**Modelo de Política de Seguridad de la Información para VisitasDomiciliarias.Net**

Versión 1

Marzo 2013

**TERMINOS Y CONDICIONES DE USO**

El uso de este “Modelo de Política de Seguridad de la Información” llamada también “Política Modelo”) se rige por los términos y condiciones que a continuación se mencionan. Quien acceda a esta “Política Modelo” conoce, entiende y acepta los términos relativos a su utilización y que a continuación se detallan:

La presente “Política Modelo” fue aprobada por la GERENCIA GENERAL de VISITAS DOMICILIARIAS.NET S.A.S, con el objeto de facilitar a los funcionarios su propia Política de Seguridad de la Información.

El texto de la “Política Modelo” fue redactado directamente por los funcionarios de la Compañía tomando como base las políticas de seguridad existentes, especialmente para el manejo de información-.

Queda expresamente prohibido su uso para fines comerciales.

Esta política puede ser utilizada siempre y cuando se solicite autorización y sea manejada para compañías similares de servicios.

**1. Introducción**

Teniendo en cuenta las variables de seguridad que afectan la contratación, vinculación o sostenimiento de personal en las diferentes compañías a nivel nacional, existe la necesidad de crear este modelo de seguridad que permite garantizar que la información que se recoge, se consigna a las empresas usuarias es veráz.

**1.1. Alcance**

La presente Política de Seguridad se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos.

Debe ser conocida y cumplida por todas los empleados de la Compañía, independiente del nivel jerárquico

**2. Términos y Definiciones**

A los efectos de este documento se aplican las siguientes definiciones:

**2.1. Seguridad de la Información**

La seguridad de la información se entiende como la preservación de las siguientes características:

* **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellaspersonas autorizadas a tener acceso a la misma.
* **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos deprocesamiento.
* **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a lainformación y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

* **Autenticidad**: busca asegurar la validez de la información en tiempo, forma ydistribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
* **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registradospara su control posterior.
* **Protección a la duplicación**: consiste en asegurar que una transacción sólo se realizauna vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
* **No repudio**: se refiere a evitar que una entidad que haya enviado o recibidoinformación alegue ante terceros que no la envió o recibió.
* **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones odisposiciones a las que está sujeto el Organismo.
* **Confiabilidad de la Información**: es decir, que la información generada sea adecuadapara sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

* **Información**: Se refiere a toda comunicación o representación de conocimiento comodatos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
* **Sistema de Información**: Se refiere a un conjunto independiente de recursos deinformación organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
* **Tecnología de la Información**: Se refiere al hardware y software operados por elOrganismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

**2.2. Evaluación de Riesgos**

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

**2.3. Administración de Riesgos**

Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

**2.4. Responsable de Seguridad Informática**

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

**2.5. Incidente de Seguridad**

Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

**3. Política de Seguridad de la Información**

***Generalidades***

La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades del Organismo y de los titulares de Unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

***Objetivo***

Proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

Mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

***Alcance***

Esta Política se aplica en todo el ámbito del Organismo, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

***Responsabilidad***

La Gerencia General, La Coordinadora Administrativa y en General todos los funcionarios de Visitas Domiciliarias.Net, son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo para aquellos que llegasen a tener personal a cargo.

La Gerencia General será la única en aprobar esta Política y es responsable de la autorización de sus modificaciones.

Los **Propietarios de la Información** **(1)** son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El **Responsable del Área de Recursos Humanos** o quién desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad.

El **Responsable del Área Informática** cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del Organismo. Por otra parte tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases. (En nuestro caso Outsorcing)

El **Responsable del Área Legal** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación del Organismo con sus empleados y con terceros. Asimismo, asesorará en materia legal al Organismo, en lo que se refiere a la seguridad de la información.

Los **usuarios de la información y de los sistemas** utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

La **Unidad de Auditoría Interna**, o en su defecto quien sea propuesto por el Comité de Seguridad de la Información es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan (Ver 12. Cumplimiento).

1 Clientes

**Política**

**3.1. Aspectos Generales**

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

* **Organización de la Seguridad**

Orientado a administrar la seguridad de la información dentro de la Compañía y establecer un marco gerencial para controlar su implementación.

* **Clasificación y Control de Activos**

Destinado a mantener una adecuada protección de los activos de la Compañía

* **Seguridad del Personal**

Orientado a reducir los riesgos de error humano, comisión de ilícitos contra la Compañía o uso inadecuado de instalaciones.

* **Gestión de las Comunicaciones y las Operaciones**

Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

* **Control de Acceso**

Orientado a controlar el acceso lógico a la información.

* **Desarrollo y Mantenimiento de los Sistemas**

Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.

* **Administración de la Continuidad de las Actividades de la Compañía**

Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

* **Cumplimiento**

Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

A fin de asegurar la implementación de las medidas de seguridad comprendidas en esta Política, Visitas Domiciliarias.net identificará los recursos necesarios e indicará formalmente las partidas presupuestarias correspondientes, como anexo a la presente Política. Lo expresado anteriormente no implicará necesariamente la asignación de partidas presupuestarias adicionales.

**3.2. Sanciones Previstas por Incumplimiento**

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido (Ver 12.4. Sanciones Previstas por Incumplimiento).

**4. Organización de la Seguridad**

**Generalidades**

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la Compañía.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Asimismo, se contemplará la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Por otro lado debe tenerse en cuenta que ciertas actividades de la Compañía, pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

***Objetivo***

Administrar la seguridad de la información dentro de la Compañía y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la Compañía.

***Alcance***

Esta Política se aplica a todos los recursos del Organismo y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

***Responsabilidad***

La Directora Administrativa será la responsable del cumplimiento de esta política.

El Comité de Seguridad (en desarrollo) de la Información tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante la Gerencia General , el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la proposición de asignación de funciones para su personal contratista y directo

El Responsable de Seguridad Informática asistirá al personal del Organismo en materia de seguridad de la información y coordinará la interacción con Organismos especializados. Asimismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información del Organismo y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

***Política***

**4.1. Infraestructura de la Seguridad de la Información**

**4.1.1. Comité de Seguridad de la Información**

La seguridad de la información es una responsabilidad de la Compañía compartida por todas los demás funcionarios de esta, junto con la Directora Administrativa quien cumplirá la función de impulsar la implementación de la presente Política.

Actualmente nos encontramos en la creación del comité de seguridad, el cual tendrá entre sus funciones:

* Revisar y proponer a la máxima autoridad de la Compañía para su aprobación, la Política y las funciones generales en materia de seguridad de la información.
* Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
* Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.

Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.

* Garantizar que la seguridad sea parte del proceso de planificación de la información.
* Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
* Promover la difusión y apoyo a la seguridad de la información dentro del Organismo.
* Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información del Organismo frente a interrupciones imprevistas.

**5. Clasificación y Control de Activos**

***Generalidades***

El Organismo debe tener un acabado conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

* Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.
* Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.
* Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.
* Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para el Organismo.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

***Objetivo***

Garantizar que los activos de información reciban un apropiado nivel de protección.

Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

***Alcance***

Esta Política se aplica a toda la información administrada en el Organismo, cualquiera sea el soporte en que se encuentre.

***Responsabilidad***

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

***Política***

**5.1. Inventario de activos**

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de seis meses.

El encargado de elaborar el inventario y mantenerlo actualizado.

**5.3. Rotulado de la Información**

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información; este control y rotulo de la información estará a cargo de la Dirección Administrativa.

**6. Seguridad del Personal**

***Generalidades***

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

***Objetivo***

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad del Organismo en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

***Alcance***

Esta Política se aplica a todo el personal del Organismo, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito del Organismo.

***Responsabilidad***

El Responsable del Área de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

***Política***

1. **Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos**

**6.1.1. Incorporación de la Seguridad en los Puestos de Trabajo**

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

**6.1.2. Control y Política del Personal**

Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que a tal efecto.

**6.1.3. Compromiso de Confidencialidad**

Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de revista, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del Organismo. La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos u otra competente.

Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

Se desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre:

1. Suscripción inicial del Compromiso por parte de la totalidad del personal.
2. Revisión del contenido del Compromiso cada seis meses

**6.1.4. Términos y Condiciones de Empleo**

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede del Organismo y del horario normal de trabajo.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

**6.2. Capacitación del Usuario**

1. **Formación y Capacitación en Materia de Seguridad de la Información**

Todos los empleados de la Compañía y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en esta, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

**6.3.5. Procesos Disciplinarios**

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Publica Nacional, para los empleados que violen la Política, Normas y Procedimientos de Seguridad de la Compañía.

***Política***

**7.1. Perímetro de Seguridad Física**

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor del Edificio en donde se encuentran las oficinas y de las instalaciones de procesamiento de información.

La Compañía utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidas por el Responsable del Área Informática con el asesoramiento del Responsable de Seguridad Informática, de acuerdo a la evaluación de riesgos efectuada.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

1. Definir y documentar claramente el perímetro de seguridad.

Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control, vallas, alarmas, cerraduras, etc.

1. Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán los siguientes medios alternativos de control de acceso físico al área o edificio). El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.
2. Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.
3. Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

El Responsable de Seguridad Informática llevará un registro actualizado de los sitios protegidos, indicando:

1. Identificación del Edificio y Área.
2. Principales elementos a proteger.
3. Medidas de protección física.

**7.2. Controles de Acceso Físico**

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad Informática del Edificio Siglo XXI junto con el Responsable del Área Informática, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

1. Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
2. Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán los siguientes controles de autenticación para autorizar y validar todos los accesos:(por ejemplo: personal de guardia con listado de personas habilitadas o por tarjeta magnética o inteligente y número de identificación personal Se mantendrá un registro protegido para permitir auditar todos los accesos.
3. Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.
4. Revisar y actualizar cada 6 meses) los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable de la Unidad Organizativa de la que dependa.
5. Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

Página 34