**POLÍTICA DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**

**I.- DEFINICIONES ESTRATÉGICAS**

La [Empresa XXX], a través de su Comité de Riesgos y Seguridad de la Información, presenta en este documento las características mínimas obligatorias de seguridad de la información y confidencialidad, integridad y disponibilidad para la organización y coordinación institucional a fin de gestionar adecuadamente la administración de la información (recopilación, procesamiento, almacenamiento y distribución) en consistencia con los principios rectores de la política general de seguridad de la información. Para los efectos de esta política, los documentos electrónicos institucionales constituirán un activo de información y se tratarán de acuerdo con la relevancia institucional. Con lo cual, se compromete a todo nivel, a proteger sus activos de información, estableciendo una adecuada gestión del riesgo, asegurando cumplimiento de requisitos legales, aplicando una estrategia de seguridad basada en las mejores prácticas y controles sobre estos recursos con el fin de protegerlos de las amenazas.

El Comité de Riesgo y Seguridad de la Información, sesionará trimestralmente o ante la convocatoria de algunos de sus miembros que fundadamente invoquen alguna situación de emergencia o relevante para la empresa, con el objeto de revisar los mecanismos de gestión para la prevención de delitos y riesgos operacionales, lo que implicaría de ser necesario el desarrollo de políticas, procedimientos, guías o protocolos adicionales.

**a.- Objetivos**

Los objetivos que busca esta política son los siguientes:

* Establecer un marco de trabajo para las autoridades y directivos que permita controlar el funcionamiento de la seguridad de la información dentro de la organización.
* Asignar las responsabilidades en relación con seguridad de la información.
* Promover la segregación de funciones.
* Establecer los mecanismos de coordinación con los contactos y encargados apropiados.
* Promover comunicación y contactos con comunidades y grupos asociadas a la seguridad de la información para fortalecer la comunidad interna tanto técnica como profesional.
* Se favorecerá la integración de la seguridad de la información en la gestión de los proyectos institucionales, sin importar la naturaleza del proyecto.

**b.- Alcance**

Esta política se aplica a todos los trabajadores y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información de la [Empresa XXX]. También se aplica a cualesquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información.

Esta política rige independientemente del lugar en el trabajador presta sus servicios a la organización, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea “presencial”, “a distancia”, “teletrabajo” u otra, en las condiciones que establezca la legislación vigente, los planteamientos de la Dirección del Trabajo o los Estados de Excepción Constitucional decretados por el Presidente de la República.

Esta política gobierna la seguridad de la información de todos los procesos estratégicos de la [Empresa XXX], establecidos en el documento institucional denominado Definiciones Estratégicas o equivalente, cubriendo a toda la organización independiente de su ubicación geográfica en el país (Chile Continental, Chile Insular o la Antártica Chilena).

**c.- Vigencia y Actualización**

La Política se considera vigente desde la fecha de su aprobación por parte de la autoridad, documento que será revisado y actualizado cada dos años o cuando el Comité de Riesgos y Seguridad de la Información lo determine, o toda vez que se produzca un cambio significativo que modifique el nivel de riesgo presente de la [Empresa XXX].

La Política deberá ser revisada por el Comité de Seguridad de la Información. No obstante, aquello, la [Unidad responsable de Ciberseguridad] promoverá la revisión permanente de esta Política y generará las propuestas de actualización que sean necesarias, con el objetivo de apoyar el ciclo de mejora continua del SGSI.

Entre los cambios que hacen necesaria la revisión de las políticas, se debe destacar:

* Cambios en las leyes o reglamentos que afecten a la [Empresa XXX].
* Incorporación o modificaciones relevantes de procesos críticos de la [Empresa XXX].
* Cambios significativos al soporte tecnológico.
* Modificaciones en la estructura de la organización.
* Cambios significativos en los niveles de riesgo a que se expone la información.
* Cambios relevantes en las Definiciones Estratégicas.}
* Ajustes necesarios producto de Estados de Excepción Constitucional.
* Ajustes necesarios para proteger las infraestructuras críticas.

Las revisiones que se efectúen a la Política de General de Seguridad de la Información deben considerar tanto la actualidad de ella, como su eficacia, eficiencia y cumplimiento.

**d.- Revisión del cumplimiento**

El Comité de Riesgos y Seguridad de la Información, anualmente, asignará la responsabilidad de ejecutar un proceso formal de revisión del cumplimiento a cargo de una o varias unidades organizacionales, pudiendo optar también por una revisión independiente interna o una externa ejecutada por una tercera parte.

Además, este Comité determinará la metodología y los alcances que estime necesarios para cumplir los objetivos estratégicos de revisión y cumplimiento de las políticas y su mejora continua.

**e.- Control de documentos**

Los documentos requeridos por el Sistema de Gestión de la Seguridad de la Información (SGSI) deben protegerse y controlarse. Con este objetivo, las acciones necesarias a implementar son:

* Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.
* Registrar los cambios o actualizaciones de los documentos una vez que son aprobados por el Comité de Riesgos y Seguridad, incorporando Tabla en Capitulo final en cada documento.
* Se deberá controlar el uso no intencionado de documentos obsoletos.
* En caso de mantenerse los documentos por cualquier propósito, éstos deberán tener una adecuada identificación a efecto de diferenciarse de los vigentes.

Las versiones pertinentes de los documentos aplicables se encontrarán disponibles para quienes lo necesiten y serán almacenados y transferidos de acuerdo con los procedimientos aplicables a su clasificación.

**f.- Difusión**

El mecanismo de difusión de la Política será a través de la Intranet, circulares informativas, correos electrónicos masivos o cualquier otro medio que el Comité de Riesgos y Seguridad de la Información estime pertinente, procurando apoyar la sensibilización con infografías que faciliten la comprensión de esta por todos los usuarios en general.

**II.- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**

La Política de Seguridad de la Información, busca establecer y formalizar las tareas, funciones y responsabilidades sobre la seguridad en los procesos de tratamiento de la información, incluyendo la recopilación, el desarrollo de sus procesos, el procesamiento mismo, el almacenamiento y la distribución de la información, lo que permitirá gestionar y controlar adecuadamente la seguridad de la información al interior de la organización, con una adecuada gestión de los riesgos, de manera de lograr una adhesión y compromiso a todo nivel.

**a.- Organización Interna**

**Organización y de la Seguridad de la Información**

El máximo organismo responsable de la coordinación y supervisión en materia de seguridad de la información en la [Empresa XXX], será el Comité de Riesgos y Seguridad de la Información, en adelante el Comité. Este Comité estará constituido por los Jefes de División y/o su representante en que se delegue la responsabilidad de la toma de decisión de las divisiones respectivas. Para efectos de presentación de cambios a las Políticas de Seguridad de la Información tanto general como específicas se requerirá de la presentación ante el [Directorio] en su calidad de supervisor general del Comité de Riesgos y Seguridad. Para los procedimientos, normativas, guías y documentos de buenas prácticas será necesario el V°B° del Encargado de Ciberseguridad, debiendo establecerse consulta al Comité cuando los cambios o nuevos documentos tuvieren un impacto relevante en la empresa o tuvieren posiciones no totalmente concordantes con las políticas general o específicas.

**Asignación de Roles y Responsabilidades sobre la Seguridad de la Información**

A continuación, se detallan la autoridad y responsabilidades de quienes participan en la administración, implementación y evaluación de la Política de Seguridad de la Información en la [Empresa XXX], la que debe estar en directa relación con la orgánica y funcionalidades descritas en la constitución del Comité de Riesgos y Seguridad de la Información:

[Directorio]:

* Supervisión General.

Responsabilidad:

* Aprobar y comunicar la Política de Seguridad de la Información.
* Supervigilar que las estrategias definidas por el Comité, para el control asociado a los activos de información, estén en concordancia con las políticas institucionales de seguridad de la información y los objetivos del negocio.

Comité de Riesgos y Seguridad de la Información:

* Supervisión y Coordinación de Decisiones.

Responsabilidad:

* Proponer las definiciones estratégicas, lineamientos y prioridades, así como también los recursos e insumos, que permitan orientar y focalizar las políticas, planes, programas e iniciativas en materias de Seguridad de la Información.
* Definir roles y las responsabilidades de todo el personal involucrado, incluyendo además colaboradores y terceras personas en materia de Seguridad de la información.
* Evaluar y seleccionar materias a incorporar en la Política de Seguridad de la Información.
* Impulsar y proponer al Jefe de Servicio las políticas y directrices definidas en materia de seguridad de la información.
* Apoyar y promover la seguridad de la información dentro de la empresa, mediante la difusión, educación y concientización sobre las Políticas y otras medidas de seguridad.
* Coordinar, supervisar y monitorear la implementación de las Políticas y procedimientos de la seguridad de la información.
* Coordinar los esfuerzos con las diferentes Divisiones, Departamentos, Servicios y todos los grupos interés de la empresa que tengan responsabilidades sobre la seguridad de la información.
* Analizar, evaluar y priorizar las estrategias de tratamiento de riegos en la Seguridad de la Información.
* Asegurar la protección de los activos de información en la empresa.
* Reportar al [Directorio], el resultado de la implementación de la Política, de los Riesgos, y de las medidas de administración de la Seguridad de la Información.
* Aprobar los aspectos operativos de la implementación del Sistema de Gestión de Seguridad de la Información.
* Definir los mecanismos a través de los cuales se implementará el alcance de la Política General de Seguridad.
* Delimitar las responsabilidades de todo el personal involucrado, incluyendo además colaboradores y terceras partes.
* Sesionar periódicamente, o cuando fuese necesario, conforme a la planificación anual definida por el Comité de Riesgo y comunicada según las instancias establecidas.
* Gestionar la actualización de las Políticas tanto General como Específicas.
* Gestionar la actualización de los Procedimientos, Guías, Protocolos y todos los documentos auxiliares que fueren necesarios para el mejor despliegue, comprensión y aplicabilidad de las directrices superiores.

Encargado de CiberSeguridad de Alto Nivel (Titular y Subrogante):

* Supervisión de alto nivel.

Responsabilidad:

* Ser el responsable de la seguridad informática en el servicio.
* Proponer al Comité de Riesgos y Seguridad de la Información las debidas respuestas y posible priorización de medidas de tratamiento de incidentes y riesgos vinculados a los activos de información de los procesos institucionales y sus objetivos de negocio.
* Identificar las amenazas o riesgos en la seguridad de la información o de sus instalaciones.
* Coordinar las actividades relativas a la seguridad de la información con el Comité de Riesgos y Seguridad de la Información.
* Coordinar con las distintas unidades del Servicio las acciones tendientes a cumplir y apoyar los objetivos de seguridad de la información.
* Mantener historial de versiones de las Políticas institucionales en la materia.
* Desarrollar políticas, estándares, procesos y directrices para asegurar la seguridad física y electrónica de sistemas automatizados. Asegurar que la política y los estándares de administración de seguridad son adecuados para el propósito, están actualizados y están implementados correctamente. Revisar nuevas propuestas de negocio y proveer asesoramiento especializado en temas e implicaciones de seguridad.
* Monitorear la aplicación y el cumplimiento de procedimientos de administración de seguridad y revisar sistemas de información para detectar infracciones reales o potenciales en la seguridad. Asegurar que todas las infracciones de seguridad identificadas se investigan rápidamente y en profundidad y que cualquier cambio al sistema requerido para mantener la seguridad sea implementado. Asegurar que los registros de seguridad son precisos y están completos y que las solicitudes de soporte se abordan de conformidad con los estándares y procedimientos establecidos. Contribuir a la creación y el mantenimiento de políticas, estándares, procedimientos y documentación de seguridad.
* Mantener los procesos de administración de la seguridad y comprobar que todas las solicitudes de soporte sean tratadas conforme a procedimientos acordados. Proveer orientación para definir derechos y privilegios de acceso. Investigar las infracciones de seguridad de conformidad con procedimientos establecidos, recomendar acciones requeridas y soportar/hacer seguimiento para asegurar que sean implementadas.
* Investigar infracciones de seguridad menores conforme a los procedimientos establecidos. Asistir a los usuarios en la definición de sus derechos y privilegios de acceso. Ejecutar tareas de administración de seguridad no estándares y resolver asuntos relacionados con la administración de la seguridad.
* Recibir y responder a solicitudes rutinarias de soporte en materia de seguridad. Mantener registros y asesorar a las personas relevantes sobre las acciones tomadas. Asistir con la investigación y resolución de asuntos relacionados con los controles de acceso y los sistemas de seguridad.
* Ejecutar tareas simples de administración de seguridad. Mantener documentación y registros relevantes.

Jefes de División:

* Implementación de las medidas de la seguridad de la información.

Responsabilidad:

* Apoyar y promover la Política de Seguridad de la información dentro de la empresa, mediante la difusión, educación y concientización sobre la Políticas y otras medidas de seguridad.
* Cumplir con los requerimientos que el Comité de Riesgos y Seguridad de la Información efectúe a las unidades.
* Construir las directrices de mapas de procesos a implementar en los Servicios de [Empresa XXX]

Jefe de Departamento de Estrategia Planificación y Control de Gestión:

* Monitorear el avance de las medidas de seguridad.

Responsabilidad:

* Realizar seguimiento a el avance general y los resultados de la implementación de las estrategias de tratamiento y control de los riesgos de la seguridad de la información.
* Reportar al Comité de Riesgos y Seguridad de la Información los resultados del control efectuado sobre las medidas de tratamiento y los riesgos de la seguridad de la información.
* Recopilar la información de los Servicios y Unidades de la empresa.
* Controlar el inventario o registro de activos de información debidamente coordinado con los responsables: división, departamento, unidad y programa.

Jefe de Auditoría Interna:

* Evaluar y mejorar la eficiencia de los procesos de gestión de riesgos, control y gobierno.

Responsabilidad:

* Asegurar la implementación de la Política de Seguridad de la Información en la Empresa.
* Verificar y evaluar el cumplimiento de las medidas de tratamiento de Riesgos en la Seguridad de la Información comprometidas con el Comité de Riesgos y Seguridad de la Información.
* Reportar el resultado de las evaluaciones al [Directorio] y al Comité de Riesgos y Seguridad de la Información.
* Evaluar el cumplimiento el avance de cada una de las etapas de la implementación del Sistema de Seguridad de la Información (SSI).
* Evaluar en forma permanente los controles internos establecidos por la Administración y recomendar medidas que signifiquen una mejora.
* Cooperar en la adopción de mecanismos de autocontrol en las Unidades operativas del Servicio.
* Verificar que los sistemas de información aplicados en la empresa generen productos confiables, oportunos y veraces.
* Velar por que las políticas y actividades de la Unidad de Auditoría Interna sean coherentes con aquellas emanadas de la autoridad.
* Remitir los informes de auditoría al [Directorio], advirtiendo sobre eventuales riesgos detectados, que requieran acciones correctivas o rectificaciones por parte del Servicio.
* Efectuar seguimientos de las medidas preventivas y correctivas emanadas de los informes de auditoría aprobados por la Autoridad.
* Participar en el Comité de Auditoría Ministerial.
* Apoyar la operación del Proceso de Gestión de Riesgos en el Servicio y cumplir con las responsabilidades establecidas para la Unidad.

Jefe División Jurídica:

* Asesoría jurídica.

Responsabilidad:

* Asesorar al Comité de Riesgos y Seguridad de la Información en materias jurídicas relacionadas con la implementación de la Política de Seguridad de la Información y evaluar la legalidad de los actos que de ésta demande.
* Asegurar la incorporación de los requisitos del Sistema de Seguridad de la información, en las diferentes celebraciones de contratos y servicios.
* Efectuar el control jurídico de los actos administrativos que realizan las unidades organizacionales dependientes de la empresa.
* Revisar e informar las investigaciones internas que se instruyan por orden de las autoridades.

Jefe [Unidad responsable de Ciberseguridad]:

* Coordinación y rol operativo.

Responsabilidad:

* Asesorar el diseño, elaboración, desarrollo, implementación, mantenimiento y actualización de planes estratégicos y acciones tendientes a otorgar seguridad a los activos de información.
* Implementar la Política General de Seguridad de la Información.
* Implementar las Políticas específicas de Seguridad de la Información.
* Implementar políticas, procedimientos, guías, protocolos, estándares, procesos y directrices para asegurar la seguridad física y lógica de sistemas automatizados. Asegurar que la política y los estándares de administración de seguridad son adecuados para el propósito, están actualizados y están implementados correctamente. Revisar nuevas propuestas de negocio y proveer asesoramiento especializado en temas e implicaciones de seguridad.
* Coadyuvar al Encargado de Ciberseguridad al monitoreo del cumplimiento de las Políticas y Procedimientos de seguridad de la Información.
* Coadyuvar a las instancias de auditoría para que puedan materializarse con las condiciones óptimas que permitan obtener conclusiones relevantes para la empresa en materia de cumplimiento de políticas y normas, así como en el cumplimiento de las metas establecidas por la gestión del riesgo institucional.
* Liderar el desarrollo técnico de los Planes de Continuidad Operacional Institucional (BCP por sus siglas en inglés) y los planes de recuperación ante desastres (DRP por sus siglas en inglés).
* Establecer una coordinación con el Encargado de Ciberseguridad para que el desarrollo de las políticas y su implementación converjan en soluciones viables, sustentables, eficaces y eficientes tanto técnica como económicamente.
* Impulsar la implementación de sistemas de monitorear del cumplimiento de procedimientos de administración de seguridad y revisión de sistemas de información para detectar infracciones reales o potenciales en la seguridad.
* Aportar toda la evidencia que permita que todas las infracciones de seguridad identificadas sean investigan rápidamente y en profundidad y que cualquier cambio al sistema requerido por la empresa para mantener la seguridad sea implementado.
* Proveer sistemas que permitan asegurar que los registros de seguridad son precisos y están completos y que las solicitudes de soporte se abordan de conformidad con los estándares y procedimientos establecidos.
* Contribuir a la creación y el mantenimiento de políticas, estándares, procedimientos y documentación de seguridad.
* Implementar procesos de administración de la seguridad y comprobar que todas las solicitudes de soporte sean tratadas conforme a procedimientos acordados.
* Implementar las directrices sobre derechos y privilegios de acceso.
* Colaborar en la Investigación de las infracciones de seguridad de conformidad con procedimientos establecidos, adoptar las recomendaciones sugeridas, manteniendo el debido seguimiento para asegurar que sean implementadas.
* Investigar desde la dimensión operativa y técnica, infracciones de seguridad menores conforme a los procedimientos establecidos. Apoyar a los usuarios en la configuración de sus derechos y privilegios de acceso.
* Recibir y responder a solicitudes rutinarias de soporte técnico en materia de seguridad. Mantener registros y asesorar técnicamente a las personas relevantes sobre las acciones tomadas. Asistir con la investigación y resolución de asuntos relacionados con los controles de acceso y los sistemas de seguridad.

Jefe Departamento de Desarrollo y Gestión de Personas:

* Coordinación y operativo.

Responsabilidad:

* Informar y notificar al personal que ingrese a la empresa sobre sus obligaciones respecto del cumplimiento de la Política General de Seguridad de la Información y de todas las normas, procedimientos y prácticas aplicadas en la [Empresa XXX]. Informar a la [Unidad responsable de Ciberseguridad] sobre el personal contratado, a efecto de protocolizar, identificar o designar el perfil de usuario del personal ingresado. Se deberá procurar que la entrega de esta información sea automatizada y en tiempo real con el objetivo de disminuir los riesgos de ciberseguridad vinculados a estos casos.
* Informar oportunamente a la [Unidad responsable de Ciberseguridad] acerca de los movimientos del personal para la creación, cambios de estado o eliminación de cuentas de correo institucionales. Se deberá procurar que la entrega de esta información sea automatizada y en tiempo real con el objetivo de disminuir los riesgos de ciberseguridad vinculados a estos casos.
* Avisar oportunamente a la [Unidad responsable de Ciberseguridad] en el caso de modificación de las funciones de un funcionario o empleado de planta, contrata u honorarios, para realizar un análisis de los derechos de accesos a la información actual que posee el usuario en cuestión y se retiran permisos de acceso a la información o se otorgarán nuevos derechos propios de la función asumida, según requiera su Jefatura. Se deberá procurar que la entrega de esta información sea automatizada y en tiempo real con el objetivo de disminuir los riesgos de ciberseguridad vinculados a estos casos.
* Coordinar con la [Unidad responsable de Ciberseguridad] y el Departamento de Administración el ingreso, desvinculación o cambios del personal, para resguardar o recuperar la información de bienes que se encuentran a su cargo y los privilegios de acceso de información.
* Incorporación de la normativa vigente, que se refiera al Sistema de Seguridad de la información, en los actos administrativos y contratos. Las normas y política expresadas en esta resolución, se considerarán parte integrante y se adjuntarán a los decretos o resoluciones de nombramiento o contrataciones de personal, de planta, a contrata o sobre la base de honorarios.

Unidad de Coordinación de Ciberseguridad

* Coordinación de alto nivel

Responsabilidad:

* Materializar los aspectos encomendados por el Directorio en materia de Ciberseguridad.
* Recomendar políticas y normas.
* Promover e impulsar la Protección de las Infraestructuras Críticas.
* Favorecer el uso de protocolos y estándares de ciberseguridad en la empresa.
* Promover buenas prácticas en el funcionamiento del Equipo de Respuesta frente a Incidentes Informáticos de la empresa (CSIRT).
* Promover planes de capacitación, entrenamiento, difusión y educación en el marco de los objetivos planteados por el Directorio.

Responsable de la Información e Instalaciones de Procesos Institucionales:

* Operativa Específica.

Responsabilidad:

* Custodiar, proteger o almacenar la información y activos, vinculados a determinado proceso Institucional.
* Definir el acceso a los activos de información y velar por su cumplimiento.

Trabajadores:

* Obligación de conocimiento y cumplimiento.

Responsabilidad:

* Conocer y cumplir la Política de Seguridad de la Información vigente, entendiendo en ésta la General y Específicas.
* Utilizar adecuadamente los activos de información a su cargo.
* Utilizar adecuadamente la plataforma tecnológica, servicios informáticos, equipamiento y dispositivos institucionales.

**Autorización para las Instalaciones de procesamiento de información**

Los procesos licitatorios para la adquisición e instalación de nuevos recursos y servicios tecnológicos serán visados por la [Unidad responsable de Ciberseguridad], y deberán estar acordes a los lineamientos de seguridad establecidas por la Política General y las Políticas Específicas vigentes. En caso de no estar alineados con estos instrumentos normativos se deberá iniciar un proceso ante el Comité de Riesgos y Seguridad de la Información tendiente a compatibilizar la nueva tecnología en las Políticas vigentes mediante presentación de informe fundado técnica, jurídica y económicamente.

Además, la [Unidad responsable de Ciberseguridad] evaluará, negará o autorizará, el uso de servidores de procesamiento de información, equipamiento personal en las dependencias, e infraestructura tecnológica de la empresa.

**Contacto con Grupos Especiales de Interés**

La [Unidad responsable de Ciberseguridad] deberá coordinar los conocimientos y experiencias que ha adquirido la Empresa, con el fin de brindar asesoría en la toma de decisiones en materia de seguridad de la información. Asimismo, podrá asociarse y hacerse asesorar por otros organismos y establecer convenios de cooperación nacionales e internacionales.

**Confidencialidad de la Información**

Los contratos o convenios de trabajo, cooperación o servicios suscritos con terceras partes y que involucren los activos de información, deberán contar con cláusulas de confidencialidad o no divulgación, debidamente validadas por la [unidad jurídica].

**b.- Partes Externas**

**Relación con terceros**

La Empresa establecerá e implementará los mecanismos de control necesarios para la seguridad de los activos de información, en sus relaciones con personal externo que le provean de bienes o servicios. Los trabajadores responsables de la supervisión o fiscalización de contratos, convenios o acuerdos o con personal externo, deberán garantizar el cumplimiento de la Política General de Seguridad de la Información por parte de éstos.

Todo contrato, convenio o acuerdo con personal externo deberá tener claramente definidas las exigencias y los distintos niveles de servicios (uso, intercambio, procesamiento, etc.), en términos de seguridad de la información, requisito que se contemplará como un numeral de las especificaciones técnicas.

La Empresa, antes de permitir el acceso a la información e instalaciones de procesamiento, deberá asegurarse de la identificación de los riesgos asociados y de la implementación de las medidas apropiadas para la disposición de la información.

La empresa deberá exigir, al momento del contrato o inicio de operaciones del servicio, la suscripción de un acuerdo de confidencialidad entre la empresa y la empresa proveedora, al igual que uno entre la empresa y cada uno de los trabajadores de la empresa contratada que tengan participación directa en los servicios prestados o tomen conocimientos de datos institucionales independientemente de si éstos son considerados públicos, reservados o secretos.

La Política de Seguridad de la Información, busca establecer y formalizar las tareas, funciones y responsabilidades sobre los procesos de tratamiento de información, incluyendo la recopilación, el desarrollo de sus procesos, procesamiento, almacenamiento y distribución de la información, lo que permitirá gestionar y controlar adecuadamente la seguridad de la información al interior de la organización, de manera de lograr una adhesión y compromiso a todo nivel.

**III.- TRABAJO A DISTANCIA O TELETRABAJO**

Por la complejidad y transversalidad del concepto se implementará una política específica y las medidas que apoyen la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de trabajo a distancia y de teletrabajo.

En esta política, en tanto no se especifique algún normativa específica o legislación jerárquicamente superior que lo reemplace, se establecerán las condiciones y las restricciones del uso del trabajo a distancia o del teletrabajo. Se deberán considerar los siguientes asuntos donde se considere aplicable y lo permita la ley vigente o los Estados de Excepción Constitucional decretados por el Presidente de la República:

* la seguridad física existente del sitio de teletrabajo, considerando la seguridad física del edificio y del entorno local;
* el entorno de teletrabajo físico propuesto;
* los requisitos de seguridad para las comunicaciones, considerando la necesidad de contar con acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se accederá y que se traspasará por el enlace de comunicaciones y la sensibilidad del sistema interno;
* la provisión de acceso a un escritorio virtual que evite el procesamiento y el almacenamiento de información en equipos de propiedad privada;
* la amenaza del acceso no autorizado a la información o a los recursos de parte de otras personas que utilizan el recinto, es decir, la familia y los amigos;
* el uso de redes domésticas y los requisitos o restricciones en la configuración de los servicios de redes inalámbricas;
* las políticas y procedimientos para evitar disputas en cuanto a los derechos de propiedad intelectual desarrollados en equipos de propiedad privada;
* acceso a equipos de propiedad privada (para verificar la seguridad de la máquina durante una investigación), lo que se puede evitar por legislación;
* acuerdos de licenciamiento de software que pueden hacer que las organizaciones se hagan responsables del software de cliente en estaciones de trabajo de propiedad privada de empleados o de usuarios externos;
* requisitos de protección de malware
* requisitos de protección en su firewall (cortafuegos).

Las pautas y disposiciones que se deberán incluir son:

* la provisión de equipos idóneos y muebles de almacenamiento para las actividades de teletrabajo, donde no se permite el uso de equipos de propiedad privada que no estén bajo el control de la organización;
* una definición del trabajo permitido, las horas de trabajo, la clasificación de información que se puede tener y los sistemas y servicios internos que se autoriza al teletrabajador a acceder;
* la provisión de equipos de comunicación idóneos, incluidos los métodos para proteger el acceso remoto;
* seguridad física;
* normas y orientación sobre el acceso a familiares y visitas a los equipos y a la información;
* la provisión de soporte y mantenimiento de hardware y software;
* la provisión de seguros;
* los procedimientos para el respaldo y la continuidad en el negocio;
* auditoría y monitoreo de seguridad;
* revocación de autoridad y derechos de acceso y la devolución de los equipos cuando concluyen las actividades de teletrabajo.

De manera obligatoria se deberá incorporar las recomendaciones y buenas prácticas sugeridas por el CSIRT de Gobierno.

En tanto no se disponga de una legislación para el sector público, a efectos de las políticas en las que se integre el concepto de “trabajo a distancia” o “teletrabajo” se asumirán las siguientes definiciones, basadas en la Ley N°21.220:

Trabajo a distancia:

Es trabajo a distancia aquel en el que el trabajador presta sus servicios, total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos, instalaciones o faenas de la empresa.

Teletrabajo:

Se denominará teletrabajo si los servicios son prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones o si tales servicios deben reportarse mediante estos medios.