y soporte

No Aplica para proveedor de acuerdo a los servicios efectuados.

17.2 Políticas o procedimientos de desarrollo seguro.

No Aplica para proveedor de acuerdo a los servicios efectuados.

17.3 ¿Contrata desarrollo externalizado? Describa tipo de control que utiliza para la supervisión y seguimiento de la actividad de desarrollo de sistemas

No Aplica para proveedor de acuerdo a los servicios efectuados.

17.4 Procedimientos de control de cambio de los sistemas

No Aplica para proveedor de acuerdo a los servicios efectuados.

17.5 Revisión técnica de las aplicaciones después de cambios en las plataformas

No Aplica para proveedor de acuerdo a los servicios efectuados.

17.6 Control de pruebas de seguridad y aceptación de sistemas

No Aplica para proveedor de acuerdo a los servicios efectuados.

17.7 El Banco es informado cuando se efectúan pasos a producción que puedan afectar el servicio

No Aplica para proveedor de acuerdo a los servicios efectuados.

17.8 Conjunto de políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento

No Aplica para proveedor de acuerdo a los servicios efectuados.

17.9 Conjunto de políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento

No Aplica para proveedor de acuerdo a los servicios efectuados.

18. Cifrado y Encriptación:

Conjunto de políticas que indique usos de los controles criptográficos para la protección de la información, así como también la protección y el tiempo de vida de las llaves cristalográficas durante todo su ciclo de vida.

18.1 Políticas de uso de los controles criptográficos

18.2 Gestión de claves

18.3 Tipo de cifrado para conexiones externas

No Aplica para proveedor de acuerdo a los servicios efectuados.

19. Servicios en la Nube:

Este ítem de revisión tiene como objetivo explicar tipos de servicios prestados, infraestructura como servicio (IaaS), plataforma como servicio (PaaS), Software como Servicio (SaaS). Así como también servicios nube contratados para la organización.

19.1 Describa tipos de servicios nube prestados

AGTEC actualmente no provee infraestructura como servicios de tipo (IaaS), plataforma como servicio (PaaS), Software como Servicio (SaaS). No obstante, hemos contratado los servicios de correo (GSuite) y espacio en la nube de Google Drive.

19.2 Quien es el responsable de lo que ocurre entre el proveedor del servicio cloud y el cliente cloud.

AGTEC cuenta con una persona responsable (Oficial de Seguridad) que se encarga de solicitar tanto las altas, bajas y modificaciones de cuentas correo que se necesiten mediar con la plataforma Gsuite. Este proceso se encuentra en directa comunicación con la asistente de administración, quien comunica cualquier actualización en este sentido.

19.3 Políticas o controles de acceso, identidad y autentificación para nube

AGTEC cuenta con una persona responsable (Oficial de Seguridad) que se encarga de solicitar tanto las altas, bajas y modificaciones de cuentas correo que se necesiten mediar con la plataforma Gsuite, así como también de la información que se requiera respaldar.

19.4 Procedimientos de administración relacionados con el entorno cloud

No Aplica para proveedor de acuerdo a los servicios efectuados.

19.5 Control o herramienta en la cual se visualiza auditoría de actividades

No Aplica para proveedor de acuerdo a los servicios efectuados.

19.6 Cuadro resumen de registros de incidentes de seguridad que afecta de servicio en la nube

No Aplica para proveedor de acuerdo a los servicios efectuados. Los servicios contratados sólo corresponden a correos y respaldos efectuados de manera discrecional de la información que AGTEC considera sensible.

19.7 Certificaciones en relación a seguridad en la nube

No Aplica para proveedor de acuerdo a los servicios efectuados

19.8 Métodos de transmisión de datos Vulnerables

No Aplica para proveedor de acuerdo a los servicios efectuados

19.9 Respaldo de datos en la nube según tipo de contingencia

Control: AGTEC establece la siguiente política en materia de respaldo y borrado seguro de la información:

Permanentemente se debe efectuar copia de respaldo de toda la información considerada confidencial o sensible y que se encuentre contenida en los computadores de las oficinas de AGTEC en la nube de Google.

A modo de procedimiento general, cuando un profesional renuncie a AGTEC o bien es desvinculado, se hará un respaldo de información de su computador en caso que se requiera acceder a ella, por razones particulares de la empresa o por algún requerimiento de algún cliente.

La información se mantendrá en la nube por un periodo no inferior a 12 meses.

20. Relación con los Proveedores:

Este ítem de revisión tiene como objetivo explicar tipos de servicios prestados de sus proveedores dentro de su organización o clientes (IaaS), plataformas como servicio (PaaS), Software como Servicio (SaaS). Así como también servicios nube contratados para la organización.

20.1 Políticas y normas de seguridad de la información orientada a la relación con proveedores.

Todo el personal externo que desarrolle labores para AGTEC deberá tomar conocimiento de la política general de seguridad de la información observando sus directrices y colaborando en su aplicación dentro de su ámbito de acción.

Para estos efectos, el trabajo o proyecto realizado por el proveedor debe ser compatible con los estándares de seguridad de la información establecidos por AGTEC.

Prestación de los servicios en AGTEC

Los proveedores sólo podrán desarrollar para AGTEC aquellas actividades cubiertas bajo un contrato de prestación de servicios.

La empresa proveedora deberá asegurar que todo su personal que presta servicios en AGTEC, tiene la formación y capacitación para efectuar el servicio contratado.

Confidencialidad de la información

El personal externo que tenga acceso a la información de AGTEC entenderá que dicha información por defecto, es de carácter confidencial.

Queda prohibido para los proveedores revelar, modificar, destruir o dar mal uso de la información, cualquiera sea el soporte de la información.

El proveedor deberá resguardar por un tiempo indefinido la confidencialidad y no podrá difundir la información a la que tiene acceso, salvo que esté debidamente autorizado por el dueño de esta.

El proveedore deberá minimizar el número de informes en formato papel que contengan información confidencial o de uso privado y se mantendrán los mismos en un lugar seguro y fuera del alcance de terceros (de acuerdo a la política de escritorio limpio).

En caso que por motivos directamente relacionados con el trabajo, el colaborador de la empresa proveedora de servicios tome conocimiento de información confidencial contenida en cualquier tipo de soporte, deberá entender que es estrictamente temporal, con la obligación de secreto y sin que con ello se le confiera derecho de posesión, titularidad o copia sobre la citada información.

Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para AGTEC.

El incumplimiento de estas será sancionado en los términos establecidos por las leyes vigentes.

Propiedad Intelectual

El personal externo deberá garantizar el cumplimiento de las restricciones legales del uso del material protegido por normas de propiedad intelectual.

Queda estrictamente prohibido el uso de programas informáticos que no cuenten con licencia original y vigente.

Queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo desarrollo o invención protegida por la propiedad intelectual sin la debida autorización.

Intercambio de información

Durante el intercambio de información, ninguna persona debe ocultar o manipular su identidad bajo ninguna circunstancia.

En relación al intercambio de información dentro del marco del contrato de prestación de servicios se considerarán no autorizadas las siguientes actividades:

- Trasmisión o recepción de toda clase de material de pornográfico, mensajes de naturaleza sexual explicita, declaraciones discriminatorias raciales y cualquier otra clase de declaraciones o mensaje clasificable como ofensivo o ilegal.
- Transmisión o recepción de material protegido de Copyright infringiendo la Ley de Protección Intelectual.
- Transmisión o recepción de material referido a campañas políticas
- Transmisión de avisaje comercial, material que tenga como propósito el tráfico de influencias y el uso de información privilegiada.
- Material relacionado con promoción de la prostitución infantil y el terrorismo.
- Cualquier forma de acoso laboral, sexual, discriminación en cualquiera de sus formas y violencia de género.

Uso apropiado de recursos

Los recursos que AGTEC pone a disposición del personal externo, están disponibles exclusivamente para cumplir las obligaciones y propósitos operativos para los cuales fueron proporcionados. AGTEC se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de los recursos.

Cualquier información introducida a la red de AGTEC o cualquier equipo conectado a ella a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en las políticas de seguridad, protección de datos de carácter personal y control de virus.

Se prohíbe expresamente:

- La comercialización o entrega de información de propiedad AGTEC o bases de datos de usuarios, personal y/o proveedores.
- El uso de los recursos proporcionados por AGTEC para actividades no relacionadas con el propósito del servicio
- Introducir en los sistemas de AGTEC o la red, contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente a la red de AGTEC cualquier tipo de malware (programas, macros, etc.), dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencias de ordenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. Todo personal con acceso a la red de AGTEC tendrá la obligación de utilizar programas de antivirus y sus actualizaciones para prevenir la entrada a los sistemas o corromper los datos informáticos.
- Intentar acceder sin autorización explicita a áreas restringidas de los sistemas de información de AGTEC.
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, dañar o alterar los recursos informáticos de AGTEC.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar datos, programas o documentos electrónicos de custodia y/o responsabilidad de AGTEC.

Equipamiento del proveedor

Los proveedores de servicios deberán asegurarse de que todo el equipamiento informático utilizado para acceder a información de responsabilidad de AGTEC cumpla las siguientes normas:

- Cuando se desatienda un puesto durante un periodo corto de tiempo el sistema deberá activar su bloqueo en forma automática.
- Ningún equipo dispondrá de herramientas que puedan transgredir el sistema de seguridad ni las autorizaciones dentro de los sistemas la organización.
- El equipo debe mantenerse de acuerdo a las especificaciones del fabricante.
- Todos los equipos del usuario estén adecuadamente protegidos frente a malware.

20.2 Método de monitoreo de provisión de servicios de terceros.

AGTEC establece un método de monitoreo y control del servicio de terceros contratados de acuerdo a los siguientes criterios:

a) El proveedor deberá cumplir con la disponibilidad de documentación acordado en el contrato de servicio.

b) Todos los productos que producirán debieran estar acorde a lo acordado en el contrato, así como los servicios que se tienen que prestar y las actividades que van a realizar.

c) Adicionalmente se establecen y definen las actividades de seguimiento, medición y control por etapas que estarán asociadas a hitos de pago, si los mismos cumplen con los criterios de calidad establecidos en el contrato.

d) El proveedor debe designar personas competentes o que cumplan con las calificaciones para llevar a cabo el servicio.

e) De manera periódica se validará y revalidará la capacidad de conseguir los resultados planificados, según criterios de validación y actividades de seguimiento y medición.

f) Se establecen y acuerdan actividades para realizar la liberación, entrega y post entrega del o los productos, en el contrato de servicio.

20.3 Estructura funcional de control del servicio.

AGTEC ha definido qué para cada servicio encomendado a un tercero, se designará un responsable del Servicio por parte de la empresa, el que interactuará de manera directa en cada una de las reuniones de avance, seguimiento y recepción de entregas de parte del tercero, a fin de validar los avances y calidad de los entregables. El responsable del Servicio interactuará con un par equivalente responsable del servicio contratado, y que ambos darán cuenta de los avances de las tareas realizadas y del cumplimiento de los plazos y entregables de acuerdo a la calidad encomendada por AGTEC y conforme lo establecido en el contrato de servicios.

20.4 Mecanismo de control y seguimiento de servicios de terceros.

El mecanismo de control y seguimiento de servicios de terceros de acuerdo a lo que ha definido AGTEC, será mediante reuniones de avance periódicas (semanal y/o quincenal) en donde se revisará el avance de cada uno de los proyectos encomendados, se revisarán indicadores de gestión, como por ejemplo, %avance real, %avance planeado, piezas de software construidas, desviaciones, riesgos, u otros indicadores relevantes, que permitan detectar el grado de sanidad de cada proyecto y establecer de esta manera actividades de mitigación por parte del Responsable del Servicio.

20.5 Cláusulas de penalización o bonificación sobre el cumplimiento de servicios.

De acuerdo a lo establecido en las cláusulas asociadas en los contratos de prestación de servicios, todo el personal externo que desarrolle labores para AGTEC deberá cumplir con lo establecido en este documento y en las políticas de seguridad. En caso de incumplimiento de cualquiera de estas obligaciones, AGTEC se reserva el derecho a veto sobre el personal que haya cometido la infracción, así como las sanciones que se consideren pertinentes en relación a la empresa o persona contratada.

20.6 Política y procedimientos relacionados a los servicios externalizados.

Los proveedores de servicios deberán asegurarse de que todo el personal que desarrolla labores para AGTEC, respete las siguientes condiciones en el desarrollo de sus actividades informáticas:

Las personas con acceso a la información de AGTEC son responsables de la actividad desarrollada por su identificador de usuario y todo lo que de él se derive.

Los usuarios no deberán utilizar ningún identificador distinto al propio, aunque disponga de la autorización del propietario.

Las personas con acceso a información con responsabilidad de AGTEC deberán seguir las directrices de gestión de contraseñas.

Seleccionar contraseñas de calidad

Pedir el cambio de contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

Cambiar las contraseñas periódicamente y evitar reutilizar o reciclar contraseñas antiguas.

Cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión (login).

Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.

Notificar cualquier incidente de seguridad relacionado con sus contraseñas como perdidas, robos o indicio de perdida de confidencialidad.

Cualquier persona con acceso a información de responsabilidad de AGTEC deberá velar para que los equipos queden protegidos, cuando vayan a quedar desatendidos.

20.7 Registro de comunicación de cambio en las políticas a proveedores.

AGTEC comunicará debidamente a los proveedores, cuáles son las políticas vigentes de relación con proveedores. En caso de existir algún cambio o modificación de alguna de ellas, serán debidamente comunicadas por vía email y de manera presencial o remota, a fin de que exista un total entendimiento de las partes involucradas y el impacto que al proveedor pueda generar.

20.8 Política o procedimientos de cambios en la relación de servicios externalizados.

AGTEC ha definido como política que cualquier servicio contratado debe quedar establecido mediante un contrato formal firmado por las partes. No obstante, lo anterior, en caso de requerir cambios adicionales a lo establecido, el procedimiento será el siguiente:

a) Identificar un nuevo requerimiento de lo inicialmente pactado o ampliación del alcance de la funcionalidad que no había sido considerado en el contrato.

b) El proveedor deberá evaluar el impacto y entregar un documento con el impacto en tiempo y costo que el cambio requiere.

c) AGTEC en caso de aceptar la evaluación entregada por el proveedor, se realizará un anexo al contrato inicial en señal de aceptación del cambio.

21. Cumplimiento Regulatorio:

Este ítem de revisión tiene como objetivo recopilar el nivel de cumplimiento de las normas vigentes que regulan a los proveedores del Banco.

21.1 Identificación de la legislación aplicable y de los requisitos contractuales.

AGTEC cumple con todas las disposiciones legales vigentes.

21.2 Protección y privacidad de la información de carácter personal.

AGTEC mantiene en formato físico y en la nube de Google toda la información de carácter personal de cada uno de los colaboradores de la empresa y con acceso restringido.

21.3 Método de control de acceso a la información.

AGTEC ha definido un responsable de seguridad que se encarga de administrar los respaldos de información y accesos a la nube de Google. De mismo modo, la gerencia cuenta con los accesos en caso que el Encargado de seguridad pueda presentar algún inconveniente.

22. Gestión de incidentes de seguridad de la información y mejoras:

Este ítem de revisión tiene como objetivo recopilar el nivel de gestión de los incidentes de seguridad en cuanto a procesos, registros y gestión del incidente.

22.1 Procesos disciplinarios para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial por parte de los trabajadores

Declaración de la Política:

Los incidentes de seguridad de la información deben ser investigados de forma apropiada por el personal entrenado y calificado para esta actividad.

Control:

De acuerdo a lo que hemos establecido, existe un proceso disciplinario formal que se comunica a los colaboradores y que indica las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad. Al momento de ingresar cada colaborador debe firmar un acuerdo de confidencialidad que permitirá proteger la información tanto de AGTEC como de los clientes en los que prestarán servicios.

El proceso disciplinario será aplicado previa verificación de que se ha producido una violación de la seguridad. Este proceso tendrá un tratamiento correcto e imparcial para los colaboradores de los que se sospeche hayan cometido alguna violación de seguridad.

El proceso disciplinario formal proporciona una respuesta gradual que tiene en cuenta factores tales como la gravedad y naturaleza de la violación de seguridad y su impacto en el negocio o en los clientes. Si esta acción corresponde a una infracción por primera vez o se trata de una acción repetida, se trata de identificar si quien ocasionó la infracción fue adecuadamente formado, o no, conoce las implicancias legales y los impactos que este puede traer para el negocio.

El proceso disciplinario tiene por objeto ser utilizado como elemento disuasivo para evitar que los colaboradores violen las políticas de seguridad de la información de la empresa y demás violaciones de la seguridad de la información.

En caso de que la infracción sea considerada como una acción deliberada, implicará una acción inmediata que puede terminar con el cese de sus funciones.

Los controles que se han establecido son.

- Evaluar si la empresa tiene la capacidad para resolver una infracción por si misma o necesita de ayuda de terceros.

- Mantener un registro con las evidencias de las infracciones
- Registrar acciones llevadas a cabo y resultados de las mismas
- Cierre de infracciones de seguridad formalmente cuando se hayan resuelto
- Realizar análisis para determinar las causas de cada infracción

22.2 Registro de publicación de políticas de incidentes de seguridad.

En AGTEC serán registrados, protegidos y revisados periódicamente las actividades de los usuarios, excepciones, y/o eventos de seguridad de información que sean reportados o detectados.

Los registros de incidentes de seguridad contienen la siguiente información relevante:

a) identificador de usuario;

b) actividades del sistema;

c) fechas, tiempos y eventos clave, como por ejemplo conexión y desconexión;

d) identificación del dispositivo, sistemas o aplicación;

e) registro de intentos de acceso exitosos y fallidos;

f) registro de intentos de acceso a los recursos y a los datos exitosos y fallidos;

g) cambios en la configuración del sistema;

h) determinación del uso de privilegios;

i) Archivos a los que ha accedido y tipo de acceso;

j) direcciones y protocolos de red;

k) alarmas que puedan generarse por el sistema de control de acceso;

l) activación y desactivación de los sistemas de protección;

m) registro de transacciones realizadas por usuarios en las aplicaciones.

22.3 Proceso de gestión de incidentes de seguridad

AGTEC ha definido el siguiente procedimiento para la gestión de los incidentes de la seguridad de la información con los siguientes objetivos generales

- Detectar, informar y evaluar incidentes de la Seguridad de la información
- Responder a incidentes
- Reportar vulnerabilidades
- Aprender de los incidentes de la Seguridad de la información

Pasos para resolver incidentes

1. Notificación del incidente:

Un colaborador cuando detecta un evento que pueda dañar el funcionamiento de la empresa, deberá comunicar el incidente mediante un correo electrónico o vía telefónica)

2. Clasificación del incidente:

Una persona definida para este tipo de necesidad, recibirá la notificación del evento y, según los parámetros internos validados con la gerencia, será clasificado, pero es un experto técnico que lo clasifica de la manera adecuada.

3. Tratamiento del incidente:

Una vez que se clasifique el evento o infracción de seguridad y se conoce la gravedad y el tiempo acordado para su resolución, un experto técnico deberá decidir cuál o cuáles serán las medidas necesarias para resolverlo.

4. Cierre el incidente:

Una vez que se resuelve el incidente, se registra la información generada durante el tratamiento y, se notifica a la persona originó la notificación del incidente, que se cerró.

5. Base de conocimiento:

Se creará una base de conocimiento con toda la información que se genere durante el tratamiento del incidente, información que servirá para posibles incidentes similares en el futuro, reduciendo el tiempo de investigación.