INFORMACIÓN DE LA POLÍTICA

TIPO DE POLÍTICA: Seguridad Informática
DUEÑO DE LA POLÍTICA: Dirección Nacional de Tecnología de Información y Comunicaciones
NUMERO DE PROCESO: SCVS-POL-DNTIC-SI-001
VERSIÓN: 004
OFICINA: Planta Central
LOCALIDAD: Guayaquil
FECHA DE ELABORACIÓN: 24 de junio de 2020

FIRMAS DE RESPONSABILIDAD

Elaborado por:

Nombre y Apellido	Cargo	Área	Firma
M.Sc. Ángel Ignacio Yánez Navarrete	Oficial de Seguridad Informática	Dirección Nacional de Tecnología de Información y Comunicaciones	

Revisado por:

Nombre y Apellido	Cargo	Área	Firma
M.Sc. Fernando Calderón	Director Nacional de Tecnología de Información y Comunicaciones	Dirección Nacional de Tecnología de Información y Comunicaciones	 FERNANDO ROBERTO CALDERON LOPEZ
M.Sc. Alvaro Acosta Ávila	Intendente Nacional de Planificación y Gestión Estratégica	Intendencia Nacional de Planificación y Gestión Estratégica	Firmado digitalmente por firma alvaro acosta 2020

Aprobado por:

Nombre y Apellido	Cargo	Firma
Ab. Víctor Anchundia Places	Superintendente de Compañías, Valores y Seguros	 Firmado digitalmente por VICTOR MANUEL ANCHUNDIA PLACES Fecha: 2021.07.14 13:21:02 -05'00'

CONTROL DE CAMBIOS

Versión	Sección y/o página	Descripción de la modificación	Fecha de la modificación
3	Varias	Recomendaciones indicas por el INPA	01/08/2013
4	Varias	Actualización	01/10/2019
5	Varias	Actualización	23/04/2020
6	Página 21	Incorporación de normas para la modalidad de teletrabajo	06/05/2020
7	Página 28	Incorporación de herramienta para videoconferencia en modalidad teletrabajo	07/05/2020
8	Varias	Recomendaciones indicas por el INPA	29/01/2021

GLOSARIO DE TÉRMINOS

AMENAZA: Elemento o acción capaz de atentar contra la seguridad de la información.

APLICACIÓN: Programa con la cual el usuario final interactúa a través de una interfaz, con el fin de realizar determinadas tareas.

C.O.B.I.T: (Objetivos de Control para Información y Tecnologías Relacionadas) Marco de trabajo para las buenas prácticas de Gobernabilidad de Tecnologías de la Información.

COMITÉ DE SEGURIDAD: Cuerpo integrado por representantes de la Dirección Nacional de Tecnología de Información y Comunicación, destinado a garantizar la seguridad informática en los procesos institucionales.

CONTRASEÑA: Combinación compuesta de caracteres alfabéticos, numéricos y caracteres especiales; requerida para tener acceso a los sistemas de información.

CONFIDENCIALIDAD: Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. La confidencialidad es el acceso a la información únicamente por personas que cuenten con la debida autorización.

DISPONIBILIDAD: Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

DIAL-UP: Es una conexión a internet o a una red de datos corporativa por medio de la utilización de un MODEM y una línea telefónica existente.

ESTACIÓN DE TRABAJO: Ordenador que facilita a los usuarios acceder a los servidores y periféricos de la red.

FTP: Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

INCIDENTE DE SEGURIDAD: Evento adverso en un sistema o red de computadoras, que compromete la confidencialidad, integridad, disponibilidad, autenticidad y confiabilidad de la información.

INFORMACIÓN: Conjunto organizado de datos procesados, que constituyen conocimiento, cuya representación se almacena en cualquier forma y en cualquier medio (magnético, papel, en pantallas de computadoras, audiovisual, entre otros).

INTEGRIDAD: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

INTERNET: Red global que proporciona comunicaciones de ámbito mundial.

ITIL: (Information Technology Infrastructure Library). Conjunto de conceptos y prácticas para la administración de servicios de tecnología de información.

MALWARE: Es un tipo de software que tiene como objetivo infiltrarse o dañar equipos o sistemas de información sin el consentimiento de su propietario. El término MALWARE hace referencia a una variedad de software hostil, intrusivo o molesto.

RESPALDOS: Consiste en guardar en un medio extraíble información sensible referida de un sistema.

RIESGO: Posibilidad de que una amenaza aproveche una vulnerabilidad y dañe un activo de información.

RIESGO RESIDUAL: Es el nivel de riesgo que permanece en la organización tras mitigar, reducir o eliminar riesgos. Exige que se tomen medidas previas para que, de manifestarse, su efecto sea mínimo.

SEGURIDAD INFORMÁTICA: Disciplina de diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

USB: (Universal Serial Bus**).** Dispositivo de almacenamiento masivo que facilita la copia y traslado de datos.

VPN: (Red Privada Virtual**).** Tecnología que permite la extensión de una red pública.

VULNERABILIDAD: Puntos débiles de un sistema informático en el cual se compromete la integridad, disponibilidad o confidencialidad,

ÍNDICE

POLÍTICAS DE SEGURIDAD INFORMÁTICA

1. ANTECEDENTES

Actualmente, en las organizaciones, los procesos agregadores de valor y los de apoyo consideran el ingreso de datos para su procesamiento, almacenamiento e intercambio de información, y se ejecutan y desarrollan gracias a las Tecnologías de la Información y Comunicaciones. Para el desarrollo y sostenimiento de los servicios de misión crítica, de cualquier institución, la información es considerada su activo principal y el de mayor valor.

El gobierno en línea está ligado a la administración pública, cuyos cambios importantes se reflejan en la organización, nuevos proyectos y políticas ligadas a estrategias de T.I.C. Es precisamente en este esquema, que los tres pilares fundamentales de la seguridad de la información, como son la confidencialidad, integridad y disponibilidad se ven expuestos a una variedad de nuevos riesgos. Frente a estas situaciones, la organización deberá proponer la política y controles apropiados, que promuevan una gestión segura de los procesos en la cadena de valor, primando la protección de la información.

Por lo tanto, surge la necesidad de que la infraestructura tecnológica cuente con una política de seguridad informática y normas que aseguren la privacidad y disponibilidad de la infraestructura tecnológica para la Superintendencia de Compañías, Valores y Seguros, además, con un lineamiento que ayude a concientizar a los funcionarios acerca de la importancia de proteger y salvaguardar uno de los activos más importantes en la Institución, la información.
Por todo lo anterior la Dirección Nacional de Tecnología de Información y Comunicación, ha elaborado, como parte de sus actividades para garantizar la ejecución de los procesos informáticos de manera segura, el presente documento de políticas de seguridad, para su aplicación por parte de todos los funcionarios de la institución, y con el objetivo adicional, de asegurar el cumplimiento de la Norma de Control Interno 410 de la Contraloría General del Estado.

La política y normas que se ha propuesto, derivan directamente de los objetivos fundamentales de todo esquema de seguridad, a saber, "*la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y la disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".*

El presente documento establece la "Política de Seguridad Informática y Normas para la Privacidad y Disponibilidad de la Infraestructura Tecnológica" para la Superintendencia de Compañías, Valores y Seguros, permitiendo con esto definir los parámetros generales para la elaboración de procesos, procedimientos, indicadores, manuales, matrices, entre otros documentos, que ayuden a realizar la gestión del riesgo y a dar soporte al cumplimiento de los objetivos institucionales.

Figura 1: Ciclo de la Seguridad Informática

2. POLÍTICA DE SEGURIDAD INFORMÁTICA

La Superintendencia de Compañías, Valores y Seguros es una institución que controla, supervisa y promueve el mercado de valores, la actividad societaria y de seguros, siendo la información un factor importante para el desarrollo de sus funciones, para lo cual se mantienen prácticas seguras en procesos como la adquisición de infraestructura, implementación de procedimientos y la elaboración y puesta en marcha de planes de contingencia, que permitan el cumplimiento de los objetivos del manejo seguro de la información. Dichas prácticas se rigen por esta política institucional, que, a su vez, se basa en el Marco Legal y Regulatorio Estatal, en la Norma de Control Interno 410 emitida por la Contraloría General del Estado, y en recomendaciones y mejores prácticas internacionales, en ese estricto orden jerárquico.

3. ALCANCE

La presente Política y Normas detalladas, están dirigidas a:

- Los funcionarios de la Superintendencia de Compañías, Valores y Seguros, sin excepción del rol que desempeñen dentro de la institución;
- Los recursos y procesos internos o externos de la institución; y,
- Las relaciones con terceros que impliquen ingreso de datos y acceso de la información.
- Todos los procesos relacionados con el ingreso, procesamiento, almacenaje y entrega de información.

4. JUSTIFICACIÓN

Permitirá la operación segura de la información y la infraestructura de T.I.C, así como el cumplimiento de la Norma de Control Interno 410 Tecnología de la información de la Contraloría General del Estado.

5. OBJETIVOS

5.1. OBJETIVO GENERAL

Proteger la información frente a amenazas internas o externas, deliberadas o accidentales, de manera que se mantenga la confiabilidad, integridad y disponibilidad de la misma para los funcionarios y usuarios de la institución.

5.2. OBJETIVOS ESPECÍFICOS

- Establecer lineamientos y directrices para el correcto uso y protección de la información en la Superintendencia de Compañías, Valores y Seguros.
- Promover el uso de las mejores prácticas de seguridad informática en los funcionarios, generar conciencia y colaboración respecto a la protección de la información y los recursos institucionales.
- Servir de guía en el comportamiento profesional de los funcionarios de la Superintendencia de Compañías, Valores y Seguros, con el fin de minimizar los incidentes internos de seguridad informática.
- Proponer e implementar los mecanismos de seguridad lógica, de manera que se cumplan los lineamientos de confidencialidad, integridad y disponibilidad de la información.
- Promover la implementación y aplicación de las mejores prácticas de seguridad física y lógica para la correcta custodia de los datos y la infraestructura de T.I.C. de la Superintendencia de Compañías, Valores y Seguros.

- Definir mecanismos para identificar y analizar el riesgo con el fin de mitigarlo, transferirlo o evitarlo, aceptando el riesgo residual.

6. RESPONSABILIDAD

- La máxima autoridad de la institución es la única facultada para la aprobación de esta Política y Normas, luego de la revisión, modificación o actualización propuesta por el Comité de Seguridad.
- Los Intendentes Nacionales, Intendentes Regionales, Directores Nacionales y Directores Regionales, son responsables de estimular y confirmar que los funcionarios a su cargo tengan acceso y conocimiento de la "Política de Seguridad Informática y Normas para la Privacidad y Disponibilidad de la Infraestructura Tecnológica".
- Una vez aprobada, todos los funcionarios de la SCVS, sea cual fuere su rol dentro de la institución, son responsables del cumplimiento de la presente política.

7. ESTRUCTURA

Para soportar la política, normas, su alcance, objetivos y cumplimiento, se consideran los siguientes roles:

Oficial de Seguridad Informática. - Responsable de realizar las actividades que permitan revisar y analizar los procesos y procedimientos para el cumplimiento de las políticas y normas detalladas. Actualizar y/o proponer nuevas normas de seguridad y de privacidad. También del monitoreo de riesgos institucionales y de investigar los incidentes relativos a la seguridad informática.

Coordinador Nacional de Producción e Infraestructura. - Encargado de revisar los procesos y procedimientos para el cumplimiento de las políticas y normas detalladas. Proponer los proyectos para mitigar, trasladar, evitar o aceptar el riesgo residual. Supervisar la investigación y monitoreo de los incidentes relativos a la seguridad. Revisar los cambios significativos en los riesgos que afecten los recursos informáticos y las aplicaciones puestas en producción.

Coordinador Nacional de Desarrollo y Datos. - Se encargará de revisar los procesos y procedimientos para el cumplimiento de las Políticas y Normas detalladas. Proponer los proyectos para mitigar, trasladar, evitar o aceptar el riesgo residual. Supervisar la investigación y monitoreo de los incidentes relativos a la seguridad. Revisar los cambios significativos en los riesgos que afecten las aplicaciones y bases de datos.

Comité de Seguridad. - Se encuentra conformado por el Director Nacional de Tecnología de Información y Comunicaciones, el Coordinador Nacional de Producción e Infraestructura, el Coordinador Nacional de Desarrollo y Datos y el Oficial de Seguridad Informática.

Este comité se encargará de revisar y proponer las nuevas iniciativas o mejoras para incrementar la seguridad informática, ayudar a que la seguridad informática sea parte del proceso de planificación institucional, evaluar y coordinar la implementación de controles específicos de seguridad informática para nuevos sistemas o servicios, promover la difusión y apoyo a la seguridad de la información dentro de la Institución.

8. ACTUALIZACIÓN

La presente política se revisará con una periodicidad mínima de 1 año, para actualizar la política y/o agregar nuevas normas, que se utilizan para orientar el uso adecuado de los recursos y servicios informáticos teniendo presente la seguridad informática en todos los procesos institucionales.

Sin embargo, en caso de que exista una vulnerabilidad detectada durante el proceso de monitoreo que indique altos riesgos e impactos, esta será atendida con carácter de urgente por parte de todos los miembros del comité, para la actualización inmediata y aprobación de la máxima autoridad.

9. SANCIONES

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente “Política de seguridad informática y normas para la privacidad y disponibilidad de la infraestructura tecnológica” conforme lo establecido en la Ley Orgánica del Servicio Público, su Reglamento y el Reglamento General para la Administración del Talento Humano de la Superintendencia de Compañías, Valores y Seguros, sin perjuicio de las acciones civiles y penales a las que hubiere lugar.

NORMAS PARA LA PRIVACIDAD Y DISPONIBILIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA

La "Política de Seguridad Informática y Normas para la Privacidad y Disponibilidad de la Infraestructura Tecnológica" regulan el correcto uso de la infraestructura tecnológica y servicios informáticos de la Superintendencia de Compañías, Valores y Seguros, tal como lo se lo define en su alcance, conforme los siguientes lineamientos:

- Privacidad.
- Utilización de cuenta de usuario y contraseña.
- Utilización de los recursos de red.
- Utilización del correo electrónico institucional.
- Utilización del servicio de Internet.
- Publicaciones en la página WEB.
- Software autorizado.
- Respaldo de la información en los servidores.
- Respaldo de la información en las estaciones de trabajo y portátiles.
- Acceso remoto (VPN).
- Uso de dispositivos externos
- Teletrabajo
- Propiedad intelectual

A. PRIVACIDAD

1. La Superintendencia de Compañías, Valores y Seguros para garantizar la privacidad de la información procurará que el acceso a sus sistemas se realice a través de un procedimiento riguroso, mediante el otorgamiento de cuentas de usuario y contraseñas. Los permisos de acceso para las cuentas de usuario serán aprobados o negados por los responsables de la información. De esta manera se asegura que, solo aquellas personas cuyas funciones requieran acceso a la información puedan tener los permisos para dicho fin. Tal como se lo describen en:

    a. Ley de Compañías
    b. Ley Orgánica de Optimización y Eficiencia de Trámites Administrativos
    c. Ley Orgánica de Transparencia y Acceso a la Información Pública.
    d. Acuerdo No. SGPR1-2019-010

2. Todo funcionario que utilice estaciones de trabajo y servicios informáticos de la Superintendencia de Compañías, Valores y Seguros, deber firmar un convenio

donde acepte las condiciones de privacidad (confidencialidad), del uso adecuado de los recursos informáticos y de la información, en estricto apego al Reglamento General para la Administración de Talento Humano, de la Superintendencia de Compañías, Valores y Seguros.

3. Es responsabilidad de todo funcionario evitar la fuga o sustracción de la información de la Superintendencia de Compañías, Valores y Seguros. Esto incluye los archivos que se encuentran almacenados en las estaciones de trabajo, portátiles o tablets asignados.

4. Todo funcionario tiene la obligación de proteger cualquier dispositivo de almacenamiento externo de información que se encuentre bajo su custodia y que contenga información reservada o confidencial para la Superintendencia de Compañías, Valores y Seguros, en estricto cumplimiento al Reglamento administración y control de bienes del sector público y las Normas de Control Interno de la Contraloría General del Estado.

5. Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, sustraída, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el funcionario deberá notificar de manera inmediata tal como lo indica el Reglamento General para la Administración del Talento Humano de la Superintendencia de Compañías, Valores y Seguros.

6. El funcionario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática, deberá reportarlo a la Dirección Nacional de Tecnología de Información y Comunicación lo antes posible, indicando claramente los datos relevantes para poder tomar las acciones preventivas o correctivas necesarias, tal como lo indica el Reglamento General para la Administración del Talento Humano de la Superintendencia de Compañías, Valores y Seguros.

B. UTILIZACIÓN DE CUENTAS DE USUARIOS Y CONTRASEÑAS.

1. Todos los funcionarios de la Superintendencia de Compañías, Valores y Seguros contarán con una cuenta de usuario para poder acceder a los servicios informáticos, la misma que se generará al momento de que el Especialista de Talento Humano ingrese los datos del nuevo funcionario y los remita a la Dirección Nacional de Tecnología de Información y Comunicación para que le otorguen los permisos respectivos.

2. Todos los funcionarios que utilicen los servicios informáticos son responsables únicos y directos por la utilización de la cuenta de usuario y contraseña que se les asigna y reciben. Es decir, son responsables por el uso apropiado o inapropiado del ingreso de datos o acceso a la información, así como de las actividades realizadas en su cuenta de usuario.

3. El ingreso y acceso a la información siempre será realizado por medio de los recursos informáticos provistos, revisados o autorizados por la Dirección Nacional de Tecnología de Información y Comunicación.

4. Está terminantemente prohibido, a todos los funcionarios, divulgar las cuentas de usuario y contraseñas, así como permitir su uso por parte de terceros (funcionarios o personal externo).

5. Está terminantemente prohibido escribir o revelar la contraseña en un papel o documento donde quede disponible, expuesta o de libre acceso. Tampoco se debe guardar en documentos de texto dentro del propio ordenador o dispositivo.

6. Está terminantemente prohibido habilitar o utilizar alguna opción (herramienta) que permita recordar o administrar contraseñas de manera particular en los servicios que utiliza.

7. Está terminantemente prohibido enviar la contraseña por mensajería indirecta (como Correos Electrónicos o SMS) o mensajería directa (como WhatsApp, Telegram, Messenger, etc.) o cualquier otra herramienta de mensajería. Tampoco se debe facilitar, ni mencionar a otros en una conversación, o comunicación de cualquier tipo, tanto si se encuentran dentro de la institución, como cuando se encuentren en lugares externos.

8. La vigencia de la contraseña será de 90 días, es decir que, finalizado este periodo, los sistemas o el usuario deberán solicitar o realizar respectivamente, el cambio de la misma.

9. La cuenta de usuario de los funcionarios tendrá el siguiente formato “napellido”, siendo “n” la primera letra de su nombre. En caso de coincidencia de los apellidos se agregará al final la primera letra de su segundo apellido.

C. UTILIZACIÓN DE LOS RECURSOS DE RED.

1. La administración y control de todos los recursos y servicios informáticos de la Superintendencia de Compañías, Valores y Seguros es responsabilidad de la Dirección Nacional de Tecnología de Información y Comunicación.

2. Todos los recursos y servicios informáticos deberán ser utilizados para trabajos que contribuyan al cumplimiento de los objetivos del Plan Estratégico Institucional de la Superintendencia de Compañías, Valores y Seguros.

3. Las estaciones de trabajo, dispositivos de almacenamiento externo, software y cualquier recurso informático asignado, deberán ser para uso exclusivo de las funciones y responsabilidades asignadas a los funcionarios de la Superintendencia de Compañías, Valores y Seguros.
4. El funcionario será responsable del buen de los recursos tecnológicos que tenga bajo su custodia o a los que tenga acceso para el cumplimiento de su trabajo.

5. Es obligación del funcionario reportar cualquier riesgo de seguridad potencial que pudiera afectar cualquier recurso informático.

6. Todo funcionario deberá mantener su estación de trabajo asignada cumpliendo con las normas de seguridad establecidas y, deberá bloquear la estación de trabajo cuando tenga que ausentarse temporalmente de su puesto de trabajo a fin de proteger la información de accesos no autorizados.

7. La Dirección Nacional de Tecnología de Información y Comunicación capacitará a los funcionarios sobre cualquier tema tecnológico, inherente a sus funciones, cuando sea requerido.

8. Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Dirección Nacional de Tecnología de Información y Comunicación, en la cual los funcionarios realicen la exploración de los recursos informáticos en la red de la Superintendencia de Compañías, Valores y Seguros, con fines de detectar y explotar una posible vulnerabilidad, así como de las aplicaciones que sobre la red operen.

9. Ningún funcionario debe probar o intentar explotar fallas de la seguridad informática, identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por la Dirección Nacional de Tecnología de Información y Comunicación.

10. Está prohibido realizar actividades que pongan en riesgo los controles de la seguridad informática o que genere interrupción a la red o servicios haciendo uso de herramientas de hardware o software, así como realizar pruebas a los controles de la infraestructura tecnológica. Ningún funcionario o persona externa podrá probar o intentar comprometer los controles internos.

11. Está terminantemente prohibido escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de software malicioso (malware) que pueda afectar o dañar el desempeño o acceso de las computadoras, a la red o a la información de la Dirección Nacional de Tecnología de Información y Comunicación; será considerado como una falta grave.

12. Toda actividad que involucre el uso de recursos informáticos de la Superintendencia de Compañías, Valores y Seguros deberá informarse y coordinarse con la Dirección Nacional de Tecnología de Información y Comunicación.

13. Está terminantemente prohibido a los funcionarios de la Superintendencia de Compañías, Valores y Seguros abrir o desarmar los equipos informáticos directamente o con la intervención de terceros. Únicamente los funcionarios de la Dirección Nacional de Tecnología de Información y Comunicación o personal autorizado por la misma, podrá llevar a cabo cualquier tipo de mantenimiento en los equipos informáticos.

14. Los funcionarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previniendo así la perdida involuntaria de información derivada del proceso de reparación. Para el efecto, podrá solicitar ayuda a un funcionario de la Dirección Nacional de Tecnología de Información y Comunicación.

15. Los funcionarios de la Superintendencia de Compañías, Valores y Seguros deberán regirse por lo establecido en los procedimientos del área de bienes para los casos de: vacaciones, salida de los equipos informáticos, desaparición, hurto o extravío.

D. UTILIZACIÓN DEL CORREO ELECTRÓNICO INSTITUCIONAL.

1. Únicamente se asignará cuenta de correo electrónico a todos los servidores de la Superintendencia de Compañías, Valores y Seguros.

2. Los funcionarios deberán utilizar el servicio de correo electrónico institucional provisto por la Superintendencia de Compañías, Valores y Seguros única y exclusivamente en los recursos tecnológicos que le hayan sido asignados por la Institución. Si el funcionario tuviere la necesidad de revisar su correo desde otro equipo o servicio externo, deberá contar con la autorización del Intendente de su Área y de la Dirección Nacional de Tecnología de Información y Comunicación.

3. Está terminantemente prohibido usar o manipular cuentas de correo electrónico asignadas a otros funcionarios y recibir mensajes institucionales en cuentas externas de correo. El uso del correo electrónico es estrictamente personal y para fines laborales dentro de la institución.

4. Está terminantemente prohibido a los funcionarios interceptar, revelar o ayudar a terceros a revelar las comunicaciones vía correo electrónico, así como también falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

5. La información que se recibe en el correo electrónico, así como los archivos adjuntos son propiedad de la Superintendencia de Compañías, Valores y Seguros.

6. Es responsabilidad de los funcionarios de la Superintendencia de Compañías, Valores y Seguros el reportar a la Dirección Nacional de Tecnología de Información y Comunicación la presencia de correos sospechosos con archivos o *links* adjuntos, evitando acceder, abrir, ejecutar o descargar su contenido sin supervisión de un Especialista de Tecnología. La inobservancia de este punto será considerada una falta grave y una violación a la seguridad de la infraestructura tecnológica.
7. Solo deben ser marcados como urgentes los correos que realmente ameritan serlo. De la misma manera se debe solicitar acuse de recibido y de lectura cuando el caso lo amerite.

8. Está terminantemente prohibido el envío de correos masivos. Serán habilitará esta opción únicamente a los funcionarios que cuenten con la autorización del Intendente o Director de su área y de la Dirección Nacional de Tecnología de Información y Comunicación.

9. Está terminantemente prohibido enviar información con algún contenido del cual no tenga los derechos correspondientes o no se señale la fuente debidamente. (ejemplo: material protegido por el derecho de autor).

10. Los correos deben ser dirigidos a las personas que requieran de la información. No se deberá agregar destinatarios (con copia o con copia oculta) ajenos al tema tratado. Por ningún concepto deben enviar correos a nivel nacional con temas que no sean de interés institucional quedando prohibidos correos referentes a despedidas, agradecimientos, pasquines, asociaciones de empleados, cooperativa de ahorro y crédito, etc.

11. Las asociaciones de empleados, cooperativas de ahorro y crédito o cualquier otra organización que agremie a empleados de la Superintendencia de Compañías, Valores y Seguros deberán crear una cuenta propia en cualquier servicio de correo electrónico gratuito como Hotmail, Gmail o Yahoo.

12. Las organizaciones gremiales de los empleados de la Superintendencia de Compañías, Valores y Seguros, deberán solicitar permisos para poder registrar las cuentas creadas, para poder realizar el envío de correos masivos informativos sólo a los agremiados. Estos correos deberán respetar las normas establecidas en los puntos del 1 al 10. Caso contrario, serán bloqueados automáticamente.

13. Se prohíbe a cualquier representante o empleado perteneciente a una asociación, cooperativa o gremio de empleados de la Superintendencia de Compañías, Valores y Seguros, el uso de las cuentas institucionales para el envío de correos masivos.

14. Queda prohibido el envío de correo electrónico sobre temas ajenos al trabajo que cada funcionario desempeña en la institución, tales como cadenas de correos, archivos de ocio, diversión, contenido obsceno, pornográfico, difamatorio, degradante o que viole la privacidad, que afecte la integridad moral de las personas en especial de aquellas que forman parte de la Superintendencia de Compañías, Valores y Seguros o que afecte la imagen de la institución, actividades mercantiles, mensajes religiosos, videos, leyendas e imágenes de cualquier tipo que no estén relacionados con la Institución.

15. La Superintendencia de Compañías, Valores y Seguros se reserva el derecho de acceder y revelar todos los mensajes enviados a través del correo electrónico para cualquier propósito y revisar las comunicaciones realizadas a través de este medio de cualquier funcionario, una vez que se haya comprobado que el funcionario ha comprometido la seguridad, violando políticas de seguridad o realizando acciones prohibidas en esta normativa.

16. El tamaño máximo permitido de un mensaje de correo electrónico, incluyendo los archivos adjuntos y contenido, no podrá ser mayor de 5 Megabytes. Se excluye de esta restricción a los permisos solicitados por los Intendentes para su uso o el de otros funcionarios.

17. Si fuera necesario leer información de un funcionario ausente, este debe re-direccionar el correo a otra cuenta de correo interna, quedando prohibido hacerlo a una cuenta de correo electrónico externa a la Superintendencia de Compañías, Valores y Seguros.

18. El correo electrónico de los funcionarios tendrá el mismo formato usado para el acceso a la red, es decir *napellido@supercias.gob.ec* siendo "n" la primera letra de su nombre. En caso de coincidencia de los apellidos se agregará al final la primera letra de su segundo apellido.

E. UTILIZACIÓN DEL SERVICIO DE INTERNET.

1. La Dirección Nacional de Tecnología de Información y Comunicación proveerá el acceso a Internet a los servidores que se encuentren debidamente autorizados y registrados en la Superintendencia de Compañías, Valores y Seguros.

2. El acceso a internet será restringido. Únicamente se dará accesos especiales a funcionarios dependiendo de las funciones o cargo y deberá ser autorizado por el Intendente del área solicitante y la Dirección Nacional de Tecnología de Información y Comunicación. Todo acceso especial también contará con bloqueos a sitios prohibidos según lo establecido en la presente política.

3. El acceso a internet provisto a los funcionarios de la Superintendencia de Compañías, Valores y Seguros es exclusivamente para su rol asignado dentro de la Intendencia a la que pertenece.

4. El acceso a internet se realizará mediante el uso de los recursos informáticos (red privada física o inalámbrica) provistos por la Superintendencia de Compañías, Valores y Seguros. Esto no incluye a los dispositivos móviles personales de los servidores.

5. Está terminantemente prohibido el acceso a internet a través de cualquier medio personal de propiedad del funcionario (módems externos o dispositivo móvil) en las estaciones de trabajo propiedad de la Superintendencia de Compañías, Valores y Seguros. Esto aplica también para los equipos que son propiedad del funcionario.

6. Está prohibido, sin excepción jerárquica, el acceso a contenido pornográfico, religioso, de turismo, de juegos, drogas, violencia, cualquier tipo de contenido que sea considerado inapropiado y que no tenga relación con las actividades de la Superintendencia de Compañías, Valores y Seguros. Esta es una norma básica y por ningún concepto puede considerarse excepciones.

7. Para la compra de pasajes y hospedaje para funcionarios, se concederá el permiso pertinente a la persona que cumpla con el rol respectivo, con la debida autorización del Director de la Dirección Administrativa.

8. El servicio de internet provisto por la Superintendencia de Compañías, Valores y Seguros se destinará para atender los servicios externos o internos que permite ejecutar los diferentes procesos institucionales. Por lo tanto, no existe la obligación por parte de la SCVS, ni de la Dirección Nacional de Tecnología de Información y Comunicación, de liberar el acceso internet a los dispositivos personales móviles (smartphones, tabletas o cualquier otro tipo de dispositivo) a los funcionarios o de personal externo dentro de la institución.

F. PUBLICACIONES EN LA PÁGINA WEB.

1. La administración del contenido especializado, que requiera su publicación en el portal web institucional es responsabilidad del funcionario que se designe como coordinador de contendido de cada área.

2. El coordinador de contenido del área es el responsable de subir la información al portal web institucional. Este contenido debe ser aprobado por la autoridad competente en cada área.

3. Todos los contenidos noticiosos de la Superintendencia de Compañías, Valores y Seguros, que requieran su publicación en el portal web institucional son responsabilidad de la Dirección Nacional de Imagen Corporativa y Comunicación Social.

4. Los contenidos dentro de la web institucional deben reflejar el respeto por la dignidad e integridad de otras entidades y personas, evitando transgredir las leyes y buenas costumbres; no puede ser de carácter publicitario, comercial, pornográfico o subversivo.

5. Toda publicación debe respetar la normativa ecuatoriana vigente en materia de derechos de autor, así como las normas internacionales de derechos de autor, registro de marcas, entre otras relacionadas.

6. Toda información y material que no sea de dominio público, tomado de otro sitio en Internet, debe obtener previamente la autorización expresa y escrita de su propietario o autor. Cuando se haga referencia al contenido publicado por otras fuentes debe quedar especificado en el sitio su autor o fuente.

7. Se podrá publicar documentos en formatos jpg, gif, png, xls, xlsx, doc, docx, ppt, pptx, mp3, pdf, zip. Cualquier otro formato requiere de autorización previa de la Dirección Nacional de Imagen Corporativa y Comunicación Social y de la Dirección Nacional de Tecnología de Información y Comunicación.

8. Se deberá tener especial cuidado en la redacción y la ortografía de la información que se publique y será responsabilidad exclusiva del funcionario que solicite la publicación.

G. SOFTWARE AUTORIZADO.

1. Todo software que se encuentre instalado en los servidores, estaciones de trabajo y portátiles propiedad de la Superintendencia de Compañías, Valores y Seguros, deberá contar con licencias autorizadas en cumplimiento con la Norma de Control Interno 410-07 Desarrollo y adquisición de software aplicativo de la Contraloría General del Estado.

2. Está terminantemente prohibido que los funcionarios instalen cualquier tipo de programa (software) en sus estaciones de trabajo, servidores o cualquier equipo conectado a la red de la Superintendencia de Compañías, Valores y Seguros, que no esté autorizado por la DNTIC.

3. Los funcionarios que requieran la instalación de software que no sea propiedad de la SCVS, deberán justificar su uso y solicitar su autorización a la Dirección Nacional de Tecnología de Información y Comunicación a través de memorando firmado por el Director o Intendente del área respectiva, indicando la(s) estación(es) de trabajo donde se instalará el software y el período de tiempo que permanecerá instalado.

4. En el caso de ser software libre, a más de la justificación y autorización del Intendente del área, deberá adjuntar el proyecto por el cual requiere la instalación del mismo de manera indefinida. Para dicho efecto se deberá realizar el Plan de Gestión, considerando el riesgo del software a instalarse.

5. La lista del software autorizado para el uso de los funcionarios de la Superintendencia de Compañías, Valores y Seguros se encuentra detallada en el Anexo I de la presente Política de Seguridad Informática y Normas de Privacidad y Disponibilidad de la Infraestructura Tecnológica.

H. RESPALDO DE LA INFORMACIÓN EN LOS SERVIDORES.

1. La Dirección Nacional de Tecnología de Información y Comunicación junto con el Coordinador Nacional de Producción e Infraestructura y el Coordinador Nacional de Desarrollo y Datos, deberán establecer la arquitectura (hardware y software), procesos, procedimientos y controles necesarios para respaldar la información de los servidores instalados en los Centros de Cómputo de las

ciudades de Guayaquil y Quito, así como de los servidores en las Intendencias Regionales.

2. Los respaldos deberán ser realizados según lo determina el "Procedimiento de respaldo y recuperación de la información".

3. La Dirección Nacional de Tecnología de Información y Comunicación asignará a un Especialista de Tecnología la función para el monitoreo y control permanente del respaldo en las ciudades de Guayaquil, Quito e Intendencias Regionales.

I. RESPALDO DE LA INFORMACIÓN EN LAS ESTACIONES DE TRABAJO Y PORTÁTILES.

1. Los funcionarios son responsables de realizar la copia de los documentos sensibles y críticos para realizar su trabajo, en el repositorio que será provisto de manera coordinada y justificada con la Dirección Nacional de Tecnología de Información y Comunicación.

2. La Dirección Nacional de Tecnología de Información y Comunicación realizará un respaldo quincenal de la información contenida en el repositorio que fuere asignado a cada área de trabajo.

3. La Dirección Nacional de Tecnología de Información y Comunicación asignará a un Especialista de Tecnología la función para el monitoreo y control permanente del respaldo.

J. ACCESO REMOTO (VPN).

1. Está terminantemente prohibido el acceso a redes externas vía VPN. Cualquier excepción deberá ser documentada y contar con la autorización de la Dirección Nacional de Tecnología de Información y Comunicación.

2. Los funcionarios no deben establecer conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo FTP u otro tipo de producto para la transferencia no segura de información empleando la infraestructura de la red de la Superintendencia de Compañías, Valores y Seguros, sin la autorización previa de la Dirección Nacional de Tecnología de Información y Comunicación.

3. Está terminantemente prohibido la conexión o administración remota de equipos por parte de los funcionarios mediante el uso de software como TeamViewer,

Real VNC, LogMeIn, AnyDesk, entre otros, a equipos externos conectados a Internet fuera de la red local de la Superintendencia de Compañías, Valores y Seguros, si previamente no ha sido coordinado, autorizado y con el debido soporte de la Dirección Nacional de Tecnología de Información y Comunicación.

4. Toda conexión remota a la red Institucional de la Superintendencia de Compañías, Valores y Seguros deberá realizarse mediante un protocolo de conexión seguro con cifrado básico VPN, el mismo que se encontrará definido por la Dirección Nacional de Tecnología de Información y Comunicación.

5. Todo permiso otorgado para una conexión hacia la red institucional de la Superintendencia de Compañías, Valores y Seguros deberá eliminarse una vez finalice el periodo de tiempo solicitado.

6. Cualquier funcionario que requiera acceso a la red institucional de la Superintendencia de Compañías, Valores y Seguros desde una ubicación remota deberá solicitarlo a la Dirección Nacional de Tecnología de Información y Comunicación, previa autorización por el Director Nacional de su área y justificando las razones de la solicitud y el tiempo que requerirá el acceso.

K. USO DE DISPOSITIVOS EXTERNOS

1. Está terminantemente prohibido el uso de dispositivos de almacenamiento externo, discos duros, memorias USB, en las estaciones de trabajo de los funcionarios; para lo cual la Dirección Nacional de Tecnología de Información y Comunicación deberá establecer los mecanismos necesarios para su bloqueo permanente.

2. Los funcionarios que requieran por sus funciones la utilización de dispositivos de almacenamiento externo deberán solicitarlo a la Dirección Nacional de Tecnología de Información y Comunicación, indicando las razones de la solicitud. La Dirección Nacional de Tecnología de Información y Comunicación implementará los mecanismos necesarios para conceder a estos funcionarios los accesos a estos dispositivos con todas las seguridades que el caso amerite.

L. TELETRABAJO

1. Los funcionarios no deberán utilizar conexiones poco confiables (conexiones Wi-Fi abiertas, redes públicas municipales, de hoteles, bibliotecas, locutorios, etc.) para conectarse a la red institucional.

2. Los funcionarios no deberán utilizar soluciones de administración remota gestionadas por terceros como pueden ser TeamViewer, Real VNC, LogMeIn, AnyDesk si previamente no ha sido coordinado, autorizado y con el debido soporte de la Dirección Nacional de Tecnología de Información y Comunicación.

3. Los funcionarios deberán permanecer alerta respecto a correos electrónicos fraudulentos, ante cualquier duda o sospecha, sobre una amenaza, phishing o malware, deben contactarse con la Dirección Nacional de Tecnología de Información y Comunicación.

4. Si el funcionario trabaja con equipo propio y este es compartido en el hogar, deberá crear un perfil nuevo específico para trabajar.

5. Si los funcionarios realizan el teletrabajo con un equipo de la institución en su casa, este no debe ser compartido con ninguna otra persona. Además, este equipo podrá ser auditado una vez regrese a la institución, por lo que está prohibida la instalación de software, que no ha sido coordinado y aprobado por la Dirección Nacional de Tecnología de Información y Comunicación.

6. Los funcionarios deberán establecer medidas para evitar el acceso de forma fortuita a información institucional por personas ajenas, como familiares o amigos. Por ejemplo, bloquear siempre el equipo cuando deba realizar una pausa, establecer tiempos para la suspensión del equipo o dejarlo apagado cuando haya terminado la jornada de teletrabajo.

7. Los funcionarios deberán guardar en lugar seguro el dispositivo mientras no se utiliza.

8. Los funcionarios, para evitar la pérdida o robo de equipos portátiles, deberán tomar medidas como: no dejarlo en el vehículo (aunque no esté a la vista), no dejarlo desatendido, evitar sacarlo de casa si no es necesario, etc.

9. Los funcionarios evitaran, de ser posible, el uso de dispositivos móviles (tablets y equipos celulares) para acceder a datos o manejar documentación institucional interna.

10. Si los funcionarios necesitan hacer uso de equipos móviles se deberán tomar las siguientes medidas de seguridad:

    a. Limitar el acceso al dispositivo mediante un bloqueo con contraseña, patrón o similar.

b. Cifrar la memoria del dispositivo en caso de contener información sensible.
c. Establecer medidas para poder localizar el dispositivo o hacer un borrado remoto del dispositivo en caso de pérdida o robo.
d. Contar con una herramienta para hacer copias de seguridad de la información del dispositivo.
e. Tomar las medidas necesarias para prevenir y detectar malware en los dispositivos móviles.
f. Mantener activas las medidas de seguridad de los dispositivos. Ej.: permisos de administrador o permitir instalar software de fuentes no fiables.
g. Instalar siempre las últimas actualizaciones de seguridad de los programas y sistemas operativos.
h. Desactivar las conexiones inalámbricas que no se utilicen como el Bluetooth, Wi-Fi o NFC.

11. Los funcionarios deben cerciorarse de que los equipos desde donde se conectan para el Teletrabajo tienen sistemas operativos debidamente parchados y software actualizado.

12. Los funcionarios deben cerciorarse de que los equipos desde donde se conectan para el Teletrabajo tienen instalado software antivirus y que este se encuentra debidamente actualizado.

13. Los funcionarios deberán periódicamente (por ejemplo, una vez por semana) respaldar la información con que trabajan en unidades de almacenamiento externas personales (Discos Duros Externos USB), y mantener estas unidades de almacenamiento en un lugar seguro.

14. Al finalizar la jornada de teletrabajo los funcionarios deberán:

    a. Cerrar todas las conexiones (VPN, servidores y páginas web) utilizando cuando sea posible la opción “desconectar” o “cerrar sesión”.
    b. Eliminar información temporal prestando especial atención a la carpeta de descargas, papelera de reciclaje, o posibles carpetas perdidas que se dejen en “Mis documentos”.
    c. Utilizar herramientas de borrado seguro para eliminar los ficheros en caso de información sensible o especialmente confidencial.
    d. Si se han utilizado certificados digitales, estos deben ser borrados de forma segura.
    e. Asegurarse de retirar cualquier memoria USB, CD o DVD que se haya utilizado en el equipo.

f. Borrar el histórico de navegación, así como las cookies, y otros datos del navegador web, prestando especial atención a las contraseñas recordadas.

15. Los funcionarios deberán cumplir, a cabalidad, la política de seguridad informática y normas para la privacidad y disponibilidad de la infraestructura tecnológica.

M. PROPIEDAD INTELECTUAL

1. Todo proceso de diseño de especificaciones funcionales, flujos y/o software desarrollado dentro de la Superintendencia de Compañías, Valores y Seguros deberá ser registrado en el Servicio Nacional de Derechos Intelectuales (SENADI) y contará con la documentación de soporte que garantice su propiedad intelectual.

ANEXO I

SOFTWARE AUTORIZADO

ANEXO II

PROCEDIMIENTO DE RECUPERACIÓN Y RESPALDO

ANEXO III

FORMATO ACUERDO DE CONFIDENCIALIDAD

ANEXO IV

SOFTWARE DE VIDEOCONFERENCIA EN MODALIDAD TELETRABAJO