Políticas, procedimientos y guías de Seguridad de la Información

INTRODUCCIÓN

Toda persona que deba tomar decisiones que involucren temas de Seguridad de la Información, deberá orientarse a cumplir con los objetivos establecidos en la presente política.

El documento elaborado integra aspectos de control que se consideran elementales si se aspira a tener un grado razonable de seguridad en cuanto al acceso y protección de la información.

Debe tenerse presente que la A.N.V. es una institución cuya creación es reciente y se encuentra en etapa de desarrollo en varias de sus áreas, es por ello, que algunos de los conceptos que se tratan en las presentes políticas no han sido todavía implementados, no obstante lo cual, se incorporan como una aspiración a cumplir cuando el grado de madurez institucional lo permita.

CONTENIDO

Conceptos iniciales

La información es un activo esencial de la Agencia Nacional de Vivienda (A.N.V.). Toda la información generada, tanto por computadoras, manualmente o hablada, es propiedad de la A.N.V.

La Dirección del Organismo reconoce la importancia de identificar y proteger los activos de información del Organismo. Para ello, evitará la destrucción, divulgación, modificación y utilización no autorizada de toda información, comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.
La Dirección del Organismo declara el cumplimiento con la normativa y legislación vigente en relación con aspectos de seguridad de la información.

Para asegurar que los objetivos del negocio y la confianza del público sean mantenidos, todos los funcionarios tendrán la responsabilidad de proteger la información del acceso no autorizado, así como también de toda difusión, modificación o destrucción accidental o intencional originados en intereses ajenos a la Institución.

La Alta Dirección es responsable de la seguridad de la información y deberá implementar controles internos diseñados para salvaguardar los activos de la compañía. Es obligación de la Alta Dirección asegurar que todo el personal incluso quienes se vinculen o contraten temporalmente, entiendan y cumplan las políticas de seguridad de la información.

La Alta Dirección tiene la responsabilidad de administrar la información, el personal y los activos relevantes a las operaciones del negocio, así como de monitorear el uso de los activos de la A.N.V.

Definición De Políticas De Seguridad De La Información

Las políticas son instructivos que indican un predeterminado curso de acción, una manera de manejar situaciones o problemas. Son declaraciones generales que proveen una guía a los empleados que deban tomar decisiones.

Las políticas se distinguen de las guías de acción por ser mandatorias. Como su cumplimiento es requerido, usan términos definitivos como "deberá", en vez de "debería". No recomiendan o sugieren, sino que exigen su acatamiento.

Las políticas no son procedimientos, aunque en ambos casos se requiera estricto cumplimiento. A diferencia de los procedimientos, las políticas provén instrucciones generales, no métodos específicos para hacer las cosas.

Las políticas están hechas para perdurar, aunque pueden ser revisadas periódicamente de acuerdo a necesidades organizacionales.

Los objetivos de las Políticas de Seguridad de la Información son:

- Proteger la información del negocio, evitando el dolo y la pérdida de información.
- Desarrollar un proceso de evaluación y tratamiento de los riesgos de seguridad. De acuerdo a su resultado implementar las acciones correctivas y preventivas correspondientes, así como elaborar y actualizar el plan de acción.
- Asegurar la implementación de controles internos
- Coordinar actividades de grupos internos y externos a la organización.
- Cumplir con los requisitos del servicio, legales o reglamentarios y las obligaciones contractuales de seguridad.
- Clasificar y proteger la información de acuerdo a la normativa vigente y a los criterios de valoración en relación a la importancia que posee para el Organismo.
- Establecer que todo el personal es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas de acuerdo a los procedimientos correspondientes.
- Establecer los medios necesarios para garantizar la continuidad de las operaciones del Organismo.

Capítulo 1. Organización

Introducción

Objetivo – Generar el marco organizativo necesario para el manejo de la Seguridad de la Información. Definir y asignar roles y responsabilidades, y coordinar la implementación de la Seguridad.

Definiciones:

- **Seguridad de la Información –** Se define como la preservación de la *Confidencialidad*, *Integridad* y *Disponibilidad* de la Información.
- **Confidencialidad –** La información es accesible sólo para usuarios autorizados.
- **Integridad –** La información y sus métodos de procesamientos son exactos.
- **Disponibilidad –** Los usuarios autorizados tienen acceso a la información y los activos asociados cuando lo requieren.

Políticas

1.1. Infraestructura

1.1.1. **Alta Dirección –** Está constituida por el Directorio de la A.N.V. y la Gerencia General.

1.1.2. **Comité de Seguridad de la Información –** Es un comité compuesto por representantes de tecnología, delegado de administración, auditoría, legales, y el oficial de seguridad.

1.1.3. **Equipo de Seguridad de Informática –** Lo integran el personal de tecnología.

1.1.4. **Oficial de Seguridad Informática–** Se refiere a un funcionario de sólidos conocimientos en el área informática y de seguridad, que pueda aportar una visión tecnológica frente a los constantes cambios.

1.1.5. **Propietario –** Son los usuarios autorizados, encargados del mantenimiento de la información.

El Propietario de la Información deberá ser el responsable de definir el acceso a los datos y deberá determinar los controles que serán aplicados a la información.

1.1.6. **Auditoria –** La Auditoria es grupo independiente al área de tecnología que realiza revisiones del cumplimiento de las normas y políticas de seguridad de la organización.

1.2. Definición de Roles y Responsabilidades

1.2.1. **Alta Dirección** – Designa los integrantes del Comité de Seguridad y es la responsable final de la seguridad de la información manejada en la Institución.

1.2.2. **Comité de Seguridad de la Información –** Tiene como sus responsabilidades:

1.2.2.1. Revisar y aprobar las políticas de seguridad de la información al máximo nivel ejecutivo.

1.2.2.2. Mantener una clara visión de la Seguridad de Información integrada con el negocio.

1.2.2.3. Controlar el cumplimiento de las directivas aprobadas con el apoyo del oficial de seguridad, y monitorear los cambios significativos en la exposición de los activos de información a las principales amenazas.

1.2.2.4. Autorizar cualquier cambio que afecte la Seguridad de la Información.

1.2.3. **Equipo de Seguridad de la Información**

1.2.3.1. Implementar las metodologías y procedimientos específicos para la Seguridad de la Información aprobados por el Comité de Seguridad, asegurando que las mismas se cumplan.

1.2.3.2. Evaluar, aprobar e informar sobre la instalación de cualquier tipo de sistema que involucre a la Seguridad de la Información a todo nivel. Por ejemplo dispositivos de seguridad de red perimetral, Firewalls, IDS, Sistemas Antivirus etc.

1.2.3.3. Asegurar que la Seguridad sea parte del Proceso de planificación en todos los temas concernientes a la Información y sugerir mejoras en caso de detectarse debilidades.

1.2.3.4. Examinar los incidentes de Seguridad de la Información.

1.2.4. **Oficial de Seguridad de la Información**– Tiene como sus responsabilidades:

1.2.4.1. Supervisión de las operaciones y manejo diario de los temas relacionados con la Seguridad de la Información.

1.2.4.2. Presentar al Equipo de Seguridad de la Información iniciativas tendientes a la mejora de la Seguridad de la Información.

1.2.4.3. Coordinar estrategias de desarrollo e implementación de seguridad con proveedores y consultores externos.

1.2.4.4. Promover soluciones y mejoras y colaborar en la toma de decisiones atinentes a la Seguridad de la Información.

1.2.4.5. Sugerir los cursos y seminarios de Seguridad para los usuarios de la A.N.V.

1.2.4.6. Analizar los incidentes de seguridad

1.2.5. **Propietario** – Su rol es definir el nivel de confidencialidad, integridad y disponibilidad de los activos, indicando cuales deben ser protegidos y quienes tienen acceso a los mismos.

1.2.6. **Auditoria** – Sus funciones son:

1.2.6.1. Realizar evaluaciones sobre la Seguridad de la Información e informar a la Alta Dirección y al Comité de Seguridad sobre el cumplimiento de las políticas y sobre los riesgos detectados.

1.2.7. **Usuarios de los recursos informáticos de la A.N.V.** – Sus funciones son:

1.2.7.1. Es obligación de los funcionarios y quienes accedan temporalmente o circunstancialmente a los recursos informáticos de la A.N.V., conocer y respetas las políticas incluidas en el presente documento.

Capítulo 2. Conexión a Internet

Introducción

Objetivo – Asegurar el buen uso de los recursos de acceso a Internet.

Alcance – Directores, personal ejecutivo, empleados, contratistas, consultores, empleados temporales y pasantes que accedan a, o desde Internet, a través de los recursos informáticos y/o la infraestructura de comunicaciones de la A.N.V.

Introducción – Se brindará acceso a Internet de forma directa (http) o mediante el Correo Electrónico a quienes tengan legítima necesidad de acceso, debido a la función que desempeñan.

Requisitos previos – Toda persona vinculada a la A.N.V. a quien se le otorgue la posibilidad de acceder a internet deberá respetar los aspectos de seguridad incluidos en el presente documento y su uso solo deberá responder a necesidades legítimas.

Riesgos involucrados – Pérdidas económicas por fraudes debidos al uso ilegítimo de información, aumento de costos operativos por manejo inadecuado de los recursos, degradación de los recursos tecnológicos, inseguridad en la operación, pérdida de reputación, demandas legales derivadas de divulgación de información.

Políticas

2.1. Forma de Acceso

2.1.1. **Acceso –** Accederán a Internet los usuarios debidamente autorizados por la Gerencia correspondiente y por motivos del negocio.

2.1.2. **Forma de Acceso** – La única forma de acceso a Internet deberá ser la proporcionada por la A.N.V., quedando prohibida la utilización de módems o cualquier otro mecanismo de conexión.

2.1.3. **Protocolos** – Los protocolos habilitados para el acceso a Internet deberán ser HTTP, HTTPS, SMTP, NTP y DNS, quedando sujeta a discreción del Comité de Seguridad de la Información la habilitación futura de otros protocolos, únicamente por motivos del negocio, a usuarios autorizados, con restricción horaria, y que no incluyan los requeridos o mencionados en el punto 2.1.4 de esta Política de Seguridad. El protocolo FTP se deberá habilitar solamente a usuarios autorizados por el Comité de Seguridad y con restricción horaria.

2.1.4. **Prohibiciones** – Deberá evitarse la utilización con fines personales de Web Mail, Chats y cualquier forma de transferencia de archivos vía HTTP, así como servicios de Mensajería Instantánea o programas Peer to Peer que no estén expresamente autorizados por el Comité de Seguridad. Se deberá prohibir el uso del protocolo POP3.

2.2. Integridad de la Información

2.2.1. **Control de Virus –** Todos los archivos bajados de Internet deberán ser analizados, previo a su uso, con la versión actualizada del Sistema de Detección de Virus provisto por TI. Si se bajara software de proveedores no confiables, este deberá ser testeado en máquinas desconectadas de la red antes de su puesta en producción. Los archivos bajados de Internet deberán ser desencriptados y descomprimidos antes de realizarles el análisis de virus.

2.2.2. **Descarga de Software** – Los usuarios no deberán instalar en computadoras de la A.N.V. software bajado de Internet, o de cualquier otra procedencia, sin el consentimiento escrito de la Gerencia de TI. En caso que los usuarios soliciten algún programa en particular, ésta solicitud deberá ser evaluada por la Gerencia de TI, quien determinará si el software cumple con requisitos legales, de funcionamiento y de seguridad.

2.2.3. **Actualizaciones Automáticas** – Los usuarios no deberán actualizar software automáticamente, incluso aquel correctamente licenciado, a menos que sean autorizados por escrito por la Gerencia de TI.

2.2.4. **Adjuntos en Correo Electrónico** – Los usuarios no deberán abrir adjuntos de correo electrónico a menos que sean enviados por una fuente conocida y confiable. Los adjuntos deberán ser analizados con la última versión del Sistema de Detección de Virus aprobado por TI, antes de ser abiertos.

2.3. Confidencialidad de la Información

2.3.1. **Intercambio de Información –** Ni el Software, ni la documentación, ni otro tipo de información interna de la A.N.V. deberá ser vendida o transferida a un tercero, salvo por motivos

del negocio y con autorización escrita del propietario del activo. Para transferir Software o Información de la A.N.V. a terceros, se deberá firmar previamente un acuerdo de confidencialidad que especifique los términos de la transferencia y la forma que los datos serán manejados y protegidos por esa tercera parte.

2.3.2. **Publicación de Información** – Los usuarios no deberán publicar información no encriptada perteneciente a la A.N.V. en sitios de Internet de acceso público que soporten el uso de FTP de forma anónima u otro tipo de servicio de acceso, a menos que sea autorizado por escrito por el propietario de la Información y aprobado por el Comité de Seguridad.

2.3.3. **Interceptación de Mensajes** – No se deberá enviar información propiedad de la A.N.V. a través de Internet a menos que sea estrictamente necesario por motivos de negocio. Deberá evaluarse la necesidad de encriptarse los datos transmitidos a través de Internet.

2.3.4. **Seguridad de Parámetros –** No se deberán enviar por Internet, en formato de texto plano, números de tarjetas de crédito, números de tarjetas de llamadas telefónicas, contraseñas de acceso o cualquier información que pueda utilizarse para ganar acceso a cualquier tipo de bienes o servicios.

2.4. Representación Pública

2.4.1. **Representación Externa –** No deberán colocarse mensajes en listas de correo u otro tipo de listas de distribución o comunicación vía Internet, a menos que sea expresamente autorizado por el Gerente de Recursos Humanos o el Departamento de Comunicación de la A.N.V. Los usuarios autorizados deberán indicar su afiliación a la A.N.V. cuando dejen mensajes en cualquiera de las listas mencionadas anteriormente. Esta indicación deberá explicitarse mediante la inclusión del nombre de la Agencia de forma directa o mediante la inclusión de la dirección de correo electrónico. A menos que el usuario sea designado como vocero oficial de la A.N.V., deberá indicar claramente que las opiniones vertidas son enteramente propias y no involucran a la A.N.V. Están prohibidas las referencias a temas políticos y la aprobación o consentimiento de productos o servicios, a menos que el usuario sea autorizado expresamente por Directorio.

2.4.2. **Comportamiento** – No deberán enviarse amenazas en contra de otros usuarios u organizaciones, ni que puedan hostigar, molestar, incomodar o alarmar a otras personas mientras se explicite la afiliación a la A.N.V. en mensajes o publicaciones en Internet.

2.4.3. **Eliminación de Mensajes** – Los mensajes enviados a grupos de discusión o foros públicos en Internet que indiquen afiliación explícita a la A.N.V. deberán ser eliminados si la Dirección estima que son inconsistentes con los intereses del negocio o alguna política existente. Esto incluye manifestaciones políticas, religiosas, maldiciones u otro tipo de lenguaje inapropiado, o que puedan considerarse discriminantes por raza, credo, color, edad, sexo, capacidades físicas u orientación sexual. Los usuarios responsables del mensaje inapropiado deberán ser informados de la decisión y tendrán la oportunidad de eliminarlos ellos mismos.

2.4.4. **Divulgación de Información Interna** – Los usuarios no deberán divulgar información interna de la A.N.V. que pueda afectar precios de servicios, relaciones con clientes o la imagen pública de la A.N.V., ni del país, a menos que sea expresamente permitido por el Propietario de la Información. Quedan excluidas de esta política las respuestas vía correo electrónico a preguntas específicas de clientes de la A.N.V.

2.4.5. **Divulgación Accidental** – No deberá publicarse en listas de correo, grupos de noticias, foros de discusión u otro tipo de forma de distribución de mensajes en Internet, partes aisladas de

información que puedan ser recompuestas por sujetos malintencionados y ser usadas contra la A.N.V. Se deberá evitar divulgar el nombre y/o modelo de productos de networking o computadoras utilizados por la A.N.V.

2.5. Derechos de Propiedad intelectual

2.5.1. **Copyright –** No deberán realizarse copias de software si así lo indicara la licencia del proveedor. No deberán reproducirse, renviarse, republicarse o redistribuirse documentos de texto, gráficos o cualquier tipo de material sometido a derechos de autor si no se cuenta con la autorización del autor o propietario. Cuando se utilice información bajada de Internet para integrarla en reportes internos, se deberá hacer referencia a los derechos de autor y la fuente de información.

2.6. Control de Acceso

2.6.1. **Seguridad en Equipos remotos** – Los usuarios de equipos remotos deberán acceder a la red interna de la A.N.V. mediante VPN (Virtual Private Network). Los equipos remotos que sean propiedad de la A.N.V. deberán ser monitoreados para verificar la instalación de la versión del sistema operativo aprobada por Gerencia de TI, con sus últimos parches instalados, la última versión del Sistema de Detección de Virus y el software de seguridad correctamente configurado. La administración del cliente de VPN se realizará de forma centralizada.

2.6.2. **Autenticación de usuarios remotos –** Los usuarios que establezcan una conexión en tiempo real con la A.N.V. a través de Internet o Extranet, se deberán conectar utilizando mecanismos seguros y encriptados de acceso y autenticación, siguiendo los lineamientos establecidos por el Comité de Seguridad y el Equipo de Seguridad de Información.

2.6.3. **Restricción de Acceso de Terceros** – El acceso a la LAN de la A.N.V. desde Internet o Extranet no deberá permitirse a empresas externas, contratistas, consultores, empleados temporales o personal de organizaciones externas, a menos que sea autorizado por el Comité de Seguridad, por una necesidad legítima y por cuestiones del negocio. Estos privilegios deberán otorgarse luego de realizada una evaluación de riesgos, sólo para una persona claramente identificada y por el periodo mínimo requerido, que deberá ser estipulado junto con la tarea a realizar y los privilegios solicitados en el pedido de acceso.

2.6.4. **Autenticación de Usuarios mediante el Navegador** – Los usuarios no deberán almacenar contraseñas en los navegadores o clientes de correo electrónico, ingresándolas cada vez que sean requeridas. Los navegadores utilizados en la empresa deberán permitir la aplicación de estas restricciones a través de directivas de grupo o similar.

2.6.5. **Proveedores de Acceso a Internet** – Con excepción de los usuarios autorizados, no se deberá acceder a Internet de ningún otro medio más que los provistos por la A.N.V. Toda la actividad hacia o desde Internet deberá pasar a través de Firewalls y Sistemas de Detección de Intrusos (IDS) de la A.N.V.

2.6.6. **Establecimiento de Conexiones de Red** – Los usuarios no deberán establecer conexiones a Internet o cualquier otra red externa que permita a usuarios ajenos a la A.N.V. ganar acceso a los Sistemas e información de la empresa. Dentro de estas conexiones se incluyen aquellas a sistemas de archivo multiusuario (KaZaA, IMESH), páginas de hackers, Sistemas de comercio electrónico y servidores FTP.

2.6.7. **Comercio Electrónico** – Deberá evitarse el uso de equipos, conexiones y cuentas de correo electrónico de la A.N.V. para realizar transacciones comerciales electrónicas (compras de bienes o servicios), sean estas personales o para la A.N.V., salvo expresa autorización del Gerente correspondiente.

2.7. Uso Personal

2.7.1. **Uso Personal –** Los usuarios con acceso permitido a Internet no deberán navegar con fines personales. No está autorizado, en horario de trabajo o fuera de éste, la utilización de recursos de la A.N.V. con fines de lucro personal, actividades recreativas, como juegos, participación en listas de noticias, redes sociales, u otra que no se corresponda con la actividad del negocio.

2.7.2. **Acceso a Sitios con contenido Ofensivo** – La A.N.V. no se hace responsable por el contenido al que los usuarios pudieran acceder a través de Internet. Cuando un usuario se conecte a un sitio Web de contenido objetable, deberá navegar hacia otro sitio o terminar de inmediato la sesión. Los usuarios que descubran un sitio que contenga material de sexo explicito, racista, sexista, violencia, o cualquier otro tipo de contenido ofensivo, deberán desconectarse del sitio de forma inmediata.

2.7.3. **Bloqueo de Sitios y Tipos de Contenido** – La posibilidad lógica de conexión a un sitio no implica que los usuarios tengan permitido el acceso al mismo. La A.N.V. podrá restringir o bloquear el acceso a sitios de Internet que considere ofensivos o potencialmente dañinos para el funcionamiento de sus recursos informáticos.

2.7.4. **Descarga de Archivos** – La A.N.V. podrá monitorear, restringir y/o bloquear la descarga de archivos que puedan causar la degradación de los recursos de red cuando lo considere necesario. Este tipo de archivos puede incluir gráficos, películas o música.

2.8. Privacidad

2.8.1. **Protección de la Información –** A menos que utilicen algún tipo de encriptación avalada por el Comité de Seguridad, los usuarios deberán evaluar los riesgos de enviar información por Internet.

2.8.2. **Registro de Accesos** – La A.N.V. podrá registrar los sitios visitados por los usuarios, archivos bajados, tiempo empleado en Internet y toda la información relativa a estas actividades. Los Gerentes de cada departamento o división podrán solicitar un reporte de esta información y la utilizarán para determinar el tipo de uso que los empleados le dan a la conexión a Internet con relación a la actividad propia de sus departamentos.

2.9. Correo Electrónico

2.9.1. **Derecho de Propiedad** – El Correo Institucional es una herramienta y un recurso propiedad de la A.N.V. y entregado en tal carácter al trabajador. La A.N.V. deberá promover el uso con fines comerciales del correo electrónico como una herramienta de mejora de la productividad. El correo debe ser utilizado exclusivamente con fines relacionados a la actividad de la A.N.V., y su contenido, a menos que terceros reclamen con evidente razón el derecho de propiedad intelectual, serán considerados de acuerdo a la relación de dependencia y a las leyes y normativas vigentes al respecto.

2.9.2. **Identidad de Usuarios** – Los usuarios no deberán falsear, tergiversar, suprimir o remplazar la identidad de otro usuario de Correo Electrónico, perteneciente o no a la A.N.V. El nombre, la dirección de correo electrónico, la empresa a la que pertenece y cualquier otra información relativa, debe reflejar al usuario que origina un mensaje de correo electrónico. No deberán enviarse mensajes anónimos por Correo Electrónico.

2.9.3. **Certificado Digital** – Los usuarios que a criterio del Comité de Seguridad lo requieran, deberán enviar sus mensajes utilizando certificados digitales emitidos por una Autoridad Certificadora (CA) aprobadas por dicho comité.

2.9.4. **Derecho de Privacidad** – Los usuarios no deberán interceptar, divulgar, o colaborar con otros usuarios en la interceptación o divulgación de correo electrónico. La A.N.V. se compromete a respetar el derecho a la privacidad de sus empleados, por lo que se responsabiliza por el mantenimiento y protección de sus correos electrónicos. La A.N.V. se reserva el derecho de utilizar Sistemas de Monitoreo, Sistemas de logueo de mensajes y otras herramientas de administración de correo electrónico.

2.9.5. **Adéndum en Correo Electrónico saliente** – Un pie de página autorizado por la A.N.V. deberá ser automáticamente agregado al final de todos los mensajes salientes originados en la misma.

2.9.6. **Reenvío de Mensajes** – Los empleados de A.N.V. no deberán reenviar correo electrónico a ninguna dirección externa a la red de la Agencia a menos que el propietario de la información o quien dio origen a la misma lo avalen, salvo que la información sea de clara naturaleza pública. En caso de no haber sido avalado por el propietario de la información, la responsabilidad del correo recaerá sobre la persona que lo reenvía.

2.9.7. **Respaldo de Información** – Si un mensaje de correo electrónico contiene información relevante a los fines comerciales o puede tener valor como respaldo de una decisión en la gestión de la A.N.V., deberá ser guardado para su futura referencia. Los usuarios deberán mover toda información considerada importante a documentos de texto, bases de datos u otro tipo de archivos para su mejor preservación. Las carpetas de los Sistemas de Correo Electrónico no deberán ser usadas para archivar información importante.

2.9.8. **Correo electrónico no deseado** – Los usuarios no deberán utilizar los Sistemas informáticos de la A.N.V. para la transmisión de correo electrónico masivo, avisos o mensajes comerciales que no sean del interés o solicitud de los destinatarios.
Esto abarca promociones, cadenas de mensajes, cadenas tipo pirámide o cualquier otro mensaje de esta clase. Cuando los usuarios reciban correo no deseado (SPAM), deberán dar aviso al Administrador de Correo de la A.N.V. para que él tome las medidas correspondientes, sin responder directamente al remitente.

2.9.9. **Información de terceros -** Los correos electrónicos que contengan información sensitiva sobre uno o más clientes deberán enviarse encriptados.

2.10. Reporte de Incidentes de Seguridad

2.10.1. **Proceso de Notificación –** Si cualquier tipo de información sensitiva de la A.N.V. se pierde, es divulgada a personas no autorizadas, o se sospecha que pudiera haber sido perdida o divulgada a personas no autorizadas, se deberá notificar de inmediato al Equipo de Seguridad

de la Información. Si cualquier tipo de uso no autorizado de los Sistemas de Información de la A.N.V. ocurre o se sospecha que ocurre, se deberá notificar de inmediato al Equipo de Seguridad de la Información. Siempre que una contraseña o cualquier otro tipo de mecanismo de acceso sean perdidos, robado o divulgado, o se sospeche de ser perdido, robado o divulgado, se deberá notificar de inmediato al Equipo de Seguridad de la Información. Cualquier tipo de comportamiento inusual de los Sistemas, como pérdida de archivos, caídas frecuentes, o mensajes perdidos, deberán ser reportados de forma inmediata a la División Sistemas. Los detalles específicos de los problemas de seguridad no deberán ser difundidos dentro de la organización, salvo a efectos de resolver un problema de seguridad.

2.10.2. **Reportes Falsos** – Los usuarios que reciban información acerca de vulnerabilidades del sistema informático deberán reenviar la información al Equipo de Seguridad de la Información, evitando notificar a otros usuarios.

2.10.3. **Control de Pruebas** – Los usuarios no deberán testear o probar los mecanismos de seguridad de la A.N.V. o de sitios de Internet de terceros sin consentimiento escrito del Equipo de Seguridad de la Información. No deberán instalarse, salvo autorización del Comité de Seguridad, herramientas de detección de vulnerabilidades, o herramientas que comprometan los mecanismos de seguridad de los Sistemas de la Agencia.

Capítulo 3. Seguridad de Redes

Introducción

Alcance – Acceso a Internet, conexiones entre zonas e instalación física.

Objetivo – Asegurar las zonas definidas en la Red de acuerdo a la valoración de los activos que contienen, tanto tecnológica como físicamente. Definir la seguridad en el perímetro de acceso y la comunicación inter-zonal.

Riesgos involucrados – Pérdidas económicas por fraudes debidos al uso ilegítimo de información, aumento de costos operativos por manejo inadecuado de los recursos, degradación de los recursos tecnológicos, inseguridad en la operación, pérdida de reputación, demandas legales derivadas de divulgación de información.

Políticas

3.1. Definiciones

3.1.1. **Zonas Inseguras –** Redes no controladas ni administradas por la A.N.V., como Internet (Red Pública) o Extranet. Dentro de estas zonas se incluyen las redes inalámbricas (wireless), mientras esta tecnología no permite un adecuado control. Los usuarios remotos que se conectan a la LAN por VPN no son considerados usuarios de la Zona Insegura.

3.1.2. **Zonas Semi-seguras (DMZ) –** El segmento controlado y administrado por la A.N.V., accesible desde la Zona Insegura.

3.1.3. **Zona Controlada –** Es el segmento controlado y administrado por la A.N.V., al cual no acceden usuarios de la Zona Insegura. El acceso a zonas controladas requiere encontrarse físicamente dentro de la Agencia, con adecuado control de acceso y utilizar tecnología de cableado como Ethernet o Fibra Óptica.

3.1.4. **Zonas Seguras o Muy Seguras –** Segmentos de red que cumplen los requisitos de las Zonas Controladas y están ubicados en un área de acceso físico restringido a administradores de Sistemas. Estos segmentos se conectan a Zonas Semi-seguras y Controladas a través de, por lo menos un enclave. Se sugieren dispositivos de Firewall con servicios de Detección de Intrusos, Antivirus en línea y que admitan la autenticación de usuarios o aplicaciones por métodos criptográficos.

3.1.5. **Extranet -** Redes de socios comerciales, clientes, proveedores, accionistas, bancos y agencias de gobierno y crédito, consideradas inseguras por falta de control físico y lógico.

3.2. Conexiones

3.2.1. **Conexión Externa** – La conexión desde Zonas Controladas a Internet se deberá realizar a través de dispositivos de Seguridad definidos por la A.N.V. y ubicados entre la Zona Semi-Segura y la Insegura. No está permitida la conexión directa de equipos de la LAN a cualquier red externa (Internet o Extranet).

3.2.2. **VPN** – Solamente usuarios autorizados deberán conectarse por VPN a la LAN de la A.N.V. La instalación y configuración del Software Cliente de VPN deberá realizarse bajo la supervisión del Equipo de Seguridad de la Información.

3.2.3. **Autenticación de Usuarios** – Los usuarios que establezcan una conexión en tiempo real con la A.N.V., a través de Internet o Extranet, se deberán conectar utilizando mecanismos seguros y encriptados de acceso y autenticación, siguiendo los lineamientos establecidos por el Comité de Seguridad y el Equipo de Seguridad de Información.

3.2.4. **Ruteo** – Las conexiones a Internet desde la LAN serán ruteadas a través de Proxy Servers.

3.2.5. **Seguridad** – Todas las conexiones de la LAN y la DMZ hacia y desde Internet deberán pasar por un Firewall y un sistema de detección de Intrusos (IDS).

3.3. Seguridad del Perímetro

3.3.1. **Conexión a Internet** – La conexión a Internet se realizará a través de los dispositivos de Seguridad definidos por la A.N.V. No está permitida la conexión directa de equipos de la LAN a Internet.

3.3.2. **Filtros de Red** –La Seguridad Perimetral deberá basarse en un Router de Acceso (Access Router), primer punto de defensa contra el acceso malintencionado desde la Zona Insegura, que deberá denegar toda conexión que no sea establecida mediante los protocolos autorizados por el Comité de Seguridad.

3.3.3. **Firewalls** – Las diferentes Zonas se deberán conectar a través Firewalls que, mediante reglas determinadas por el Equipo de Seguridad de la Información y aprobadas por el Comité de Seguridad, filtrarán sobre la combinación de origen, destino, usuario y servicio, las comunicaciones inter-zonales.

3.3.4. **Detectores – Prevención de Intrusos (IDS-IPS) de Red** – El acceso a la LAN desde la Zona Insegura deberá ser controlado por Sistemas de detección de intrusos, que deberán detectar, bloquear, registrar y alertar sobre cualquier tipo de intento de intrusión.

3.4. Segmentación

3.4.1. **Seguridad en Sub Redes** – Todas las redes internas que contengan información sensitiva, deberán residir en un segmento (Sub Red) seguro. La clasificación, en términos de seguridad de las distintas Sub Redes que deberán ser protegidas, será determinada por el Equipo de Seguridad de la Información y supervisada por el Comité de Seguridad, sobre la base de Análisis de Riesgos efectuados periódicamente.

3.4.2. **Acceso denegado por Defecto** – Toda ruta de conexión o servicio que no esté específicamente permitido por las políticas de acceso, deberá ser bloqueado por el Firewall. La lista de accesos y servicios permitidos para cada segmento deberá ser documentada y distribuida por el Equipo de Seguridad de la Información a los Administradores de Sistemas y ser reflejados por las reglas de los Firewalls.

3.4.3. **Acceso a los Dispositivos de Seguridad** – Los privilegios para modificar la funcionalidad, conectividad y servicios soportados por los Dispositivos de Seguridad (Firewalls, Routers, IDSs), deberán ser restringidos a un grupo mínimo de técnicos calificados y con conocimientos de las necesidades del negocio. Los privilegios serán otorgados por el Oficial de Seguridad quien será el Custodio de las claves con máximos privilegios sobre estos dispositivos. Estos técnicos deberán ser empleados permanentes de la A.N.V., a menos que estén debidamente autorizados por el Comité de Seguridad y sean supervisados por un técnico de la empresa nombrado por el Oficial de Seguridad. Todos los Dispositivos de Seguridad deberán tener al menos dos técnicos adecuadamente entrenados para administrarlos. Se deberán asegurar cursos periódicos, seminarios y conferencias de actualización a los técnicos especializados. Los especialistas en estos Dispositivos de Seguridad no deberán tomar su licencia anual en forma simultánea, asegurando alta disponibilidad.

3.5. DMZ

3.5.1. **Zonas Desmilitarizadas** – Los Servidores que presten servicio a usuarios externos a la A.N.V., tales como Web y de Correo, deberán estar protegidos por un Firewall y ubicarse en una zona desmilitarizada (DMZ).

3.5.2. **Conexiones Externas** – Toda conexión de entrada en tiempo real a la DMZ de la A.N.V. desde Internet, deberá pasar por un Firewall antes que los usuarios remotos tengan acceso a la Pantalla de Logon.

3.5.3. **Detectores de Intrusos** – Los dispositivos involucrados en el manejo de Información ubicados en la Zona Semi-Segura (Proxys, Web Servers, e-Commerce Servers, Servidores de Correo, etc.), deberán tener instalado un Detector de Intrusos de Servidor, configurado de acuerdo a las especificaciones dictadas por el Equipo de Seguridad de la Información y aprobadas por el Comité de Seguridad.

3.6. Conexión Extranet

3.6.1. **Extranet –** Los usuarios de Extranet deberán acceder únicamente a la DMZ de la A.N.V.

3.6.2. **Acceso a la DMZ –** El acceso desde Extranet a la DMZ deberá realizarse a través de un Firewall, mediante una conexión exclusiva, con reglas definidas para restringir el acceso solamente a aquellos usuarios designados por socios comerciales debidamente autorizados por los Propietarios de la Información y la Gerencia de TI.

3.6.3. **Autenticación –** Los usuarios de Extranet que accedan a la red de la A.N.V. se deberán conectar utilizando mecanismos seguros y encriptados de acceso y autenticación, siguiendo los lineamientos establecidos por el Comité de Seguridad y el Equipo de Seguridad de Información.

3.7. Conexión Wireless

3.7.1. **Red Inalámbrica (Wireless)** – Los dispositivos Wireless deberán considerarse pertenecientes a la Zona Insegura. Las comunicaciones provenientes desde la misma deberán pasar por un Firewall.

3.8. Tecnología

3.8.1. **Equipos Dedicados** – Las aplicaciones de Seguridad deberán correr en Sistemas Dedicados, sin otra función simultánea. Cualquier servicio o programa que no sea necesario para la función de Seguridad, deberá ser deshabilitado.

3.8.2. **Comunicación de Ataques** – Los dispositivos de Seguridad que detecten intrusiones, ataques, intentos de ataques o pruebas que indiquen posibles intentos de ataques, deberán alertar a los Técnicos que estén en condiciones de tomar acciones correctivas y al Oficial de Seguridad. Las alertas deberán ser comunicadas vía correo electrónico, o cualquier otro método que se asegure fehacientemente la entrega del mensaje de alerta.

3.8.3. **Acceso Remoto a Consolas** – Los Técnicos que sean alertados de ataques, deberán acceder a las Consolas de Firewalls e IDS para tomar las medidas correctivas, incluso si no se

encuentran físicamente dentro de la A.N.V.

3.8.4. **Logs –** Todos los cambios que se realicen a los parámetros de configuración de los Firewalls, Reglas o Rutas de Acceso deberán ser registradas en un log. Todo tipo de actividad sospechosa, indicativa de uso no autorizado o intento de compromiso de la seguridad de la Red, deberá ser registrado en un log. Los logs deberán ser revisados periódicamente por técnicos pertenecientes al Equipo de Seguridad de la Información, designados por el Oficial de Seguridad para asegurar que los equipos estén operando en forma segura.

3.8.5. **Respaldo de los Logs –** La integridad de los logs generados deberá ser protegida mediante encriptación, firmas digitales o similares. Los registros de logs deberán ser respaldados y borrados del sistema lo más rápido posible. Los respaldos serán almacenados en un lugar seguro y físicamente protegido por al menos seis meses.

3.8.6. **Actualización de los Equipos –** Los dispositivos de Seguridad de la A.N.V. deberán correr versiones actualizadas del Software de Aplicación y del Sistema Operativo. Todos los dispositivos de Seguridad deberán estar suscriptos al mantenimiento de Software y servicios de Actualización de Software que brinde el proveedor.

3.9. Seguridad Física

3.9.1. **Dispositivos de Seguridad** – Todos los dispositivos de seguridad de la A.N.V., como Firewalls, IDSs, Routers, etc., deberán alojarse en lugares protegidos en forma adecuada, accesible solo por personal autorizado y monitoreados en forma continua.

3.10. Monitoreo

3.10.1. **Fallas** – Se deberá monitorear en forma continua todos los dispositivos de red y Servidores que contienen información y procesos sensibles, buscando posibles fallas físicas (Desconexión de equipos de ruteo, errores en tarjetas de comunicaciones, capacidades excedidas, etc.).

3.10.2. **Vulnerabilidades** – Deberán ser monitoreados permanentemente los anuncios de proveedores de Software y Hardware sobre nuevas vulnerabilidades que puedan existir en cualquier dispositivo, servidor, estación de trabajo o equipo de comunicación de la red y tomarse las medidas correctivas lo más rápido posible.

3.10.3. **Vulnerabilidades de Equipos de Seguridad** – Los técnicos responsables por el mantenimiento de Firewalls, IDSs y otro tipo de dispositivos de seguridad, deberán estar suscriptos a listas de avisos sobre nuevas vulnerabilidades y tomar las medidas correctivas sugeridas, de ser necesarias.

Capítulo 4. Clasificación de la Información

Introducción

Alcance – Información bajo control de la A.N.V., incluyendo información de clientes, socios de negocios, proveedores y terceros.

Objetivo – Clasificar la información para generar una adecuada protección contra su divulgación, utilización, modificación o borrado no autorizado.

Introducción – Todo usuario que acceda a los Sistemas de Información de la A.N.V. cumple un importante rol en el manejo de la Seguridad de la Información y deberá ser responsable por la protección de la Información que se le delega.
El sistema de Clasificación de Información de la A.N.V. se basa en la normativa legal vigente y en el modelo de la Necesidad de Conocer (Need to know). Significa que la información no es divulgada a ninguna persona que no tenga una legítima y demostrable necesidad de recibir esta información.

Riesgos involucrados – Pérdidas económicas por fraudes causados por el uso indebido de información, inseguridad en la operación, pérdida de reputación tanto de la A.N.V. como del país, demandas legales derivadas de divulgación de información.

Políticas

4.1. Rótulos de Clasificación de la Información

4.1.1. **Clasificación de la Información-** La Información en poder de la A.N.V. deberá ser clasificada de acuerdo a la normativa vigente en la materia como Secreta, Reservada o Confidencial (ley 18381).

La clasificación estará a cargo de los usuarios autorizados encargados de su mantenimiento (propietarios).

4.1.2. **Uso Interno** – La Información podrá a su vez ser limitada en su uso interno, siempre que el uso indebido de la misma pueda dañar al organismo, la organización, o a sus integrantes tanto en el ámbito interno como externo.

Toda aquella información que no sea limitada en su uso interno podrá ser de libre acceso para los trabajadores de la A.N.V..

4.1.3 Etiquetado- La información será clasificada y etiquetada por parte de los propietarios como de uso interno o de libre acceso para quienes se desempeñen en la A.N.V..

Por defecto, la información será etiquetada como de Uso Interno. Por lo tanto toda información sin etiquetar será considerada de Uso Interno.

4.1.4. **Responsabilidad** – Será responsabilidad del usuario propietario de la información la clasificación y el etiquetado de la misma como de uso interno o de acceso libre.

4.2.4. **Otros aspectos** – Todo funcionario o persona que desempeñe tareas para la A.N.V., debe tomar las medidas necesarias a efectos de que:

- La etiqueta se mantenga respetando el ciclo de vida natural de la información, no pudiendo alterarse sin la autorización del propietario.

- La etiqueta esté acorde al medio que la soporta y permanezca si el medio es cambiado.

- Se conserve la categoría más restrictiva cuando se integre información de distintas categorías.

- Toda información de procedencia externa que no se distinga claramente como Pública, será etiquetada según la Política de rotulado de la A.N.V.. La persona que reciba dicha información será el responsable de asignarle una clasificación y de etiquetarla, preservando las notas de Copyright, derechos de autor, etc.

4.3. Manejo de Documentos con Terceros

4.3.1. **Acuerdos de confidencialidad** – La divulgación de información -que no sea pública- a terceros, deberá estar precedida por la firma de un acuerdo de confidencialidad.

4.3.2. **Firma de acuerdos de confidencialidad** – Los trabadores de la A.N.V. no deberán firmar acuerdos de confidencialidad provistos por terceros sin la autorización del Área Jurídica de la A.N.V..

4.4. Manejo y Transporte

4.4.1. **Almacenamiento de medios de respaldo** – Toda información sensitiva grabada en medios de respaldo y almacenada fuera de las oficinas de la A.N.V. deberá ser protegida mediante encriptación u otro medio que garantice razonablemente su seguridad.

4.4.2. **Almacenamiento local** – La información sensitiva, tanto impresa en papel como la contenida en medios de almacenamiento electrónico, deberá preservarse con los niveles de seguridad adecuados.

4.5. Destrucción y Eliminación

4.5.1. **Destrucción y Eliminación de la información** – Deberá ser destruida o eliminada cuando no sea útil a los fines del negocio. Los Propietarios de la Información deberán determinar, junto al Área Jurídica de la A.N.V. los períodos mínimos de retención de ciertos tipos de información que la legislación determine.

4.5.2. **Eliminación o mantenimiento de equipos** – Antes de enviar equipos al proveedor para su recambio, al servicio técnico, realizar su venta, donación o eliminación definitiva. La información de la A.N.V. deberá ser destruida de forma adecuada. Los discos duros o cualquier otro tipo de medio de almacenamiento electrónico no podrán ser donados, arrojados a la basura o reciclados a menos que la información que contengan sea eliminada en forma adecuada que imposibilite su recuperación por parte de terceros.

Capítulo 5. Equipamiento Informático

Introducción

Alcance – Equipamiento informático, como Desktops, Equipos Móviles o Servidores.

Objetivo – Proteger el Equipamiento Informático asegurando una adecuada configuración y utilización dentro y fuera de la Empresa. Definición de estándares y configuración.

Riesgos involucrados – Pérdidas económicas por fraudes debidos al uso ilegítimo de información, aumento de costos operativos por manejo inadecuado de los recursos, inseguridad en la operación, pérdida de reputación.

Políticas

5.1. Desktops y Equipos Portátiles en la Intranet

5.1.1. **Sistema Operativo –** Los equipos Desktops y Portátiles de la A.N.V. deberán ejecutar un Sistema Operativo autorizado por la Gerencia de TI.

5.1.2. **Nuevos Equipos –** Toda incorporación de equipamiento informático o tecnológico, ya sea por compra, donación o cualquier otro mecanismo, deberá cumplir con las especificaciones dictadas por el Gerencia de TI en cuanto a características y configuración de Hardware y Software, y seguir el procedimiento establecido. Antes de concretarse la incorporación, deberá contar con la autorización del Gerencia de TI y la supervisión del Equipo de Seguridad Informática, quienes comprobarán el cumplimiento de las especificaciones técnicas y de seguridad definidas por el Comité de Seguridad.

5.1.3. **Instalación y Configuración –** Todos los equipos Desktops y Portátiles de la A.N.V. deberán ser instalados y configurados por el Gerencia de TI. Los usuarios no deberán instalar otro Sistema Operativo, remplazar al existente o generar un sistema de booteo múltiple. Tampoco deberán actualizar el Sistema Operativo existente, o instalar cualquier tipo de Software utilitario, juegos o programas sin la autorización escrita de la Gerencia de TI y la supervisión del Equipo de Seguridad de la Información.

5.1.4. **Antivirus –** Todos los equipos deberán tener instalado el Sistema de Detección de Virus definido por la política correspondiente, no pudiendo los usuarios desinstalarlo, deshabilitarlo o reconfigurarlo sin la autorización del Equipo de Seguridad de Información.

5.1.5. **Módems –** Los usuarios de la A.N.V. no deberán usar o instalar módems a estaciones de trabajo conectadas a redes LAN de la A.N.V. u otra red interna de comunicación. En caso de equipos Portátiles con módem, éstos no deberán conectarse a Internet mientras permanezcan conectados a la LAN de la A.N.V.

5.1.6. **Puertos USB –** Por defecto se deshabilitarán todos los puertos USB tanto de los desktops como de los equipos Portátiles. Únicamente se habilitarán por razones de servicio y mediante expresa autorización de la Gerencia correspondiente.

5.1.7. **Bloqueo** – Los equipos deberán bloquearse luego de transcurridos un lapso razonable de tiempo con las facilidades que provee el sistema operativo o mediante el protector de pantalla.

5.2. Equipos de la A.N.V. fuera de la Intranet

5.2.1. **Autorización** – El traslado de un equipo Portátil fuera de las oficinas de la A.N.V. deberá ser autorizado por un Gerente de División o de Área según corresponda. El Equipo de Seguridad de la Información deberá controlar que el equipo cumpla con las Políticas establecidas antes de aprobar su salida. Este procedimiento deberá ejecutarse cada vez que el equipo salga de la A.N.V.

5.2.2. **Hardware y Configuración de Setup** – Para ser autorizada su utilización fuera de la Intranet de la A.N.V., los equipos Portátiles deberán ser configurados de la siguiente manera: el ingreso al Setup de la BIOS debe estar protegido por contraseña, el acceso a los discos debe estar

protegido por contraseña. El usuario no podrá tener derechos de administrador del equipo.

5.2.3. **Antivirus, Firewall Personal e I.D.S. –** Los equipos que se utilicen fuera de la Intranet de la A.N.V. deberán tener instalado software Antivirus y Firewall Personal previamente configurado por el Gerencia de TI bajo la supervisión del Equipo de Seguridad de la Información, y eventualmente si se considera y fuera posible un software Detector de Intrusos (IDS). Los usuarios no deberán desinstalarlo, deshabilitarlo o reconfigurarlo sin la autorización del Equipo de Seguridad Informática.

5.2.4. **Certificados –** Todos los certificados digitales que se utilicen en equipos Portátiles de la A.N.V. deberán residir en dispositivos independientes, como por ejemplo USB, o eventualmente, en el propio equipo Portátil, de acuerdo a la decisión que tome el Equipo de Seguridad de la Información en cada caso. Para el caso de utilizar dispositivos externos, deberán ser protegidos por contraseña y no ubicarse en el mismo equipaje/maletín del computador.

5.2.5. **Seguridad de Información Sensitiva** – Toda la información sensitiva que resida en los discos locales de los Equipos Portátiles de la A.N.V. deberá ser configurado para encriptar las carpetas de información corporativa, usando el software autorizado para ello. Los usuarios deben almacenar todos los documentos de trabajo en dichas carpetas.

5.2.6. **Bloqueo** – Los equipos deberán bloquearse luego de transcurridos un lapso razonable de tiempo con las facilidades que provee el sistema operativo o mediante el protector de pantalla con contraseña.

5.2.7. **Puertos USB –** Por defecto se deshabilitarán todos los puertos USB tanto de los desktops como de los equipos Portátiles. Únicamente se habilitarán por razones de servicio y mediante solicitud fundada por parte de por parte de las jefaturas de departamento correspondientes o la Gerencia de TI.

5.3. Servidores.

5.3.1. **Sistema Operativo –** Los Servidores deberán ejecutar Sistemas Operativos autorizados por el Equipo de Seguridad de Información con la supervisión del Comité de Seguridad.

5.3.2. **Configuración de Seguridad –** Los Servidores deberán configurarse de modo que cumplan con las normas de seguridad vigentes y las mejores prácticas de la industria.

5.3.3. **Antivirus –** Los Servidores deberán tener instalado y en ejecución un Sistema de Detección de Virus de Servidor de acuerdo a la Política de Antivirus de la A.N.V.

5.3.4. **Detección de Intrusos –** Los Servidores de Misión Crítica ubicados en la DMZ deberán ejecutar un agente del Sistema de Detección de Intrusos (IDS) de Servidor. Eventualmente, los servidores ubicados en zonas seguras podrían contemplar también esta política.

5.4. Adquisición de hardware y/o software

5.4.1. **Adquisición de hardware y/o software –** La adquisición de equipamiento informático y de software, deberá ser avalada y/o iniciada por la Gerencia de TI, a efectos de mantener la compatibilidad con los recursos existentes en la A.N.V. y con los lineamientos técnicos definidos para el Área de Tecnología.

Capítulo 6. Seguridad Física del entorno de TI

Introducción

Alcance – El entorno físico donde se encuentra la información, como Centros de Cómputos, oficinas con equipamiento informático (Servidores, Desktops, Equipos Móviles) y repositorios de copias en medios magnéticos (CD-ROMs, disquetes, cintas magnéticas) o no magnéticos (papel).

Objetivo – Proteger la Información de la A.N.V. de su robo, divulgación, utilización, modificación o borrado en forma no autorizada, mediante controles de acceso físico.

Políticas

6.1. Seguridad del Perímetro

6.1.1. **Acceso de Terceros –** Todo visitante externo que requiera acceso al Centros de Cómputos o cualquier otra instalación que contenga equipamiento informático con información sensitiva deberá ser registrado y acompañado en todo momento por personal autorizado.

6.1.2. **Instalaciones de Servidores y Equipo de Comunicaciones** – Los servidores y equipos de comunicación deberán estar alojados en recintos adecuados, lejos de peligros externos, y en un lugar separado del muro exterior por paredes internas de piso a techo y sin ventanas.

6.1.3. **Resistencia al Fuego** – Las instalaciones de Servidores y Equipo de Comunicaciones deberán estar protegidas por paredes y aberturas no combustibles y resistentes al fuego.

6.1.4. **Aberturas Blindadas** – Las instalaciones de Servidores y Equipo de Comunicaciones deberán estar equipadas con aberturas blindadas que no puedan ser forzadas.

6.1.5. **Cierre de Aberturas** – Las aberturas de las instalaciones de Servidores y Equipo de Comunicación deberán estar dotadas de brazos que las cierren de forma automática y alarmas que alerten si quedan abiertas por más de un periodo dado.

6.2. Control de Acceso Físico

6.2.1. **Control de Acceso Físico a Información Sensitiva** – El acceso a oficinas, salas de servidores y áreas de trabajo que contengan información sensitiva, deberá ser físicamente restringida mediante dispositivos electrónicos que permitan el registro. Solamente deberán acceder los empleados debidamente autorizados por la Gerencia de TI que tengan la necesidad de acceso físico a los equipos.

6.2.2. **Acceso de Servicios Externos** – El acceso a las áreas que contengan información sensitiva por parte de Servicios Externos tales como Limpieza, Mantenimiento o Reparación, deberá ser controlada y regulada.

6.2.4. **Registro de Accesos** – El Equipo de Seguridad de Información deberá mantener el registro, por un periodo no menor a los tres meses, de las personas que tuvieron acceso a los servidores y equipos de comunicaciones.

6.2.5. **Reportes de Identificaciones** – Deberá generarse una lista mensual de todas las personas que poseen identificadores de acceso a áreas restringidas donde reside información sensitiva, que deberá ser revisada por el Equipo de Seguridad para realizar las modificaciones que considere necesarias.

6.2.6. **Identificaciones de Visitantes** – Todas las personas que accedan a la A.N.V. deberán tener visible la identificación que se le suministra a su ingreso al edificio para poder acceder a zonas restringidas.

6.2.7. **Visitantes acompañados** – Todos los individuos que no sean empleados, contratados o consultores autorizados de la A.N.V., que accedan a zonas restringidas, deberán ser acompañados y supervisados en todo momento por personal debidamente autorizado.

6.2.8. **Personas sin Identificación** – Todo persona que acceda a zonas restringidas de la A.N.V., sin

la debida Identificación, deberá ser interceptada y solicitársele su identificación. Si no justifica su presencia, deberá ser acompañado a la recepción o al puesto de guardia más cercano.

6.2.9. **Acceso al Centro de Cómputos** – Solamente deberán acceder al Centro de Cómputos los empleados designados por la Gerencia de TI y avalado por el Oficial de Seguridad.

6.2.9.1. Una lista de empleados autorizados a acceder debe ser mantenida, revisada periódicamente y actualizada por la Gerencia de TI.

6.2.9.2. El acceso al Centro de Cómputos deberá ser monitoreado y registrado en video las 24 horas del día.

6.2.9.3. Programadores, usuarios y otros empleados sin necesidad de ingreso al Centro de Cómputos, no deberán hacerlo.

6.2.10. **Acceso a Respaldos** – El acceso a los lugares donde se almacenan respaldos en cintas magnéticas, discos y documentación de Sistemas, deberá ser restringido a los empleados que, debido a las responsabilidades de su trabajo, necesitan acceder a dicha información.

6.3. Seguridad en Oficinas, Recintos e Instalaciones

6.3.1. **Acceso a Oficinas** – El acceso a toda oficina, sala de servidores o similar, o área de trabajo que contenga información sensitiva, deberá estar físicamente restringido. Solamente deberá tener acceso a esas áreas el personal identificado y autorizado a tales efectos.

6.3.2. **Cerrado cuando no se usa** – Cuando no está en uso, la información sensible deberá ser protegida contra divulgación no autorizada. Si el responsable de la información debe retirarse de la oficina donde está contenida, la información sensitiva no deberá permanecer sobre escritorios o en cualquier lugar donde pueda ser leído, salvo que todas las puertas y ventanas de la oficina queden bajo llave.

6.3.5. **Indicaciones sobre ubicación** – No deberán existir señales que indiquen la ubicación del Centro de Cómputos o Centros de comunicaciones.

6.3.6. **Registros de Audio, Video o Imagen** – Las personas que accedan a áreas donde se encuentre equipo sensible no deberán utilizar ningún equipamiento de registro de imagen o voz (Cámaras de video o imágenes, grabadores, celulares con posibilidad de registro de voz o imágenes, etc.).

6.4. Áreas de Carga y Descarga Aisladas

6.4.1. **Áreas de entregas** – Se deberá disponer de un área de almacenamiento que haga las veces de depósito intermedio de las entregas de computadoras, equipos u otro tipo de suministros, de forma de evitar el acceso de proveedores a las áreas que contienen equipamiento o información sensible.

6.5. Contexto y Protección de Equipos

6.5.1. **Fumar, Comer y Beber** – Los empleados y visitantes no deberán fumar, comer o beber en las áreas que contengan equipos de computación o comunicación.

6.5.2. **Control del Ambiente del Centro de Cómputos** – Los Centros de Cómputos de la A.N.V. deberán contar con un sistema de detección de humo y extinción de fuego, acondicionamiento de energía eléctrica, aire acondicionado y control de humedad.

6.5.3. **Acceso Físico –** Todos los Centros de Cómputos de la A.N.V. deberán estar custodiados por guardias de seguridad que aseguren el acceso solamente al personal autorizado.

6.5.4. **Registro de Acceso –** Todas las personas que accedan al Centro de Cómputos podrán ser pasibles de registro para cumplir con la norma establecida en 6.3.6 (Registro de Audio, Video o Imagen).

6.5.5. **Alarmas en el Centro de Cómputos** – Los Centros de Cómputos de la A.N.V. deberán estar equipados con alarmas que alerten sobre:

6.5.5.1. **Desastres** – Fuego e inundación, etc.

6.5.5.2. **Accesos no autorizados -** Accesos no autorizados al recinto del Centro de Cómputos.

6.5.5.3. **Fallas en la Energía eléctrica –** Fallas o variaciones en el suministro de Energía Eléctrica y los dispositivos encargados de manejarla (estabilizadores, transformadores, UPS, etc.).

6.5.6. **Monitoreo y Alertas –** Todas las alarmas deberán ser monitoreadas las 24 horas y alertar de forma automática a un responsable que pueda tomar una acción inmediata. El alerta deberá enviarse, de ser necesario, por distintos medios (mensaje desplegable, correo electrónico, beeper, teléfono celular, etc.), que aseguren que el receptor de la misma las reciba en cualquier circunstancia.

6.5.7. **Registro de acceso –** Los Servidores que contengan información sensible del Centro de Cómputos deberán ser controlados mediante sistemas de registro en video las 24 horas.

6.5.8. **Sistemas de Computación Propios** – Los empleados de la A.N.V. no deberán utilizar computadoras, periféricos o software de su propiedad dentro de edificios de la Agencia, sin la previa autorización de la Gerencia de TI.

6.6. Suministro de energía eléctrica

6.6.1. **Equipos de Acondicionamiento eléctrico** – Todos los servidores deberán estar protegidos mediante fuentes ininterrumpibles de poder (UPS), filtros de energía eléctrica y fusibles aprobados previamente por el Gerencia de TI.

6.6.2. **Contingencia** – El suministro de energía eléctrica deberá realizarse mediante dos fuentes que aseguren la conexión a líneas de entrada de corriente diferentes.

6.7. Seguridad en el Cableado

6.7.1. **Cables de Energía Eléctrica y Datos** – La instalación y mantenimiento del cableado eléctrico y de telecomunicaciones deberá seguir los lineamientos de seguridad de la industria.

6.7.2. **Monitoreo de Fallas** – Se deberá disponer de una revisión periódica a fin de detectar posibles fallas en el cableado de datos o energía eléctrica.

6.8. Mantenimiento de Equipos

6.8.1. **Mantenimiento Preventivo** – Se deberá realizar mantenimiento preventivo con la regularidad determinada por las especificaciones del Proveedor a todo equipo de computación y comunicaciones.

6.8.2. **Registro de Fallas** – Deberá generarse y mantenerse un registro de fallas de todo el equipamiento informático y de comunicaciones. Se detallará la identificación del equipo (nombre, número, modelo, etc.), el detalle de la falla y de la reparación, y las fechas de falla y de reparación.

6.9. Seguridad de Equipos fuera de la empresa

6.9.1. **Aprobación de Uso fuera de la empresa** – El uso de equipos informáticos de la A.N.V. fuera de las oficinas de la empresa deberá ser aprobada por la Gerencia de TI.

6.9.2. **Controles de Seguridad** – Las medidas de Seguridad que tomen los usuarios de equipos que se utilicen fuera de la A.N.V. deberán ser las mismas que para los equipos que se utilicen dentro de la empresa.

6.10. Eliminación o Reutilización de Equipos

6.10.1. **Información Sensitiva** – El Equipo de Seguridad de la Información deberá comprobar que toda la información sensitiva ha sido borrada de cualquier dispositivo antes de liberarlo para vender, regalar o donar a terceros.

6.10.2. **Software y Licencias** – El Gerencia de TI deberá ser responsable de que los equipos descontinuados, vendidos, regalados o donados, no contengan software licenciado por la A.N.V., material sometido a derechos de propiedad ni información propiedad de la A.N.V.. Dicho material deberá ser borrado de acuerdo a los procedimientos de eliminación definidos por las Políticas en tal sentido.

6.11. Otras medidas complementarias

6.11.1. **Apagado de Computadoras** – Todas las computadoras de escritorio que manejen Información Sensible, deberán ser apagadas al finalizar la jornada laboral.

Capítulo 7. Control de Acceso

Introducción

Alcance – Todos los usuarios de equipos informáticos de la A.N.V., dentro o fuera de la red, sean empleados o no de la empresa.

Objetivo – Proteger la Información que se almacena en equipos de la A.N.V. mediante su correcta configuración y otorgamiento de permisos.

Introducción – Deberán acceder a la red de la A.N.V. solamente los usuarios que tengan legítima necesidad de hacerlo, debido a la función que desempeñan. Los contratistas, consultores, empleados temporales y pasantes que requieran acceso, deberán ser autorizados por la Gerencia correspondiente.

Requisitos - Para acceder a la red, la Gerencia de Área correspondiente, deberá atenerse al procedimiento establecido.

Políticas

7.1. Acceso al Sistema

7.1.1. **Ingreso de Usuario** – Para acceder a los Sistemas de la A.N.V. se deberá ingresar como mínimo una Identificación de Usuario y una contraseña.

7.1.2. **Días, Horarios y Computadoras** – Los días y horarios habilitados para el acceso de usuarios al sistema, como los equipos desde los cuales tienen permiso de acceso, serán los determinados por la Gerencia del Área correspondiente, de acuerdo a las actividades que desempeñe el usuario en la organización.

7.1.3. **Utilitarios de Sistemas** – El uso de programas utilitarios que puedan obtener acceso a la información evitando los controles del Sistema o de las Aplicaciones, deberá ser restringido a usuarios debidamente autorizados por el Comité de Seguridad de la Información, y sólo para trabajos puntuales. El Oficial de Seguridad deberá llevar un registro de todos los accesos y tareas realizadas por este tipo de utilitarios. Si no se justificara su utilización, deberán ser eliminados del sistema.

7.2. Mantenimiento de Usuarios

7.2.1. **Identificación de Usuarios –** Todos los que tengan acceso a los Sistemas Informáticos de la A.N.V. deberán tener asignada una Identificación o Nombre de Usuario. Estos deberán ser únicos para cada empleado. El nombre de usuario no deberá hacer referencia al nivel de acceso o privilegio que el usuario tiene (ej. "administrador", "gerente").

7.2.2. **Asignación de Identificación de Usuario** – La Gerencia de Área correspondiente, deberá atenerse al procedimiento establecido para dar acceso a aquellos empleados que requieran utilizar los recursos informáticos de la A.N.V. Cada persona es responsable por la actividad que realice en el sistema con la Identificación y contraseña que le sea asignada, o con cualquier otro tipo de mecanismo de autorización de acceso a datos o programas.

7.2.3. **Asignación de Permisos** – El acceso a la información deberá ser autorizada por los propietarios de la misma siguiendo el Principio de Necesidad de Conocer y Usar, a pedido de la Gerencia de Área correspondiente y ateniéndose a los procedimientos establecidos. En momentos de incorporar un Sistema, se le deberá exigir que cumpla con el requerimiento de contar con una herramienta que permita conocer los usuarios autorizados en cada rol o perfil. La responsabilidad primaria por el control de este aspecto recaerá sobre el Gerente del Área correspondiente.

7.2.4. **Registro de usuarios –** El Equipo de Seguridad de Información deberá mantener un registro de los permisos y privilegios asignados a cada usuario de la A.N.V., sus modificaciones y revocaciones. Los funcionarios que administran la seguridad del Sistema no deberán conocer las contraseñas de los usuarios.

7.2.5. **Control de Usuarios -** En lapsos no mayores a 6 meses o cuando la coyuntura lo demande, se deberán realizar controles al registro de usuarios, inhabilitando las cuentas que no se utilicen por períodos prolongados y borrando las que no correspondan o sean redundantes, debiendo actuarse en consecuencia con los permisos que tuvieran asignados. Complementariamente, se debe evaluar en cada caso, la conveniencia de inhabilitar también los recursos de hardware

que disponían dichos usuarios. Para los permisos que involucren el acceso a información sensible, los controles deberán hacerse cada 3 meses.

7.2.6. **Desvinculación de Usuarios –** Deberán eliminarse inmediatamente los privilegios de Sistema y acceso a la información de los usuarios que dejen de pertenecer a la A.N.V.

7.2.7. **Reutilización de Identificación de Usuarios –** No deberá reasignarse la identificación de un usuario a otro nuevo, incluso si el primero ha sido dado de baja.

7.2.8. **Usuarios Administrativos –** Los usuarios genéricos o con privilegios especiales (que permitan evadir los controles de seguridad de aplicaciones y/o del Sistema) del tipo "Administrador", "Root", etc., deberán ser utilizados solamente para fines administrativos por empleados debidamente autorizados, controlados y restringidos por el Equipo de Seguridad de la Información.

7.2.9. **Identificación de Usuarios Administrativos –** El nombre de usuario genérico deberá ser cambiado una vez instalado el software que lo generó. Esto incluye administradores de Sistemas, administradores de Sistemas de correo electrónico, administradores de bases de datos, etc.

7.2.10. **Controles de usuarios Administrativos** – Los privilegios asignados a los Usuarios Genéricos deberán estar basados en el Principio de Necesidad de Conocer y Usar y en el Principio de Event by Event.

7.2.11. **Procedimientos de Sistemas** – Se deberá promover el desarrollo y utilización de rutinas automáticas, procedimientos, scripts, etc., que eviten la asignación de permisos especiales o la utilización de usuarios genéricos.

7.3. Manejo de Contraseñas

7.3.1. **Contraseñas Seguras –** El Sistema de Control de acceso de usuarios deberá asegurar el uso de contraseñas seguras. La política de contraseñas deberá ceñirse a las buenas prácticas en la selección y uso de las mismas, se deberá evaluar periódicamente si su complejidad y extensión cumplen con los estándares de la industria.

7.3.2. **Difícil de Adivinar** – Los usuarios no deberán utilizar como contraseña palabras comunes (que puedan encontrarse en un diccionario), derivadas de la identificación de usuario o de sus datos personales, como nombres de familiares, número de cedula de identidad, teléfono particular, fechas personales (como la de nacimiento de los hijos o de casamiento) nombres o palabras que puedan asociarse al usuario, secuencias de caracteres (del tipo abcdef, 123456, etc.). Los usuarios deberán ser entrenados mediante documentación o cursos, sobre la elección de Contraseñas seguras.

7.3.4. **Cambio de Contraseñas** – Los Sistema de Control de Acceso deberán asegurar que no se pueda reutilizar una contraseña de acuerdo a las buenas prácticas del uso de las mismas.

7.3.5. **Expiración de Contraseñas** – El Sistema de Control de Acceso deberá requerir el cambio de las contraseñas de usuarios con una frecuencia adecuada a las buenas prácticas. Si un usuario sospecha que su contraseña fue divulgada, deberá cambiarla de inmediato.

7.3.6. **Almacenamiento de Contraseñas –** Los usuarios deberán ser responsables por el control y la confidencialidad de sus contraseñas personales. No deberán compartirla con otras personas, compañeros de trabajo o supervisores. Las contraseñas no deberán ser escritas en archivos de

texto, procedimientos, macros, scripts, teclas de función de acceso o firma automática, ni enviadas en correos electrónicos o almacenadas en medios magnéticos. Tampoco deberán escribirse en papeles, post-its, teclados, monitores, pads, portalápices o cualquier otro tipo de medio. Solamente deberán almacenarse en forma encriptada, en repositorios específicos para tales fines aprobados por el Equipo de Seguridad de la Información y el Oficial de Seguridad. Estos repositorios deberán estar protegidos por una clave de acceso.

7.3.7. **Mejores prácticas** – Los Gerentes de Área serán responsables de promover y divulgar entre los funcionarios, las mejores prácticas en cuanto al manejo de contraseñas y la privacidad de las mismas.

7.4. Asignación de Contraseñas

7.4.1. **Contraseñas Temporarias** – Las contraseñas entregadas por Mesa de Ayuda deberán expirar, forzando al usuario a elegir otra contraseña antes que se complete el proceso de logon.

7.4.2. **Reasignación de Contraseñas** – La reasignación de contraseñas se deberá realizar a pedido de un usuario debido a la pérdida de la misma o la sospecha de que ha sido divulgada. Para que Mesa de Ayuda realice la nueva asignación, el usuario deberá probar su identidad de acuerdo al procedimiento establecido.

7.4.3. **Entrega de Contraseñas** – Las contraseñas temporarias serán comunicadas al usuario por parte de Mesa de Ayuda, luego de la comprobación fehaciente de la identidad del mismo, la cual será responsable de verificar que el usuario ingrese al Sistema por primera vez sin inconveniente alguno.

7.5. Registro de Eventos de Seguridad

7.5.1. **Expectativa de Privacidad** – Los usuarios no deberán esperar privacidad durante el uso de los sistemas de información de la A.N.V. Por motivos de seguridad, la A.N.V. podrá registrar, revisar y utilizar la información almacenada en los Sistemas o que haya pasado por los mismos, registrar la actividad de los usuarios, incluyendo programas utilizados, información accedida o modificada, sitios Web visitados, etc.

7.5.2. **Registro de Acceso al Sistema –** Los eventos de acceso al sistema referidos a usuarios y contraseñas deberán ser registrados en logs del Sistema operativo. Como mínimo deberán registrarse: Identificación de Usuario, Fecha y Hora de acceso y salida del sistema, intentos de acceso fallidos.

7.5.3. **Registro de Uso de la Información –** Los procesos de uso y manejo de la Información alojada en el Sistema informático deberán ser monitoreados y registrados en Sistemas de logs del sistema operativo u otros sistemas de registro de eventos que permitan registrar identificación de usuario, fecha y hora de ocurrencia de los eventos, tipo de evento, archivos accedidos, programas o utilitarios utilizados para acceder a la información, uso de cuentas con privilegios especiales, arranques y paradas de los Sistemas, conexión y desconexión de dispositivos de entrada/salida, accesos a registros de Sistemas, violaciones a las políticas de acceso de Firewalls o IDS-IPS, errores en el manejo de los propios registros de eventos.

7.5.4. **Mantenimiento de Registros de Eventos** – Los registros de eventos obtenidos deberán mantenerse por un plazo razonable que será acordado entre el Oficial de Seguridad y el Comité de Seguridad, para su utilización como evidencia en caso de detectarse algún incidente de seguridad. Este plazo puede ser modificado por requerimientos de la Asesoría Legal.

7.5.5. **Revisión de Registros de Eventos** – Los eventos generados deberán ser revisados en forma periódica, utilizando herramientas informáticas que automaticen este proceso. Se deberá prestar especial atención a los eventos de: desactivación de los Sistemas de monitoreo o registro de eventos, alteraciones a archivos que contengan eventos previamente registrados, modificación o borrado de archivos de registros, llenado de archivos (si se dispone de un registro cíclico). El o los responsables de la Revisión de los logs pueden pertenecer al Equipo de Seguridad de la Información, pero no deberán desempeñar el rol de configuradores de las herramientas de monitoreo de la información.

7.5.6. **Sincronización del Tiempo** – Para poder tener una fiel interpretación de los eventos que se investiguen, deberá lograrse una sincronización precisa de la hora del sistema con la Hora Universal (UTC), mediante la utilización de Servicios del tipo Windows Time Service. Dentro de la red, todos los equipos deberán estar sincronizados entre sí.

7.6. Procedimientos de Autenticación

7.6.1. **Autenticación** – El procedimiento de Autenticación es utilizado para verificar que el usuario es quien dice ser. La forma más común de autenticación es el ingreso de una contraseña, un secreto que solamente el usuario conoce y este será el requerimiento mínimo para autenticarse.

7.6.2. **Autenticación avanzada** – En caso de existir información de muy alta confidencialidad, a juicio del Comité de Seguridad, se deberá analizar la implementación de alguna tecnología que permita mayor seguridad y fiabilidad al momento de la autenticación de usuarios.

7.6.3. **Bloqueo de cuenta -** Todas las computadoras de la A.N.V. deberán configurarse para permitir una cantidad mínima de intentos de ingreso de contraseña, después de los cuales si no fue ingresada una contraseña correcta, la cuenta deberá ser bloqueada automáticamente, y solo podrá desbloquearse con la asistencia de personal de Tecnología, después de la comprobación fehaciente de identidad del usuario.

7.7. Acceso de Terceros (Outsourcing)

7.7.1. **Requerimientos de Seguridad** – El acceso de Terceros (Auditores o Empresas Externas) a información de la A.N.V. deberá estar controlado y sujeto a los mismos controles y medidas de seguridad que para los usuarios de la empresa.

7.7.2. **Contrato de Confidencialidad** – El acceso de terceros debe estar regido por un Contrato de Confidencialidad como se define en 2.3.1 (intercambio de Información). Dicho contrato deberá detallar los controles de acceso y las condiciones de seguridad definidas en esta Política, incluyendo métodos de acceso, usuarios autorizados y responsabilidades legales de la Empresa que brinda el servicio.

Capítulo 8. Antivirus

Introducción

Alcance – Equipos Informáticos de la A.N.V.

Objetivo – Proteger los equipos contra amenazas de Virus Informáticos y cualquier tipo de Código Malicioso.

Políticas

8.1. Requerimientos

8.1.1. **Control de Virus –** Todos los equipos de la A.N.V. deberán tener instalado un Sistema de Control de Virus aprobado por el Equipo de Seguridad de la Información. Todos los archivos provenientes de fuentes externas deberán ser analizados antes de su ejecución o utilización. Los equipos personales deberán tener habilitado el análisis de protocolo POP3 a pesar de que dicho protocolo no está permitido.

8.1.2. **Antivirus de Correo Electrónico –** El Servidor de Correo Electrónico deberá tener instalado un Antivirus especializado. Este deberá controlar los correos y archivos adjuntos antes que el Sistema de Correo los distribuya a los usuarios.

8.1.3. **Archivos encriptados o Comprimidos –** Todos los archivos provenientes de fuentes externas, vía Internet o cualquier tipo de medio magnético, que estén encriptados o comprimidos, deberán ser desencriptados o descomprimidos antes de ser analizados por el antivirus.

8.1.4. **Deshabilitación –** Los usuarios no deberán cerrar o deshabilitar los Sistemas de control de virus instalados en sus equipos de escritorio o móviles.

8.1.5. **Posesión y desarrollo de Virus –** Los usuarios no deberán escribir, compilar, copiar, propagar, ejecutar o intentar introducir intencionalmente cualquier tipo de código diseñado para auto-replicarse, causar daño o degradar la performance de los sistemas de la A.N.V.

8.2. Instalación, Actualización y Configuración

8.2.1. **Instalación Automática** – Al conectar un nuevo Servidor, Estación de Trabajo o Equipo Móvil a la Red de la A.N.V. deberá instalarse un antivirus y ejecutarse las actualizaciones disponibles a la fecha de instalación.

8.2.2. **Actualización centralizada** – Las actualizaciones del Sistema de Control de Virus de la A.N.V. deberán descargarse a un Servidor que las distribuirá al resto de los equipos de la Red.

8.2.3. **Configuración centralizada** – El servidor definido en el punto anterior deberá configurar, aplicar y monitorear los parámetros locales del Sistema de Control de Virus, indicando: Identificación del equipo, versión del antivirus instalada, última fecha de actualización, ultimo virus detectado (fecha y hora). Si se detecta un virus o código malicioso en cualquier computadora de la red, el sistema deberá alertar (mensaje desplegable, correo electrónico, beeper, teléfono celular, etc.)

8.2.4. **Servidores –** Los Servidores de la A.N.V. deberán actualizar su antivirus de forma automática y desatendida. Los sistemas deberán verificar con frecuencia no la aparición de nuevas actualizaciones.

8.2.5. **Estaciones de Trabajo –** Las Estaciones de Trabajo de la A.N.V. deberán actualizar su antivirus cada vez que se encienden, de forma automática y desatendida.

8.2.6. **Equipos Móviles –** Los equipos móviles deberán actualizar su antivirus de forma automática y desatendida cada vez que se conecten a la Red de la A.N.V. Si se conectan a otra Red, deberán actualizar su antivirus desde Internet de forma automática o manual. Los usuarios que

utilicen equipos Móviles deberán ser entrenados en el procedimiento de actualización manual.

8.3. Reporte de Virus

8.3.1. **Detección de Virus** – Cualquier usuario que reciba una alerta de virus, deberá desconectar físicamente su equipo de la red y avisar a Mesa de Ayuda. Los usuarios no deberán intentar remover un virus por su propia cuenta.

8.3.2. **Sospecha de código malicioso** – Si un usuario sospecha que está siendo víctima de un virus u otro tipo de código Malicioso, deberá seguir el mismo procedimiento descrito en 8.3.1.

Capítulo 9. Respuesta a Incidentes

Introducción

Alcance – Incidentes que involucren equipamiento informático o la información contenida.

Objetivo – Generar los Procedimientos necesarios para reportar incidentes de seguridad, solucionarlos, reparar los daños causados y documentarlos, creando una base de conocimiento para futuras consultas.

Políticas

9.1. Roles y Responsabilidades

9.1.1. **Definición de Incidente** – Un incidente es un evento que provoca cierto nivel de crisis y requiere llevar a cabo una acción para reducir o eliminar el riesgo causado. Puede ir desde la Intrusión a una Computadora, la Negación de Servicios (DoS), Infecciones de Virus, Acceso no autorizado, hasta eventos que normalmente llevan a tomar medidas de Recuperación ante Desastres (Disaster Recovery) como cortes de energía o desastres naturales.

9.1.2. **Grupo de Respuesta a Incidentes** – El Grupo de Respuesta a Incidentes (GRI) de la A.N.V. deberá estar formado por el Oficial de Seguridad y el Equipo de Seguridad de Información, los integrantes de Mesa de Ayuda, los Administradores de Sistemas, los Administradores de Red y la Gerencia de Sistemas. Adicionalmente se sumará personal no técnico (RRHH, Legal, Relaciones Externas), o técnico (Administradores de Bases de Datos, Desarrollo), de acuerdo al tipo de Incidente.

9.1.3. **Funciones del GRI** – Recibir los reportes de incidentes generados en la empresa, determinar su grado de importancia, escalar el problema cuando sea pertinente y tomar las acciones correctivas necesarias. Este grupo deberá entrar en acción solamente en caso de un Incidente, continuando sus miembros sus actividades habituales cuando no sea requerida su participación. También será su función la de crear, mantener y actualizar los procedimientos y guías asociados con la Respuesta a Incidentes.

9.1.4. **Líder del GRI** – El GRI deberá tener un líder, en general el Oficial de Seguridad, que será responsable por las acciones tomadas por el grupo durante el transcurso de un incidente y de coordinar dichas acciones basándose en los procesos y guías generados.

9.1.5. **Líder del Incidente** – Cada incidente deberá tener un líder "ad hoc" nombrado por el Oficial de Seguridad que será el responsable de llevar a cabo todas las actividades durante un incidente determinado. Todas las comunicaciones relativas a los progresos del incidente deberán pasar por el Líder del Incidente.

9.2. Reporte de Incidentes

9.2.1. **Datos Requeridos –** Cuando un usuario de la A.N.V. reporte un incidente a Mesa de Ayuda, deberá especificar: Fecha y Hora del reporte, quien realiza el reporte del incidente, naturaleza del mismo, cuando ocurrió, el hardware y el software involucrado.

9.3. Respuesta a Incidentes

9.3.1. **Detección Inicial** – Cuando un usuario sospeche la existencia de un incidente de seguridad, deberá reportarlo a Mesa de Ayuda, quien lo derivará al equipo de seguridad informática. Este equipo verificará su ocurrencia, los sistemas comprometidos, usuarios involucrados y su impacto potencial sobre el negocio.

9.3.2. **Estrategia de Respuesta** – Una vez determinada la ocurrencia de un incidente, el GRI deberá establecer la mejor estrategia de respuesta. Esta deberá considerar factores técnicos y del negocio y según la gravedad del mismo deberá ser aprobada por la dirección de la A.N.V.,

por lo que deberá presentarse en términos no técnicos indicando los pros y contras. Por ejemplo, Tiempo de caída de la red, Tiempo de no-acceso de usuarios al sistema, Obligaciones Legales, Imagen Pública, Robo de Propiedad Intelectual, etc.

9.4. Investigación

9.4.1. **Investigación –** Luego de aprobada la estrategia, el GRI deberá determinar el por qué, el qué, el cuándo, el dónde y cómo aislar el incidente.

9.4.2. **Procedimiento de Respuesta –** Para llevar a cabo la investigación forense del incidente, el GRI deberá construir un proceso de respuesta al incidente y una política que lo soporte. A pesar que algunas de las Políticas en las cuales se basará el proceso de respuesta son las Políticas de Seguridad actualmente aprobadas, el GRI podrá necesitar rever la forma que dichas políticas se pueden aplicar en el incidente actual y recomendar cambios que soporten las actividades en la respuesta al incidente.

9.4.3. **Recolección de Evidencias –** Durante la fase de Investigación, se deberán recabar evidencias que puedan servir para determinar y probar quién llevó a cabo el ataque y qué vulnerabilidades o errores en la configuración de los Sistemas fueron explotadas. La toma de evidencia se puede realizar durante el desarrollo del ataque.

9.5. Medidas Preventivas

9.5.1. **Implementación de Medidas de Seguridad** – La meta de esta fase será la implementación de medidas que prevengan que el incidente siga causando daño.

9.5.2. **Aislamiento del Problema** – Se deberá aislar y contener el problema que generó el incidente antes de comenzar con la recuperación de los Sistemas.

9.6. Aprendizaje

9.6.1. **Investigación Forense** –Antes de cerrar el incidente, si se justifica por su gravedad, se deberá realizar una investigación donde se estudie información recabada en las fases de Investigación y Solución para intercambiar experiencias y actualizar los procedimientos, basado en los nuevos conocimientos adquiridos. Esta investigación deberá llevarse a cabo por el Grupo de Respuesta a Incidentes, el Líder del Incidente y el Oficial de Seguridad, con la supervisión del Equipo de Seguridad de la Información, y de ser necesario, el Comité de Seguridad.

9.6.2. **Base de Conocimiento** – Los resultados de las investigaciones y las medidas correctivas tomadas en la solución de los incidentes, deberá integrar una Base de Conocimiento. Esta Base será consultada ante nuevos incidentes para determinar si los procedimientos y soluciones utilizadas son aplicables o puedan servir para generar nuevos procedimientos y soluciones.

Capítulo 10. Gestión de la Continuidad de las actividades de la A.N.V.

Introducción

La Gestión de la continuidad del negocio es un proceso crítico que debe involucrar a todos los niveles del Organismo.
La responsabilidad de la gestión de la continuidad del negocio recae en la dirección de la organización, quien deberá tener en cuenta su cometido.
El desarrollo e implementación de un sistema de gestión de la continuidad del negocio, es una herramienta básica para garantizar que las actividades de la A.N.V. se restablezcan dentro de los plazos requeridos.
Se deberá contar con un proceso formal y documentado para garantizar la continuidad del negocio, donde la capacidad de continuar las actividades sea primordial para la organización en sí, así como para sus clientes y partes interesadas.
Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y de gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades y asegurar la reanudación oportuna de las operaciones indispensables.

Objetivo – Generar los Procedimientos necesarios para minimizar los efectos de las posibles interrupciones de las actividades normales de la A.N.V. (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos del negocio mediante una combinación de controles preventivos y acciones de recuperación.
Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:

a) Prevención, prueba y mantenimiento del plan.
b) Activación y Administración de la Crisis.
c) Recuperación.
d) Operación en régimen de contingencia.
e) Vuelta a la normalidad.

Incumplimiento de la Política de Seguridad de la Información

El incumplimiento de estos y otros requisitos de Seguridad de la Información puede resultar en una acción disciplinaria. En alguna ocasión, una solicitud de incumplimiento puede ser establecida, en esos casos, el incumplimiento debe ser aprobado luego de un proceso de valoración y aceptación del riesgo. El proceso requiere un memo de aceptación del riesgo firmado por los Directores y aprobado por el Equipo de Seguridad de la Información. Más detalles sobre el proceso de aceptación del riesgo pueden ser obtenidos a través de una Auditoría interna.

Preguntas sobre este documento podrán ser realizadas al Comité de Seguridad de la Información a través de correo electrónico **SEGINFO@ANV.GUB.UY**

Glosario de términos técnicos

Ad Hoc	Ad hoc es una locución latina que significa literalmente «para esto». Generalmente se refiere a una solución elaborada específicamente para un problema o fin preciso y, por tanto, no es generalizable ni utilizable para otros propósitos. Se usa pues para referirse a algo que es adecuado sólo para un determinado fin.
Autenticación	Verificación de la identidad de un usuario
Autoridad certificadora	En criptografía una autoridad de certificación, certificadora o certificante (AC o CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública
Certificado digital	Un certificado digital (también conocido como certificado de clave pública o certificado de identidad) es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad (por ejemplo: nombre, dirección y otros aspectos de identificación) y una clave pública.
Copyright	El derecho de autor es un conjunto de normas jurídicas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística, musical, científica o didáctica, esté publicada o inédita.
Crackers	El término cracker (del inglés crack, romper) se utiliza para referirse a las personas que rompen algún sistema de seguridad. La finalidad de los cracker es siempre el delito con beneficio económico
Detector de intrusos	Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red
Dispositivos biométricos	Dispositivos de autenticación de individuos mediante la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo
DMZ	En seguridad informática, una zona desmilitarizada (DMZ, de-militarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna.
e-Commerce	El comercio electrónico, también conocido como e-commerce (electronic commerce en inglés), consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas.
Encriptación	Criptografía (del griego krypto= «oculto», y graphos= «escribir», literalmente «escritura oculta») se ha definido como la parte de la criptología que se ocupa de las técnicas que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado y/o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes
Equipo Portátil	Se entiende por Equipo Portátil todo dispositivo móvil que proporcione portabilidad y posea capacidad de procesamiento, con conexión permanente o intermitente a la red por ejemplo: notebook, netbook, tablet, teléfonos inteligentes, etc.
Extranet	Una extranet es una red privada que utiliza protocolos de Internet, protocolos de comunicación e infraestructura pública de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios, clientes o cualquier otro negocio u organización. Se puede decir en otras palabras que una extranet es parte de la Intranet de una organización que se extiende a usuarios fuera de ella. Usualmente utilizando Internet
Firewall	Un cortafuego (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
FTP	FTP (siglas en inglés de File Transfer Protocol, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la transferencia de archivos
Hackers	Hacker (seguridad informática), una persona que irrumpe en computadoras y redes informáticas. Los hackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta o por el desafío

HTTP	Hypertext Transfer Protocol o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web.
HTTPS	Hyper Text Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hiper Texto, es decir, es la versión segura de HTTP.
IDS	Ver Detector de intrusos
Imesh	iMesh es una aplicación de tecnología peer-to-peer que permite el intercambio de información gratuita en casi cualquier formato. Usa una red P2P (IM2Net) privada. iMesh es propiedad de la compañía americana iMesh, Inc
Información sensitiva	Toda aquella información que no es de uso público
Intranet	Una intranet es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales
ISP	Un proveedor de servicios de Internet (o ISP, por la sigla en inglés de Internet Service Provider) es una empresa que brinda conexión a Internet a sus clientes
IT	Acrónimo inglés de Information Technology (Tecnologias de la información)
KaZaa	Kazaa (antes llamado "KaZaA") es una aplicación para el intercambio de archivos entre pares
LAN	Una red de área local, red local o LAN (del inglés local area network) es la interconexión de una o varias computadoras y periféricos
Ley 18.381 art 8ª Información Secreta	Se entiende por información secreta aquella definida en ese carácter por ley.
Ley 18.381 art 9ª Información Reservada	Se clasificará como información reservada aquella cuya difusión pueda comprometer la seguridad pública o la defensa nacional; menoscabar la conducción de las negociaciones o bien, de las relaciones internacionales, incluida aquella información que otros estados u organismos internacionales entreguen con carácter de reservado al Estado uruguayo; dañar la estabilidad financiera, económica o monetaria del país; poner en riesgo la vida, la dignidad humana, la seguridad o la salud de cualquier persona; suponer una pérdida de ventajas competitivas para el sujeto obligado o pueda dañar su proceso de producción; desproteger descubrimientos científicos, tecnológicos o culturales desarrollados o en poder de los sujetos obligados.
Ley 18.381 art 10ª Información Confidencial	Se clasificará como información confidencial I) la entregada en ese carácter siempre que: refiera al patrimonio de la persona; comprenda hechos o actos de carácter económico, contable, jurídico o administrativo, relativos a una persona física o jurídica, que pueda ser útil para un competidor; esté amparada por una cláusula contractual de confidencialidad y II) los datos personales que requieran previo consentimiento informado.
Logs	Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why) un evento ocurre para un dispositivo en particular o aplicación.
DNS	Domain Name System o DNS (en español: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.
One-Time password	La autenticación con contraseña de un solo uso u OTP (del inglés One-Time Password) es una variación de la autenticación con usuario/contraseña. En este método de autenticación se dificulta el acceso no autorizado haciendo que cada contraseña sea válida para una única sesión. Se tiene que usar una contraseña nueva para cada sesión.
Peer-to-Peer	Una red peer-to-peer, red de pares, red entre iguales, red entre pares o red punto a punto (P2P, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.
Perímetro de acceso	Ver DMZ

POP3	Post Office Protocol (POP3, Protocolo de la oficina de correo) en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto
Principio Event-by-Event	Paradigma de programación en el que tanto la estructura como la ejecución de los programas van determinados por los sucesos que ocurran en el sistema, definidos por el usuario o que ellos mismos provoquen
Principio de Necesidad de conocer y usar	Asignación de privilegios mínimos necesarios para tareas especificas
Proxy	Su finalidad más habitual es la de servidor proxy, que consiste en interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc. Esta función de servidor proxy puede ser realizada por un programa o dispositivo
Routers	Un router —anglicismo, también conocido como encaminador, enrutador, direccionador o ruteador— es un dispositivo de hardware usado para la interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar
SMTP	Simple Mail Transfer Protocol (SMTP) Protocolo Simple de Transferencia de Correo. Protocolo de red basado en textos utilizados para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.)
Spam	Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor
Tecnología de dos factores	Sistema de autenticación que requiere que el usuario ingrese 2 tipos de datos para obtener acceso. El usuario tiene que validar precisamente 2 factores: algo que sabe (PIN, Password) y algo que tiene (credencial almacenada en un dispositivo de Hardware)
VPN	Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada
Web mail	Servicio de correo basado en http/https
Web server	Servidor de internet
Zona semi-segura	ver DMZ

Historia del documento

Ediciones			
Revisión	**Fecha**	**Motivo de Revisión**	**Modificaciones**
1.0	22/07/2010	Generación del Documento	Provisorio hasta revisión por parte del Comité de Seguridad de la Información.
1.1	29/12/2011	Revisión Gral. por inicio de funciones del Comité de Seguridad de la información	Se modifican definición Confidencial (4.1.1)
1.2	31/05/2012	Revisión Gral. de la política	Se cambia el punto "Requisitos previos" del Capítulo 2. Se agrega glosario de términos
1.3	01/08/2012	Revisión Gral. de la política	Se cambian varios términos del documento en general.
1.3.1	30/08/2012	Revisión Gral. de la política	Se modifica el punto 2.9.5 para que no sea muy específico acerca del adendum. Se agrega al glosario la definición de "Información sensitiva"
1.3.2	24/09/2012	Revisión Gral. de la política	Se modifica la redacción de varios puntos de la política y se modifico el capitulo 4.
1.3.3	26/10/2012	Revisión Gral. de la política	Se agrega capitulo 10.