SUPERINTENDENCIA DE PUERTOS Y TRANSPORTE

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

DOCUMENTO VERSION 28/12/16

Bogotá, diciembre de 2016

TABLA DE CONTENIDO

1 OBJETIVO

La política de Seguridad Informática tiene como objetivo principal, establecer reglas claras sobre el buen uso de los sistemas informáticos y de comunicaciones de la Superintendencia de Puertos y Transporte por parte de usuarios, administradores o terceros. De igual manera, proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.

La política de Seguridad Informática, busca establecer controles administrativos y operativos, que regulen de manera efectiva el acceso de los usuarios a los sistemas a nivel de aplicación, sistema operativo, base de datos, red y acceso físico; asegurar la implementación de las medidas de seguridad comprendidas en esta política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

2 ALCANCE

Esta Política abarca todo el ámbito de la Superintendencia de Puertos y Transporte, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la Superintendencia de Puertos y Transporte a través de contratos o acuerdos con terceros. Ningún empleado, funcionario, contratista, departamento, grupo, oficina, comité, organización o unidad operativa está exenta de estas políticas.

De igual manera comprende a los datos e información de la Superintendencia de Puertos y Transporte, sin importar la presentación o formato de almacenamiento ni su localización, propósito, consideraciones de custodia o uso original.

3 DEFINICIONES

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

- **Confidencialidad:** Garantizar que todos los recursos informáticos estén protegidos contra uso no autorizado o revelaciones accidentales. Asegurar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** Establecer mecanismos y métodos de procesamiento para garantizar que toda la información que se maneje se encuentre libre de errores y/o corrupción por personas o procesos no autorizados. Salvaguardar que la información se mantenga con exactitud, tal como fue generada, sin ser manipulada ni alterada.
- **Disponibilidad:** Garantizar que la información se encuentre sólo a disposición de las personas, procesos o aplicaciones que deben tener acceso a ella y en el momento que así lo requieran.
- **Información:** Conjunto de datos procesados y organizados.
- **Amenaza:** Circunstancia que tiene el potencial de causar daño o una perdida. Las amenazas pueden materializarse dado el lugar a un ataque en un equipo.
- **Vulnerabilidad:** debilidad d un sistema de información que puede ser utilizado para causar daños específicos.
- **Riesgo:** Posibilidad que una amenaza se materialice, dando a lugar un ataque a un componente tecnológico.

4 APLICABILIDAD

Esta política aplica para todos los funcionarios, contratistas, personal temporal, practicantes y demás personas que ingresen a los sistemas de información o instalaciones de la Superintendencia de Puertos y Transporte.

5 POLITICAS

5.1 POLITICA DE SEGURIDAD DE LA INFORMACION.

Cumpliendo con lo establecido en las actividades definidas para desarrollar la implementación del modelo de sistema de gestión de seguridad de la información para la Superintendencia de Puertos y Transporte se definen las siguientes políticas que determinan lo siguiente:

5.1.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Superintendencia de Puertos y Transporte se compromete a establecer las siguientes funciones, roles y equipos de trabajo, que serán parte esencial de la implementación, ejecución y desarrollo del sistema de gestión de seguridad de la información.

Comité de Seguridad de la Información: Procederá a revisar y proponer a la máxima autoridad de la Superintendencia de Puertos y Transporte para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad; aprobar las principales iniciativas para incrementar la seguridad de la información , de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información; garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios; promover la difusión y apoyo a la seguridad de la información dentro de la Superintendencia de Puertos y Transporte y coordinar el proceso de administración de la continuidad de las actividades del Organismo.

Coordinador del Comité de Seguridad de la Información, será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente política.

Oficial de Seguridad de la Información, cumplirá funciones relativas a la seguridad de los sistemas de información de la Superintendencia de Puertos y Transporte, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

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

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

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

El Responsable del Área Jurídica verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la Superintendencia de Puertos y Transporte con sus funcionarios y con terceros.

El Superintendente tiene a cargo las siguientes responsabilidades:

- Aprobar las políticas, los procedimientos y estándares alineados con los requerimientos técnicos y de negocio.
- Aprobar nuevas políticas de Seguridad a la organización cuando sea necesario.

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

5.1.2. GESTIÓN DE ACTIVOS.

La Superintendencia de Puertos y Transporte debe tener un perfecto conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Activos como:

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

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

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

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de 6 meses.

El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable del Área de Informática y el Responsable de cada Unidad Organizativa.

El levantamiento de información para la identificación de los activos de información deberá realizarse mínimo una vez al año o cuando se cree un nuevo activo de información no incluido en el inventario.

Será responsabilidad dEl Oficial de Seguridad de La Información su cumplimiento apoyado con las diferentes áreas funcionales de la Superintendencia de Puertos y Transporte. Dentro del inventario deberán incluirse al menos lo siguiente:

- Infraestructura: Física, Tecnología Hardware y Tecnología Software
- Información: Electrónica, Papel
- Gente: Dueños de la información, Dueños de los activos, Usuarios
- Servicios críticos de la Superintendencia de Puertos y Transporte.

El levantamiento de información deberá realizarse a través de cuestionarios los cuales serán distribuidos al personal de administración técnica y no técnica o canalizados a través de los dueños de los activos de información, si es que estos ya fueron identificados en procesos anteriores. El cuestionario también podría utilizarse durante las visitas de revisión y las entrevistas al personal.

La información mínima por cada uno de los activos identificados debe ser lo siguiente:
Nombre del activo, Proceso que apoya, Descripción, Tipo de Activo, Dueño del activo, Descripción del almacenamiento utilizado y Tipo de información que procesa y/o almacena.

Todos los aplicativos o sistemas de información necesariamente deben tener asignado un "propietario", el cual es el encargado de definir los niveles de privacidad de la información, así como los usuarios y permisos que cada uno deba tener sobre ella.

La valoración de los activos deberá realizarse y/o revisarse cada vez que se desarrolle el proceso de identificación de activos en la organización, es decir, como mínimo una (1) vez al año o cuando se cree un nuevo activo de información no incluido en el inventario.

La Superintendencia de Puertos y Transporte es propietaria de la información almacenada en dispositivos electrónicos e informáticos que sean propiedad o arrendada por la Superintendencia de Puertos y Transporte. Debe asegurarse, a través de medios legales y/o técnicos, que la información de propiedad privada está protegida con los controles adecuados de seguridad.

La información debe ser clasificada en términos de su valor y criticidad para la Superintendencia de Puertos y Transporte, así como de cualquier requerimiento legal.

Los dueños de los activos de información son responsables de asignar la clasificación correspondiente a los activos bajo su responsabilidad.

El dueño de la información es responsable por la actualización de la clasificación de la información de acuerdo a los cambios de la Superintendencia de Puertos y Transporte.

El dueño de la información es autónomo de reclasificarla cuando lo considere necesario y debe cambiar del rotulo o etiqueta y notificar a los usuarios y custodios

Los controles de seguridad asignados a los activos deben corresponder a la clasificación asignada.

La información se deberá clasificar de acuerdo a los siguientes parámetros:

Tipo de Información	**Descripción**
Reservada	Información que compete exclusivamente a Directivos de la Superintendencia de Puertos y Transporte, cuya perdida, alteración o divulgación no autorizada afecte derechos de terceros, involucre estrategias de negociación y competitividad o pueda causar daños y perjuicios graves a la imagen de la Superintendencia de Puertos y Transporte y clientes.
Confidencial	Información cuya divulgación, perdida o alteración no autorizada, podría resultar en desprestigio moderado o perdidas económicas para la Superintendencia de Puertos y Transporte. Puede tener acceso a esta información todo el personal de la Superintendencia de Puertos y Transporte y terceros que hayan firmado un convenio de confidencialidad y cuyo contrato los obligue a cumplir con lo establecido.
Uso Interno	Información requerida por empleados, contratistas, clientes o proveedores para el desarrollo normal de sus actividades o funciones, tendrá acceso a esta información todo el personal directo de la Superintendencia de Puertos y Transporte y los terceros que hayan firmado un convenio de confidencialidad y cuyo contrato los obligue a cumplir con lo establecido.
Publica	Información cuya distribución, publicación o divulgación a empleados, terceros o público en general ha sido formalmente autorizada y distribuida por los canales de comunicación formalmente establecidos (masivos, o cualquier otro medio). La aparición de esta información en los medios de comunicación masiva no debe implicar ningún impacto negativo para la Superintendencia de Puertos y Transporte.

Tabla. Niveles de clasificación de la información

Los funcionarios de la Dirección de Informática son claramente custodios, así como los administradores de sistemas locales. Siempre que la información sea almacenada en un computador personal, el usuario inmediatamente será su custodio.

Los usuarios son responsables de familiarizarse y atender todos los aspectos de la política de seguridad. En caso de existir dudas por parte de los usuarios con respecto a la manipulación apropiada de la información estas deben ser consultadas con el custodio o dueño.

Es deber de los responsables efectuar la clasificación de la información de acuerdo con los patrones definidos por este procedimiento.

La información, datos y documentos deben ser claramente marcados, de manera que todos los usuarios estén enterados de su nivel de clasificación.

Se debe firmar un acuerdo de confidencialidad con terceras partes, en caso de requerir entregar información electrónica o escrita confidencial o interna, con las restricciones de su uso.

Se deben utilizar los mecanismos apropiados de control de acceso a la información dependiendo de su nivel de clasificación.

Los empleados, contratistas o terceros no pueden tomar información secreta, confidencial o interna cuando dejan de trabajar para la Superintendencia de Puertos y Transporte.

Información clasificada como confidencial/reservada o interna, debe ser enviada a la impresora, evitando que personal no autorizado tenga acceso a ésta.

La información que sea catalogada como confidencial/reservada que requiera ser transmitida por medios de comunicación públicos debe utilizar un esquema de cifrado con el fin de proteger su confidencialidad e integridad.

En el caso de envío por medio de correo electrónico fuera de la Superintendencia de Puertos y Transporte de información confidencial requiere que el correo vaya firmado y utilice un esquema de cifrado.

Los empleados de los terceros con los cuales la Superintendencia de Puertos y Transporte tiene acuerdos comerciales no deben revelar información confidencial a terceras partes a menos que el originador de la información haya aprobado su revelación y la parte que la reciba haya firmado un acuerdo de confidencialidad.

El Oficial de Seguridad de La Información o quien haga sus veces, verificará que los activos de información se encuentren debidamente etiquetados de acuerdo a su clasificación.

Destrucción de Información confidencial/reservada o interna: Cuando ya no se requiera una información clasificada como confidencial/reserva o interna, debe ser destruida mediante un método aprobado por seguridad de la información.

Se debe borrar la información confidencial/reservada o interna de los medios magnéticos por un método o programa aprobado por Seguridad de la Información, cuando se requiere deshacerse del medio o equipo, enviar a servicio técnico o devolver a su proveedor.

En caso de enviar los equipos a mantenimiento o asignarle el equipo a una persona diferente que contenga información confidencial/reservada, la información debe ser borrada de manera que no sea posible su recuperación.

Por ningún motivo se deben reutilizar hojas que contengan información confidencial de la Superintendencia de Puertos y Transporte (firmas de clientes y directivos, datos financieros, cifras y

tablas, facturas, etc.), esta documentación debe ser destruida.

Los datos en medios electrónicos deben ser borrados de manera confiable. Se debe formatear totalmente o destruir físicamente los medios (CD's, Cintas, USB) donde existan copias de información confidencial.

Los equipos portátiles que contengan información confidencial/reservada, deben tener los mecanismos necesarios para evitar que ante la pérdida del equipo una persona no autorizada pueda acceder a la información almacenada.

Los dispositivos periféricos pertenecientes a los equipos (memoria, baterías, fuentes de poder, discos duros, monitores, etc.), y elementos de control como son etiquetas de licencias, placas de inventario, tarjetas de RFID (Identificadores de Radio Frecuencia), número serial, entre otros, no deben manipularse, retirarse o cambiarse de lugar por ningún motivo. Estos serán verificados a la devolución del equipo y cualquier desperfecto daño o ausencia de los mismos implicara la reposición, cobro al usuario responsable y las medidas disciplinarias a que dé lugar.

Está prohibido extraer información de los sistemas y repositorios de información de la compañía en dispositivos de almacenamiento externo (CD, DVD, USB, Celulares, SmartWatch, Discos Duros, ZIP, entre otros), sin previo conocimiento y autorización formal del Jefe de área y avalado por el Oficial de Seguridad de la Información

Cuando se presente alguna situación en donde el retiro del funcionario implique una investigación interna, el equipo, los medios periféricos y los medios de almacenamiento que se estén utilizando no deberán ser desconectados y entraran a cadena de custodia el tiempo que dure la investigación. Dicha actividad solo puede ser realizada por el Oficial de Seguridad de la Información y será responsabilidad del jefe inmediato del área comunicarse con dicha área.

Todo funcionario de la Superintendencia de Puertos y Transporte, deberá entregar en su totalidad y el mismo día de su retiro o renuncia, los respaldos de información realizados durante su vida laboral en la compañía a su jefe inmediato y al El Oficial de Seguridad de la Información, quien será el encargado de velar por la custodia de estos medios y su posterior envío al área responsable del archivo.

Todo funcionario de la Superintendencia de Puertos y Transporte que posea equipos de la Superintendencia de Puertos y Transporte para el desempeño de sus labores y sea retirado o haya renunciado a la compañía, deberá entregar el dispositivo a su jefe inmediato y a la Coordinacion Administrativa quien será el responsable de custodiar este medio y realizar el proceso de baja respectivo. Los equipos deberán quedar inactiva el mismo día que el funcionario haya sido retirado de la compañía.

Todo funcionario de la Superintendencia de Puertos y Transporte que requiere el uso de su equipo personal (Laptop, Desktop, Tablet, dispositivos móviles) para el desempeño de sus funciones, debe tener la autorización previa del Superintendente.

5.1.3 CONTROL DE ACCESO.

Los empleados de la Superintendencia de Puertos y Transporte pueden acceder, usar y/o compartir información de propiedad de la Superintendencia de Puertos y Transporte sólo en la medida en que esté autorizado y cuya información sea necesaria para cumplir con las tareas asignadas de cada empleado.

Las contraseñas a nivel del sistema y del usuario deben cumplir con la política de contraseñas. Está prohibido el acceso a otra persona, ya sea deliberadamente o por falta de seguridad en su acceso.

Todos los dispositivos de computación deben estar protegidos con un protector de pantalla protegido por contraseña con la función de activación automática establecida en 10 minutos o menos. Debe bloquear la pantalla o cerrar la sesión cuando el dispositivo esté desatendido.

Deben existir procedimientos y estándares formales establecidos para la creación, modificación y eliminación de usuarios, roles y perfiles.

La cuenta de usuario o identificador (ID) debe ser único para los funcionarios y/o las partes interesadas.

Se debe acceder a los sistemas de información o dispositivos de red a través de la cuenta de usuario asignada, la cual debe cumplir con los controles y estándares de seguridad definidos.

La contraseña es personal e intransferible y no puede ser compartida por ningún motivo, la misma debe cumplir con los estándares y controles de seguridad definidos.

La definición de roles y perfiles está basada en el menor privilegio requerido para el correcto desempeño de sus funciones.

Deben existir controles que permitan monitorear las diferentes acciones realizadas por los usuarios garantizando la trazabilidad y registro de evidencias.

Las cuentas genéricas deben tener asignada la responsabilidad de su utilización a un colaborador y deben ser utilizadas exclusivamente para establecer comunicación con otro recurso informático o de red. Dichas cuentas no deben ser de uso personal.

Las cuentas privilegiadas deben ser utilizadas, exclusivamente para el mantenimiento y atención de incidentes sobre los recursos informáticos o de red, las mismas deben ser custodiadas y monitoreadas por el dueño del servicio.

Debe asegurarse que se tienen identificados y/o documentados todos los privilegios y facultades de accesos asignados, asociadas a las diferentes plataformas tecnológicas (sistemas operativos, bases de datos, aplicaciones, repositorios de archivos, etc.)

Los privilegios o facultades asignadas deben ser restringidas o limitadas específicamente a lo que les compete saber, basado en el principio de mínimo privilegio (lo estrictamente necesario).

El área que haga uso de un servicio de información debe especificar claramente y por escrito, la asignación de dueños de la información o autorizadores. Tales declaraciones deben indicar a los individuos que se les ha concedido autoridad para originar, modificar o borrar información específica.

Todas las cuentas de usuario creadas en los sistemas informáticos o de comunicación, deben tener un identificador único y deberán tramitarse mediante un requerimiento de solicitud de acceso debidamente diligenciado de acuerdo al perfil y funciones que va a desempeñar el usuario, y aprobado por su autorizador. siguiendo un procedimiento formal, que asegure el desempeño correcto de la requisición, establecimiento, uso, suspensión y cierre de los accesos solicitados en los elementos y servicios de red, incluyendo las autorizaciones adecuadas.

Los accesos deben bloquearse máximo al sexto (6) intento fallido.

Los sistemas de información deben generar aviso de recordatorio de vencimiento de contraseña máximo con 7 días de anticipación. En ningún proceso de ingreso, los usuarios deberán utilizar la opción “Recordar Contraseña”, esto con el fin de evitar que automáticamente el acceso habilite la aplicación por personas diferentes al titular del equipo.

En cada sistema de información, deberá usar una contraseña con una longitud mínima de 8 caracteres máximo de 10 caracteres.

Ningún sistema de información o elemento de red de la Superintendencia de Puertos y Transporte deben permitir el ingreso sin validar el respectivo usuario y contraseña que permitan validar y registrar el acceso.

Cada sistema de información o elemento de red de la Superintendencia de Puertos y Transporte deberá

forzar el cambio de contraseña cuando el usuario realice el primer acceso. En dado caso que el sistema o dispositivo de red no pueda ejecutar esta obligación, es responsabilidad del usuario cambiar la clave de acceso en los periodos de tiempo definidos en esta política.

Máximo cada 60 días, el sistema automáticamente solicitará al usuario el cambio de su contraseña, el usuario deberá cambiarla en forma inmediata.

Cada usuario tiene permitido establecer máximo tres sesiones en cada sistema de información o de comunicaciones de la Superintendencia de Puertos y Transporte, la concurrencia solo puede ocurrir si se da sobre la misma estación de trabajo.

Para el personal directo que ingrese a la Superintendencia de Puertos y Transporte, el área de Recursos Humanos solicitará los accesos lógicos de Red, Correo Electrónico e Intranet, pero es de aclarar que la responsabilidad sobre el uso de los accesos recae sobre la Dirección a la cual el nuevo funcionario pertenecerá.

Los derechos de acceso a cuentas privilegiadas (Administradores de dominio, cuentas de servicios, administradores de aplicaciones y bases de datos) deben ser revisados semestralmente y cuando existan cambios, se deberá reportar formalmente de acuerdo al procedimiento establecido.

Aquellas cuentas de usuario que su tiempo de inactividad sea igual a 90 días se proceda a inhabilitar. Si pasados 30 días, posterior a la inhabilitación de la cuenta (90+30=120 días) no se presentan accesos se procederá con su eliminación. La responsabilidad de este control es de los administradores de cuentas de usuario de los sistemas.

Las contraseñas nunca deben incorporarse al software desarrollado o modificado por los empleados. Si por alguna necesidad de la Superintendencia de Puertos y Transporte de la operación actual de los sistemas se requiere utilizar contraseñas genéricas en el código fuente de una aplicación para acceder a información de otras aplicaciones o de las bases de datos, la responsabilidad sobre el uso de esta contraseña será estrictamente exclusivo de la Dirección que tiene a cargo el aplicativo que está usando la contraseña.

Todo usuario que olvide o pierda su contraseña de red deberá recuperarla mediante los mecanismos de recuperación automática establecidos para este propósito. En caso no poderlo hacer, porque el sistema de información no tiene está opción, se deberá solicitar a su jefe inmediato la gestión de recuperación de contraseña a través de la mesa de servicio y/o cualquier otro mecanismo formal.
Las contraseñas no deben ser reveladas ni compartidas.

En caso de sospecha de revelación de contraseñas a personas no autorizadas, estas contraseñas deben ser cambiadas inmediatamente.

Las contraseñas no deben ser escritas u olvidadas en un lugar en donde puedan ser del conocimiento de personal no autorizado.

En la creación de las contraseñas, evitar el uso de palabras comunes o que se encuentren en un diccionario y evitar el uso de su nombre, fecha de nacimiento, números telefónicos, o cualquier dato personal que pueda ser del conocimiento de otras personas que laboren en la Superintendencia de Puertos y Transporte.

No se deben permitir dentro de los sistemas informáticos o de comunicación, cuentas de usuario que presenten contraseñas en blanco o nulas.

Deben combinar caracteres alfanuméricos (al menos un número).

El repositorio en donde se almacenan las contraseñas de los sistemas y aplicaciones deben ser almacenadas en forma cifrada de tal forma que no puedan ser comprometidas con técnicas de análisis criptográfico.

Las contraseñas deben viajar cifradas en el momento de autenticación.

5.1.4. POLITICA DE NO REPUDIO.

Para fines de seguridad y mantenimiento de la red, las personas autorizadas dentro de la Superintendencia de Puertos y Transporte pueden supervisar los equipos, los sistemas y el tráfico de la red en cualquier momento.

La Superintendencia de Puertos y Transporte se reserva el derecho de auditar las redes y sistemas periódicamente para asegurar el cumplimiento de la política de seguridad de la información.

Cada sistema de información deberá controlar el registro de máximo las últimas 24 contraseñas utilizadas por el usuario, esto con el fin de evitar la reutilización de las mismas.

El uso de los principales sistemas de la Superintendencia de Puertos y Transporte, debe ser monitoreado con el objetivo de identificar algún intento de intrusión. El monitoreo debe contemplar como mínimo los siguientes puntos:

- Intentos fallidos recurrentes para tener acceso a los sistemas.
- Intentos fallidos recurrentes realizados por un usuario legítimo que excede los privilegios de acceso autorizado.
- Patrón sospechoso de accesos exitosos (ejemplo: día inusual, hora poco usual, ubicación distinta a la habitual).
- Intentos deliberados para evadir los controles de seguridad establecidos.
- Patrones de intrusión sospechosos que potencialmente llevan a la negación del servicio (Caballos de Troya, virus, bombas lógicas, entre otras).
- Altas y bajas de usuarios en sistemas sin una solicitud aprobada correctamente.
- Modificaciones en los privilegios de usuarios sin una solicitud aprobada correctamente.

Los registros de auditoría deben ser respaldados de forma periódica.

El monitoreo de la seguridad debe llevarse a cabo por las áreas responsables de entregar los servicios de seguridad informática a los sistemas de información de la organización, en función de garantizar los niveles apropiados de operación del negocio dentro de la disponibilidad, integridad y confidencialidad requerida, encontrándose dentro de sus responsabilidades:

Proporcionar un reporte periódico mensual de los incidentes de seguridad identificados.

Analizar las alertas generadas por las herramientas tecnológicas de seguridad para detectar posibles eventos de seguridad, generando la documentación que permita identificar el hallazgo, el análisis desarrollado, sus causas y acciones de mejora.

5.1.5 PRIVACIDAD Y CONFIDENCIALIDAD

Esta política contiene una descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente (Ley 1581 de 2012). La política de privacidad debe contener lo siguiente:

Ámbito de aplicación. La política de seguridad del presente capitulo será aplicable a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento. El régimen de protección de datos personales que se establece en la presente política no será de aplicación: a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente política; b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo; c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia; d)

A las bases de datos y archivos de información periodística y otros contenidos editoriales; e) A las bases de datos y archivos regulados por la Ley 1266 de 2008; f) A las bases de datos y archivos regulados por la Ley 79 de 1993. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo.

Asegurarse que los usuarios de terceros que requieren información de la entidad hayan firmado un acuerdo de confidencialidad de la información (NDA – Non Disclosure Agreement por sus siglas en inglés), o en el caso de contratistas, que el acuerdo este incluido como parte del contrato firmado con la entidad. El acuerdo de confidencialidad debe firmarse antes de intercambiar cualquier tipo de información confidencial y tendrá una vigencia de dos (2) años a partir de su firma.

Para los casos en que la entidad lleve a cabo intercambio de información con otras entidades (socios de negocio, clientes proveedores, entidades regulatorias, etc.), deben existir procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información a intercambiar a través de cualquier tipo o infraestructura de comunicaciones, con base a la clasificación de la información, las políticas de seguridad y procedimientos de la entidad

Se debe considerar como intercambio de información todo aquello que puede ser realizado a través del uso de los diferentes tipos de infraestructura de comunicación, incluyendo Internet, correo electrónico, fax, CD's, DVD's, medios removibles de almacenamiento de información, audio, video y medios impresos.

Datos sensibles. Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Tratamiento de datos sensibles. Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;
c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;
d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

Derechos de los Titulares. El Titular de los datos personales tendrá los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;
b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la ley 1581 de 2012;
c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;
e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;
f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Autorización del Titular. En el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
b) Datos de naturaleza pública;
c) Casos de urgencia médica o sanitaria;
d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
e) Datos relacionados con el Registro Civil de las Personas. Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la ley 1581 de 2012.

Suministro de la información. La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos.

Deber de informar al Titular. El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
c) Los derechos que le asisten como Titular;
d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.
e) Parágrafo. El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta.

Personas a quienes se les puede suministrar la información. La información que reúna las condiciones establecidas en la ley 1581 de 2012 podrá suministrarse a las siguientes personas:

a) A los Titulares, sus causahabientes o sus representantes legales;
b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial;
c) A los terceros autorizados por el Titular o por la ley.

Consultas. Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado. El Responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular. La consulta se formulará por el medio habilitado por el Responsable del Tratamiento o Encargado del Tratamiento, siempre y cuando se pueda mantener prueba de esta. La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Reclamos. El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta ley, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:

- El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo. En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.
- Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.
- El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Deberes de los Responsables del Tratamiento. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;
c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;
d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;
g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;
h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;
i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;
j) Tramitar las consultas y reclamos formulados;
k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;
l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;
m) Informar a solicitud del Titular sobre el uso dado a sus datos;
n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Deberes de los Encargados del Tratamiento. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;
d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;
e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;
f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley 1581 de 2012 y, en especial, para la atención de consultas y reclamos por parte de los Titulares;
g) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley;
h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;
i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;
j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;
k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;
l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

5.1.6. INTEGRIDAD.

Todos los sistemas de misión crítica de la Superintendencia de Puertos y Transporte deben:

- Identificar, informar y corregir las fallas del sistema de información.
- Probar actualizaciones de software relacionadas con la corrección de defectos para la eficacia y posibles efectos secundarios sobre los activos de información de la organización antes de la instalación.
- Incorporar corrección de defectos mediante el proceso de gestión de configuración de la organización.

Protección contra código malicioso: Todos los sistemas de la Superintendencia de Puertos y Transporte deben:

- Emplear mecanismos de protección de código malicioso en los puntos de entrada y salida de información y en las estaciones de trabajo, servidores o dispositivos de computación móvil (por ejemplo, correo electrónico, medios removibles y sitios web maliciosos) para detectar y erradicar el código malicioso.
- Actualizar los mecanismos de protección de códigos maliciosos (incluidas las definiciones de firmas) siempre que se disponga de nuevas versiones de acuerdo con la política y los procedimientos de gestión de la configuración organizativa.
- Configurar mecanismos de protección de código malicioso (por ejemplo, análisis en tiempo real, análisis periódicos, detección de códigos maliciosos) para proteger los sistemas y activos de información de la empresa.
- Abordar la recepción de falsos positivos durante la detección y erradicación de códigos maliciosos y el consiguiente impacto potencial sobre la integridad del activo de información.

Monitoreo del Sistema de Información: Todos los Sistemas de la Superintendencia de Puertos y Transporte deben:

- Monitorear eventos en el activo de información y detectar ataques.
- Identificar el uso no autorizado de los activos de información.
- Implementar dispositivos de monitoreo dentro del activo de información para recopilar información esencial determinada por la organización, y para rastrear tipos específicos de transacciones de interés para la organización.
- Aumentar el nivel de actividad de monitoreo de activos de información siempre que exista una indicación de un mayor riesgo para las operaciones y los activos de la organización, basados en información policial, información de inteligencia u otras fuentes creíbles de información.

Asegurarse que los usuarios de terceros que requieren información de la Superintendencia de Puertos y Transporte hayan firmado un acuerdo de confidencialidad de la información (NDA – Non Disclosure Agreement por sus siglas en inglés), o en el caso de contratistas, que el acuerdo este incluido como parte del contrato firmado con la Superintendencia de Puertos y Transporte. El acuerdo de confidencialidad debe firmarse antes de intercambiar cualquier tipo de información confidencial y tendrá una vigencia de dos (2) años a partir de su firma.

Para los casos en que la Superintendencia de Puertos y Transporte lleve a cabo intercambio de información con otras entidades (socios de negocio, clientes proveedores, entidades regulatorias, etc.), deben existir procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información a intercambiar a través de cualquier tipo o infraestructura de comunicaciones, con base a la clasificación de la información, las políticas de seguridad y procedimientos de la Superintendencia de Puertos y Transporte.

5.1.7 DISPONIBILIDAD DEL SERVICIO.

El Administrador y/o Coordinador de Disponibilidad son los responsables de capacitar y suministrar los recursos necesarios para planeación, implementación y ejecución del proceso.

El proceso de Administrar Disponibilidad debe trabajar en conjunto con el proceso de Administrar Niveles de Servicio para alinear y validar que los Niveles de Servicio acordados se mantengan.

El proceso de Administrar Disponibilidad debe integrarse a las políticas generadas por el Sistema de Gestión de Seguridad de la Información ISO/IEC 27001 establecido en la Superintendencia de Puertos y Transporte.

Los planes de Disponibilidad deben tener una vigencia anual, realizando revisiones periódicas durante su vigencia, para realizar los ajustes a los mismos.

El plan de disponibilidad de cada servicio debe mantenerse actualizado para asegurar que se reflejen los cambios acordados y requeridos por el negocio.

El plan de disponibilidad de cada servicio debe contener la información necesaria para administrar los datos y requerimientos de la disponibilidad.

Se debe crear y mantener un seguimiento al plan de disponibilidad con el fin de mejorar el entorno de disponibilidad de los servicios y los componentes de la infraestructura para garantizar los requerimientos de disponibilidad futuros puedan ser cubiertos.

El Comité Directivo en conjunto con el Comité de Seguridad de la información de la Superintendencia de Puertos y Transporte, deben definir una estrategia para la continuidad del negocio, así como desarrollar, documentar, probar y mantener el Plan de Continuidad, que conduzcan a la restauración de los procesos críticos del negocio, con el objeto de dar continuidad en el servicio a sus socios de negocio.

El proceso de administración en la continuidad del negocio deberá incluir los siguientes puntos:

- Generar el Análisis de Impacto al Negocio (BIA).
- Estrategia para la continuidad del negocio.
- Elaborar en el plan de continuidad del negocio.
- Considerar la contratación de seguros para la protección de los activos tecnológicos de la Superintendencia de Puertos y Transporte

Sin excepción, dentro del proceso de desarrollo del plan de continuidad del negocio (BCP) se debe hacer énfasis en mantener niveles de seguridad de información acordes con el resultado del análisis de riesgo y su clasificación, dentro de los procesos alternos utilizados antes, durante y después de la contingencia.

Los documentos e información necesaria para llevar a cabo el proceso de continuidad del negocio deben ser clasificados como información “confidencial”.

La información debe ser copiada y resguardada en un lugar fuera de las instalaciones de la Superintendencia de Puertos y Transporte

La continuidad del negocio debe estar basada en las consideraciones dispuestas en el documento de análisis de impacto al negocio (BIA) el cual incluye los siguientes puntos:

- o Identificar riesgos de interrupción
- o Considerar escenarios de interrupción
- o Análisis de costo beneficio para la mitigación de los riesgos
- o Identificar controles para la mitigación de los riesgos
- o Evaluar el impacto financiero, legal y a clientes

El BIA debe ser utilizado como una herramienta para identificar los procesos críticos del negocio, sus riesgos asociados y los impactos que estos generan, con el fin de facilitar las estrategias de contención y recuperación de acciones durante y después de una interrupción para salvaguardar la vida humana y conservar los activos.

El BIA debe ser actualizado por lo menos una vez al año y cuando se presente un cambio sustancial en la estrategia del negocio, en los procesos críticos de negocio y/o al entorno de la organización.

Es responsabilidad de la Gerencia Seguridad IT de la Información la elaboración de un programa anual de revisión y actualización del BIA.

Cada área critica de la Superintendencia de Puertos y Transporte, está obligada a tener un plan de contingencia desarrollado y alineado con esta política, validado por la Dirección a la que pertenezca dicha área en la Superintendencia de Puertos y Transporte.

Los planes de contingencia deben contener lo siguiente:

- Plan de respuesta a emergencias: ¿Quién debe ser contactado, ¿cuándo y cómo?
- ¿Qué acciones inmediatas deben ser tomadas en caso de ciertos acontecimientos?
- Plan de Sucesión: Describa el flujo de responsabilidad cuando el personal normal no está disponible para desempeñar sus funciones.
- Estudio de datos: Detalle de los datos almacenados en los sistemas, su criticidad y su confidencialidad.
- Criticidad de la lista de servicios: Enumere todos los servicios prestados y su importancia. También explica el orden de la recuperación tanto a corto como a largo plazo.
- Plan de copia de seguridad y restauración de datos: Detalle los datos que se copian, los medios en los que se guardan, donde se almacena estos medios, y con qué frecuencia se realiza la copia de seguridad. También debe describir cómo se recuperan los datos.
- Plan de Reemplazo de Equipo: Describa qué equipo se requiere para comenzar a proporcionar servicios, enumerar el orden en que es necesario, y dónde se puede comprar dicho equipo.

- Gestión de Medios de Comunicación: ¿Quién se encarga de dar información a los medios de comunicación?

Para el caso de los servicios que fueran proporcionados por terceros y que estén relacionados con los procesos críticos del negocio de la Superintendencia de Puertos y Transporte, se deberá revisar las nuevas propuestas (nuevos proveedores o renovaciones) y los contratos existentes (proveedores actuales) a fin de poder identificar los riesgos y documentar las decisiones con relación al nivel de riesgo identificado y su tratamiento (mitigación, aceptación, transferencia o evasión).

El BCP debe ser probado por lo menos una vez al año y cuando se presente un cambio sustancial en la estrategia del negocio, en los procesos críticos de negocio y/o al entorno de la Superintendencia de Puertos y Transporte.

En la ejecución de dichas pruebas deben participar las áreas que den soporte al proceso o áreas críticas del negocio, el grupo responsable de la continuidad del negocio y seguridad Informática. Los resultados de las mismas deben ser documentados en forma detallada, identificando cada una de las actividades y su prioridad de recuperación y sus resultados, identificando puntos de mejoras y estableciendo un plan de trabajo para realizar los ajustes necesarios.

Recursos Humanos será responsable por asesorar en la definición de planes y programas en conjunto con las Gerencias, quienes a su vez serán responsables por suministrar la información necesaria con respecto a las necesidades para la construcción de los planes de formación.

Las necesidades de capacitación de cada área deben estar alineadas a la planeación estratégica de la Superintendencia de Puertos y Transporte y deben ser el resultado de los procesos de acompañamiento.

5.1.8. REGISTRO Y AUDITORÍA.

Todos los sistemas que manejan información confidencial, aceptan conexiones de red o que toman decisiones de control de acceso (autenticación y autorización) registrarán y conservarán el registro de auditoría con la información suficiente para responder las siguientes preguntas:

- ¿Qué actividad se realizó?
- Quién o qué realizó la actividad, incluyendo desde dónde o en qué sistema se realizó la actividad
- ¿Sobre qué o quién se realizó la actividad?
- ¿Cuándo se realizó la actividad?
- ¿Con qué herramienta (s) se realizó la actividad?
- ¿Cuál fue el resultado de la actividad (como éxito vs. fracaso)?

Las siguientes actividades deberán ser registradas en el momento que sean desarrolladas por un sistema:

- Crear, leer, actualizar o eliminar información confidencial, incluyendo información confidencial como por ejemplo las contraseñas;
- Crear, actualizar o eliminar información no cubierta en punto anterior
- Iniciar una conexión de red;
- Aceptar una conexión de red;
- Autenticación y autorización de los usuarios y desconexión de los mismos

Conceder, modificar o revocar derechos de acceso, incluyendo la adición de un nuevo usuario o grupo, cambio en los niveles de privilegios de usuario, cambio de permisos de archivos, cambio de permisos de objetos de base de datos, cambio reglas en el Firewall y cambios de contraseñas de usuario;

Cambios en la configuración de sistemas, redes o servicios, incluida la instalación de software, parches y actualizaciones, u otros cambios de software instalados;

Todos los registros deberán contener los siguientes elementos de forma directa o indirecta:

- Tipo de acción - ejemplos incluyen autorizar, crear, leer, actualizar, eliminar y aceptar conexiones de red.
- Subsistema que realiza la acción - los ejemplos incluyen el nombre del proceso o de la transacción, proceso o identificador de transacción.
- Identificadores (tantos como sean posibles) para el sujeto que solicita la acción - ejemplos incluyen nombre de usuario, nombre de equipo, dirección IP y dirección MAC. Tenga en cuenta que tales identificadores deben ser estandarizados para facilitar la correlación de eventos.
- Identificadores (tantos como sean posibles) para el objeto sobre el que se realizó la acción – ejemplos incluyen nombres de archivo a los que se accede, identificadores únicos de registros a los que se accede en una base de datos, parámetros de consulta utilizados para determinar los registros a los que se accede en una base de datos, nombre de equipo, dirección IP, dirección MAC.
- Fecha y hora en que se realizó la acción, incluida la información pertinente sobre la zona horaria,
- Si la acción fue permitida o denegada por mecanismos de control de acceso.
- Descripción y/o razón de los códigos que indican que la acción fue denegada por el control de acceso, si aplica

Es responsabilidad de los dueños de los activos de información garantizar que estos controles estén habilitados sobre los sistemas de información

El tiempo de retención de los registros de auditoría debe der de un (1) año.

5.1.9. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

La gestión del Incidente de seguridad debe ser prioridad para las áreas encargadas de realizar las actividades de mitigación y normalización y para todas las áreas del negocio a las cuales se les solicite justificación de un incidente de seguridad.

La justificación sobre el comportamiento categorizado como incidente de seguridad debe ser enviada al área de Seguridad de la Información en un periodo no mayor a cinco (5) días hábiles, en caso de no recibir respuesta satisfactoria al incidente generado, se debe escalar al superior inmediato.

Mensualmente el Oficial de Seguridad de la Información, debe realizar una clínica de Incidentes para validar la gestión realizada sobre los incidentes de seguridad.

Realizar perfilamiento de redes y sistemas el cual consiste en la medición de características esperadas de funcionamiento normal. Para tal efecto se debe extraer la siguiente información:

- Promedio de consumo de recursos de un sistema (e.g. CPU, memoria, disco, IOPS)
- Promedio de consumo de recursos de red de un sistema (e.g. BW)
- Checksum de los binarios de un sistema

Mantener los registros de logs y auditoría por lo menos un periodo de seis (6) meses hacia atrás con lo cual se pueden identificar comportamientos normales y anormales de las aplicaciones, sistemas y redes e investigar también indicadores de compromiso e inferir precursores

En caso de un incidente de seguridad debe realizarse una correlación de eventos: Evidencia que un incidente puede ser capturado en diferentes fuentes de información (e.g. FW, IPS, aplicación, etc).

Mantener todos los servidores y equipos de red y seguridad sincronizados con una fuente de reloj, vía NTP. Si la Superintendencia de Puertos y Transporte no cuenta con uno, es posible utilizar un NTP público (e.g. http://tf.nist.gov/tf-cgi/servers.cgi)

Crear y mantener una base de conocimientos actualizada con el fin de documentar incidentes anteriores que permitan agilizar el proceso de detección y análisis de inicdentes futuros

Utilizar sniffers de paquetes para recolectar información adicional necesaria para poder identificar comportamientos que no son visualizados tan directamente.

Registrar cada uno de los incidentes, mediante la utilización del sistema GLPI.

Una vez que el incidente ha sido detectado, analizado y priorizado el grupo de respuesta a incidentes debe notificar a los individuos apropiados de acuerdo a la matriz de escalamiento de incidentes mediante las diferentes herramientas disponibles para tal efecto

Prevención de incidentes al mitigar los riesgos encontrados en los diferentes sistemas de información, aplicaciones y/o redes de comunicación

Identificar precursores e indicadores a través de alertas generadas por múltiples fuentes como por ejemplo: IPS, WAF, SIEM, AAA, PIM, AV, herramientas de integridad de archivos, entre otros

Generar una línea base a nivel de registro de eventos y auditoría en todos los sistemas de información.

En caso de un incidente, seguir el proceso de gestión de incidentes de seguridad descrito en el documento P9- Modelo de atención de incidentes de seguridad de la información. – Superintendencia de Puertos y Transportes. Septiembre 2016

Los funcionarios directos, empleados de firmas contratista y/o terceros con acceso a la infraestructura de la Superintendencia de Puertos y Transporte, deben estar educados y concientizados sobre las guías implementadas sobre la seguridad de la información y en particular la guía de atención de incidentes

El Agente Primer Punto de Contacto es el encargado de recibir las solicitudes por parte de los funcionarios/empleados sobre posibles incidentes. También debe registrarlos en la base de conocimiento y debe ser el encargado de escalarlos a la persona encargada de la atención de incidentes. Este Agente debe contar adicionalmente con capacitación en Seguridad de la Información (con un componente tecnológico fuerte) y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes. Adicionalmente debe contar con una capacitación básica en técnicas forenses, específicamente en recolección y manejo de evidencia

El Administrador del Sistema es la persona encargada para configurar y mantener un activo informático. También debe ser notificado por el agente de primer punto de contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al agente de primer punto de contacto sobre el incidente la solución del mismo. Los administradores deben contar con capacitación en Seguridad de la Información (con un componente tecnológico fuerte no solo en su plataforma si no en Redes y erradicación de vulnerabilidades) y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes. Adicionalmente debe contar con una capacitación en técnicas forenses, específicamente en recolección y manejo de evidencia.

El Oficial de Seguridad de La Información es la persona encargada de configurar y mantener un activo informático relacionado con la seguridad de la plataforma ej. Firewall, Sistemas de Prevención de Intrusos, Routers, Sistemas de Gestión y Monitoreo. También debe ser notificado por el agente de primero contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al agente de primer contacto sobre el incidente y la solución del mismo. Se recomienda que los administradores de esta tecnología sean expertos en Seguridad de la Información (con un componente tecnológico fuerte en Redes y erradicación de vulnerabilidades, Ethical Hacking y técnicas forenses) y debe conocer perfectamente la clasificación de Incidentes de la Superintendencia de Puertos y Transporte.

El Analista Forense debe ser un experto en el tema forense, quien debe estar disponible en caso de que un incidente de impacto alto (o uno que amerite acciones disciplinarias o legales o investigación profunda) requiera una investigación completa para solucionarlo y determinar los siguientes Ítems:

- Que sucedió.
- Donde sucedió.
- Cuando Sucedió.
- Quien fue el Responsable.

- Como sucedió.

Este actor debe ser un apoyo para los demás actores en caso de dudas sobre los procedimientos y debe ejercer un liderazgo técnico en el proceso de atención de Incidentes de seguridad de la información.

El Líder del Grupo de Atención de Incidentes debe responder a las consultas sobre los incidentes de seguridad que impacten de forma inmediata, y es el encargado de revisar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a los directivos. El Líder Grupo de Atención de Incidentes estará en la capacidad de convocar la participación de otros funcionarios de la organización cuando el incidente lo amerita (Prensa y Comunicaciones, Gestión de Talento Humano, Gestión Jurídica, Tecnología, Representante de las Directivas para el SGSI). También debe estar al tanto del cumplimiento de los perfiles mencionados y de revisar el cumplimiento de los procedimientos y mejores prácticas, así como también de los indicadores de gestión, y en capacidad de disparar si lo amerita planes de contingencia y/o continuidad. El Líder del Grupo de Atención de Incidentes será el responsable del modelo de Gestión de incidentes y debe estar en la capacidad de revisar todos los incidentes de seguridad y los aspectos contractuales que manejan el outsourcing del servicio help desk.

5.1.10 CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

El personal de la Superintendencia de Puertos y Transporte que tiene asignado un equipo de cómputo personal y/o telefonía tiene la responsabilidad de:

- Resguardar y cuidar los equipos.
- Resguardar y cuidar la información propiedad de la Superintendencia de Puertos y Transporte contenida en los equipos.
- Reportar a la Mesa de ayuda cualquier mal funcionamiento que pudiera presentarse en el equipo.
- Firmar carta de asignación del equipo de cómputo personal y/o telefonía.
- Usar el equipo de cómputo personal asignado para actividades relacionadas con el desempeño de sus funciones dentro de la Superintendencia de Puertos y Transporte.
- Conservar las configuraciones asignadas por la Gerencia de Red Corporativa.
- Comunicar al área Administrativa las necesidades de mover o reubicar su equipo de escritorio y/o telefonía, no aplica para portátiles.
- Comunicar inmediatamente a la Mesa de ayuda y al jefe inmediato la pérdida total o parcial de cualquier componente de hardware o software del equipo de cómputo y/o telefonía.
- No está permitido el préstamo o intercambio de equipos de cómputo o partes de los mismos propiedad de la Superintendencia de Puertos y Transporte por parte de los funcionarios.

Apagar el equipo de cómputo personal al término de la jornada laboral.

En caso de requerir dejar encendido su equipo de cómputo, esto debe ser justificado, debe bloquear el mismo y apagar el monitor para el caso de los PCs y reiniciarlo por lo menos una vez por semana.

Los dispositivos periféricos pertenecientes a los equipos (memoria, baterías, fuentes de poder, discos duros, monitores, etc.), y elementos de control como son etiquetas de licencias, placas de inventario, tarjetas de RFID (Identificadores de Radio Frecuencia), número serial, entre otros, no deben manipularse, retirarse o cambiarse de lugar por ningún motivo. Estos serán verificados a la devolución del equipo y cualquier desperfecto daño o ausencia de los mismos implicara la reposición, cobro al usuario responsable y las medidas disciplinarias a que dé lugar.

No se deben colocar en los equipos ningún tipo de etiquetas autoadhesivas que contengan distintivos decorativos tales como calcomanías, publicidad o emblemas entre otros.

Si sospecha que un virus ha infectado su computador o la red datos de la Superintendencia de Puertos y Transporte, comuníquese inmediatamente con la Mesa de Ayuda del área de informática.

Retirar de los escritorios o lugares visibles la información que haya sido utilizada sin importar el medio en que se encuentre (papel, discos, medios magnéticos y otros).

No utilizar documentos con información confidencial para reciclaje.

Proteger la información siempre que abandone su escritorio, sin importar el tiempo de ausencia.

Restringir el uso de fotocopiadoras y otra tecnología de reproducción a usuarios no autorizados.

Retirar inmediatamente de las impresoras los documentos que contengan información confidencial.

Utilizar los recursos asignados, para almacenar los activos de información sensible.

Velar que las salas de reuniones permanezcan cerradas y será exclusivo para reuniones de trabajo.

Todo equipo (computadoras, aire acondicionado, ventiladores, y otros) que fuere utilizado en las salas de reuniones, deben permanecer apagados, asimismo se deben retirar los documentos utilizados para evitar exposición y/o pérdida de información.

Queda terminantemente prohibido tener sustancias y/o líquidos en su escritorio que pudieran dañar documentos originales y/o equipo de trabajo y la información almacenada en ellos.

El escritorio de la computadora no debe poseer archivos o carpetas con accesos directos que faciliten la ubicación de información, excepto los instalados por la Dirección de Informática.

El único fondo de pantalla autorizado para los usuarios que utilizan equipo propiedad de la Superintendencia de Puertos y Transporte, es el o los logotipos que defina la Dirección de Informática.

Todos los usuarios deben terminar las sesiones activas cuando finalicen su tarea.

El usuario debe bloquear su equipo al retirarse de su área de trabajo por el motivo que fuere.

El sistema debe bloquear automáticamente el equipo luego de cinco minutos de usuario inactivo.

Los equipos en áreas de atención al ciudadano deben tener una protección específica contra accesos no autorizados cuando se encuentren desatendidos.

Cuando el usuario abandone su escritorio para asistir a alguna reunión, capacitación entre otros, debe verificar que no exista información sensible o documentos sobre el escritorio.

No dejar en lugares visibles y fácilmente accesibles USB, CD, DVD y otro tipo de medios de resguardo de información.

El servicio de acceso a internet de la Superintendencia de Puertos y Transporte no puede ser usado para lo siguiente (las descripciones se realizan a título enunciativo y no limitativo):

a) La distribución masiva de anuncios o mensajes no solicitados;
b) La propagación intencional de virus informáticos u otros programas dañinos
c) La congestión innecesaria y premeditada de la red local y/o WAN de la Superintendencia de Puertos y Transporte;
d) Utilización del servicio contratado como transporte para entrar a cualquier otra red o equipos sin autorización de sus propietarios o administradores;
e) La suplantación y modificación de la identidad de los paquetes de datos y mensajes: modificación de la cabecera de los paquetes TCP/IP, mensajes de correo electrónico (mail) y mensajes enviados a grupos de noticias (news);
f) La instalación no autorizada de programas o software que modifiquen el sistema operativo de los equipos del funcionario perjudicando su desempeño;

g) La utilización del servicio, o cualquiera de los elementos que lo integran con fines ilícitos tales como transmisión y/o difusión de materiales o contenidos que incurran en lo previsto en el Código Penal,
h) La realización de pruebas de la vulnerabilidad de los diferentes activos de información que operan en la Superintendencia de Puertos y Transporte o equipos en la Internet, sin el consentimiento expreso de la Dirección de informática de la Superintendencia de Puertos y Transporte.

Todo el personal de la Superintendencia de Puertos y Transporte debe conocer lo estipulado en la política de seguridad. No conocer la política no es excusa para su no cumplimiento y/o penalización en caso de no seguir las normas y directrices especificadas

Realizar de forma semestral evaluaciones sobre los conocimientos, las actitudes y las prácticas del personal para determinar el nivel, el alcance y el tipo de sensibilización y capacitación que deberán emprenderse para las distintas categorías de personal (mandos bajos, medios, altos)

Las campañas de sensibilización deben realizarse de forma trimestral abordando un tema específico del Plan de sensibilización. Se identifican 3 niveles:

- **Nivel Básico** Dirigido a todos los funcionarios de la Superintendencia de Puertos y Transporte; desarrollado con conceptos básicos, entre otros:
  - Contraseñas Seguras
  - Internet Seguro
  - Amenazas en la red
  - Seguridad física
- **Nivel Técnico** Dirigido a los profesionales y administradores de la Superintendencia de Puertos y Transporte, con temas más técnicos, mayor grado de profundización y complejidad en el área de la seguridad de la información.
  - Contraseñas Seguras
  - Internet Seguro
  - Ingeniería Social
  - Seguridad física
  - Gestión de incidentes
  - Gestión de riesgos
- **Nivel Jurídico** Dirigido a los profesionales y/o directivos con una profundización más amplia en las nuevas leyes y regulaciones más relevantes a tener en cuenta en un modelo de seguridad de la información, como la Ley 1266 de 2008 de Habeas Data y la Ley 1273 sobre Delitos Informáticos.
  - Delito Informático
  - Computación forense

Como instrumentos de sensibilización deben utilizarse:

- Afiches los cuales permiten:
  - Abrir la campaña y darla a conocer.
  - Captar la atención de los funcionarios para que interactúen con el Modelo de Seguridad.
  - Relacionar los afiches con los comportamientos que se buscan en cada uno de las personas como pieza fundamental en el nuevo Modelo de Seguridad de la Información.
  - Sensibilizar y capacitar a través de las imágenes y el texto de los instrumentos.

Los afiches se colocarán al inicio de la campaña dando a conocer lo que se quiere hacer para que las personas se familiaricen con el nuevo Modelo de Seguridad de la Información; la idea es que se cambien cada mes con nuevos enunciados para que las personas tengan en cuenta las principales prevenciones, peligros y factores relacionados con la seguridad de la información.

- Folletos los cuales permiten:
  - Explicar conceptos claves en forma breve sobre la seguridad de la Información y las principales recomendaciones para que el Modelo de Seguridad de la Información sea utilizado por todos los funcionarios
  - Desarrollo de textos con una secuencia lógica de adquisición de conocimientos y comprensión de

los mismos.

- Profundizar sobre las principales políticas y controles del Modelo de Seguridad de la Información en la Superintendencia de Puertos y Transporte
- Aconsejar sobre una adecuada higiene de la información.

Los folletos serán distribuidos al mismo tiempo que se lancen los primeros afiches de la campaña, con esto se le da apoyo y un impacto más proporcionado.

Medios BTL (Below The line) los cuales tienen los mismos objetivos que los folletos; la información de este es tener un contacto directo y a la vez dinámico, para que las personas interactúen con el Modelo de Seguridad de la Información, esto hará que la recordación sea mayor. Por ejemplo, utilización de crucigramas con preguntas de seguridad, sopas de letras, entre otros.

Fondos de pantalla permiten:

- Unir los elementos más importantes de las piezas gráficas y sus conceptos en una sola idea dinámica.
- Proteger la información sensitiva de las estaciones de trabajo.
- Reforzar los conceptos básicos de Seguridad de la Información.

Recordatorios: Elementos de sensibilización que serán entregados a las personas que asistan a las capacitaciones
Presentaciones:

- Plasmar con mayor profundidad conceptos, definiciones y explicaciones técnicas del Modelo de Seguridad de la Información
- Facilitar a la Estrategia de Gobierno en Línea, la difusión y el entendimiento del Modelo de Seguridad de la Información implementado en las entidades objetivo.

6 RESPONSABILIDADES

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Superintendencia de Puertos y Transporte, cualquiera sea su situación, el área a la cual se encuentre afectada y cualquiera sea el nivel de las tareas que desempeñe. Son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

7 INCUMPLIMIENTO DE LA POLÍTICA

La violación de la política será motivo para acciones disciplinarias incluyendo la terminación del contrato, acción civil y penal.

El funcionario que utilice las herramientas de tecnología informática para acceso a direcciones en Internet que contengan pornografía, juegos o salas de conversación será sancionado administrativamente.

El área de Recursos Humanos y/o Control Interno Disciplinario hará cumplir la sanción administrativa para los funcionarios que incurran en cualquiera de los siguientes delitos informáticos a través de Internet, los cuales pueden ser transfronterizos, así como analizar cómo afectaría a la Organización dichos sucesos:

- Acceso no autorizado.
- Destrucción de Datos ó archivos ó informes.
- Infracción de los derechos de autor.

- Infracción de Copyright de Bases de Datos.
- Interceptación de e-mail.
- Estafas electrónicas.
- Transferencias de Fondos en forma ilegal.
- Delitos convencionales como espionaje, terrorismo, narcotráfico, proselitismo de sectas, propaganda de grupos extremistas.
- Mal uso, como: Usos comerciales no éticos, agresión moral.
- Accesos a páginas de contenido no apto, o promueva el uso de éstas.
- Participar de juegos en línea a través de la red.

Versión 1.0, 28 de diciembre de 2.016.

Reviso: **Dr. Alcides Espinosa Ospino** – Secretario General

Ing. Jennifer Mendoza Velandia - Oficial de Seguridad de la Información

Ing. Urias Romero Hernandez - Coordinador Grupo Informática y Estadística