



**POLITICAS DE SEGURIDAD DE
INFORMACION**

DICIEMBRE 2019

INDICE

	Pág.
INTRODUCCION	
1. Objetivo	04
2. Finalidad	04
3. Alcance	04
4. Compromiso de Confidencialidad	04
5. Vigencia	04
6. Definición de términos	04
7. Responsabilidad	05
8. Cumplimiento	05
9. Disposiciones Generales	05
10. Políticas de la Organización de la Seguridad de la Información	06
10.1 Política de Clasificación y Control de Información	06
10.2 Política de Fomento de Cultura de Seguridad de la Información	07
10.3 Política de Seguridad Física y Ambiental	07
10.4 Política de Control de Acceso a la Información	08
10.5 Política de Administración de Acceso de Usuarios y cambio de contraseñas	08
10.6 Política de Responsabilidad de Acceso de los Usuarios	09
10.7 Política de Protección frente a Software Malicioso	09
10.8 Política de uso del Correo Electrónico	10
10.9 Política de uso adecuado de Internet	11
10.10 Política de uso de periféricos y medios de almacenamiento	12
10.11 Política de uso de Conexiones remotas	12
10.12 Política de copias de respaldo de la Información	12
10.13 Política de privacidad y Protección de Datos Personales	13
10.14 Política de gestión de los incidentes de seguridad Información	14
10.15 Política de Cumplimiento	14
10.16 Política de responsabilidad por los activos	14
11. Sanciones para las violaciones a las políticas de seguridad de Información	15

INTRODUCCION

Las Políticas de Seguridad de la Información en National Enterprise of Security S.A. identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la entidad, razón por la cual es necesario que la entidad establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este documento describe las políticas de seguridad de la información, definidas por National Enterprise of Security S.A. Para la elaboración del mismo, las políticas incluidas en este documento se constituyen como parte fundamental del Sistema de Gestión de Seguridad de la Información de National Enterprise of Security S.A. y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La seguridad de la información es una prioridad para National Enterprise of Security S.A. y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

Considerando que toda organización es dinámica, este documento está sujeto a permanente revisión y actualización en forma periódica, dependiendo de los cambios en la organización y los avances en las tecnologías de la información, su seguridad y protección.

	POLITICAS DE SEGURIDAD DE LA INFORMACION		
	VERSIÓN : 01	CODIGO:	PAGINA: 4 DE 15

1. OBJETIVO

Establecer las políticas de seguridad de la información que se administran en National Enterprise of Security S.A., necesarias para proteger los activos de información contra acceso no autorizado, divulgación, duplicación, modificación, destrucción, pérdida, robo o mal uso que se pueda producir en forma intencional o accidental, así mismo asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2. FINALIDAD

Dar a conocer a todo el personal de National Enterprise of Security S.A. y personal externo que tiene un vínculo con National Enterprise of Security S.A. la existencia y operación de las políticas de seguridad de la información.

3. ALCANCE

Esta política de seguridad de la información debe ser cumplidos por todos los colaboradores, consultores, contratistas y terceros que laboren o tengan relación con National Enterprise of Security S.A., para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

4. COMPROMISO DE CONFIDENCIALIDAD

Es un documento en los que los colaboradores de National Enterprise of Security S.A. o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

5. VIGENCIA

El presente documento tendrá vigencia a partir del día siguiente de su aprobación por la Gerencia General.

6. DEFINICION DE TERMINOS

Para efectos de presente documento, se definen los siguientes términos:

a) Información

Es un conjunto organizado de datos en cualquier forma con inclusión de formas textuales, numéricas, graficas, etc., y en cualquier medio, ya sea magnético, en papel, en pantallas de computadora u otro.

b) Confidencialidad

Es aquella característica que permite garantizar que la información en cualquier medio solo será vista y accedida por personas autorizadas para el cumplimiento de sus funciones.

	POLITICAS DE SEGURIDAD DE LA INFORMACION		
	VERSIÓN : 01	CODIGO:	PAGINA: 5 DE 15

c) Disponibilidad

Es aquella característica que permite garantizar que la información en cualquier medio siempre estará disponible en el momento que se necesite consultar o acceder por personal autorizado.

d) Integridad

Es aquella característica que permite garantizar que la información en cualquier medio solo será modificada por personas autorizadas bajo estrictas normas de operación.

e) Control

Es una herramienta de gestión del riesgo, que incluye normas, procedimientos, estándares, estructuras organizacionales, de naturaleza administrativa, técnica, gerencial o legal.

7. RESPONSABILIDADES

7.1 Es responsabilidad de la Dirección de Gestión de Tecnología hacer uso de la política de Seguridad de la Información, como parte de sus herramientas de gestión, de definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento.

7.2 Personal Interno

- Aceptar por escrito la adhesión a la presente política de seguridad de información.
- Cumplir con lo estipulado en las políticas de seguridad de información.
- Informar a la Dirección de Gestión de Tecnología situaciones que amenacen con la seguridad de la información.

7.3 Personal Externo

- Aceptar por escrito la adhesión a la presente política de seguridad de información.
- Cumplir con lo estipulado en las políticas de seguridad de información en lo que respecta a su relación con terceros.

8. CUMPLIMIENTO

El cumplimiento de la Política de Seguridad de la Información es obligatorio para todo el personal. Si los colaboradores, consultores, contratistas, terceras partes violan estas políticas, la organización se reserva el derecho de tomar las medidas correspondientes.

9. DISPOSICIONES GENERALES

9.1 National Enterprise of Security S.A. garantizara la aplicación de las medidas de seguridad de la información establecidas y optimizara su gestión mediante la Dirección de Gestión de Tecnología de la información.

	POLITICAS DE SEGURIDAD DE LA INFORMACION		
	VERSIÓN : 01	CODIGO:	PAGINA: 6 DE 15

9.2 Cuando exista la necesidad de otorgar algún acceso lógico y físico de información a personas o empresas que no tengan ningún vínculo directo y/o contrato con National Enterprise of Security S.A. deberán ejecutarse medidas que garanticen la seguridad de la información, las cuales serán establecidas previamente por la Dirección de Gestión de Tecnología y los responsables de dicha área.

9.3 En todos los contratos suscritos ya sea por prestación de servicios personales, servicios para la administración y control de los sistemas de información, redes y/o ambientes de procesamiento de información, consultorías, servicios entre otros, se deberá establecer la inclusión de términos relacionados a la seguridad de la información.

9.4 La presente política será revisada anualmente por la Dirección de Gestión de Tecnología, para establecer la necesidad de actualización o reafirmación de la vigencia.

10. POLITICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

Las políticas de seguridad de la información, contenidas en este documento serán adecuadas a los cambios que se presenten de acuerdo a mejoras tecnológicas.

10.1 POLITICA DE CLASIFICACION Y CONTROL DE LA INFORMACION

Se deben garantizar que los activos de información reciban un apropiado nivel de protección y uso, en función al grado de sensibilidad que presenten.

Toda la información debe ser identificada, clasificada y documentada de acuerdo con las guías de clasificación de la información establecidas por la Dirección de Gestión de Tecnología de información.

Una vez clasificada la información, se proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte del personal y/o terceras partes que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

10.1.1 NORMAS DIRIGIDAS A: TODOS LOS USUARIOS

- Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.
- Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíen faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres,

	POLITICAS DE SEGURIDAD DE LA INFORMACION		
	VERSIÓN : 01	CODIGO:	PAGINA: 7 DE 15

fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

- Tanto los usuarios como el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.
- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

10.2 POLITICA DE FOMENTO DE CULTURA DE SEGURIDAD DE INFORMACION

Lineamientos para asegurar que el personal tenga presente sus roles y responsabilidades y considere los riesgos de seguridad de la información, así como para definir el marco apropiado para el entrenamiento del personal en los aspectos de seguridad relacionados con su actividad.

Esta política abarca a toda la información utilizada en National Enterprise of Security S.A. para el desarrollo de sus actividades y es aplicable, obligatoriamente, por el personal, así como a las entidades proveedoras de servicios involucradas en la utilización de la información y los sistemas que la soportan.

10.3 POLITICA DE SEGURIDAD FISICA Y AMBIENTAL

Lineamientos para prevenir accesos no autorizados a los ambientes físicos de National Enterprise of Security S.A., donde se almacena y/o procesa información sensible y para evitar daño, modificación, pérdida o mal uso de la información o de los equipos que la soportan.

National Enterprise of Security S.A. proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Toda utilización, ingreso, copia o interferencia indebida con fines de alterar, dañar o destruir los recursos informáticos existentes en National Enterprise of Security S.A., podrá ser considerada y catalogada como "Delito Informático", según el Capítulo X, artículos 207-A y 207-B del Código Penal (Ley Nro. 27309).

10.3.1 NORMAS DIRIGIDAS A: TODOS LOS USUARIOS

- Los jefes de oficina deben velar porque las contraseñas de sistemas de alarmas, cajas fuertes, llaves y otros mecanismos de seguridad de acceso físico a sus áreas solo sean utilizados por personal autorizado

	POLITICAS DE SEGURIDAD DE LA INFORMACION		
	VERSIÓN : 01	CODIGO:	PAGINA: 8 DE 15

y, salvo situaciones de emergencia u otro tipo de eventos que por naturaleza lo requieran, estos no sean transferidos a otros.

- Los ingresos y egresos de personal a las instalaciones de National Enterprise of Security S.A. deben ser registrados; por consiguiente, los jefes y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.
- Los jefes y personal deben portar el carne que los identifica como tales en un lugar visible; en caso de pérdida del carne, deben reportarlo a la mayor brevedad posible.
- Aquellos jefes y/o personal provisto por terceras partes para los que apliquen, en razón del servicio prestado, deben utilizar carne de visita que faciliten su identificación.

10.4 POLITICA DE CONTROL DE ACCESO A LA INFORMACION

La Dirección de Gestión de Tecnología, como responsables de las redes de datos y los recursos de red, debe controlar que dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Asimismo las redes inalámbricas deben contar con métodos de autenticación que evite accesos no autorizados.

La Dirección de Gestión de Tecnología debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

10.4.1 NORMAS DIRIGIDAS A: TODOS LOS USUARIOS

- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las fueron autorizadas.

10.5 POLITICA DE ADMINISTRACION DE ACCESO DE USUARIOS Y CAMBIO DE CONTRASEÑAS

La Dirección de Gestión de Tecnología establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información. Así mismo, velará porque los usuarios o personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

La asignación de contraseñas se debería controlar a través de un proceso de administración formal, mediante el cual debería respetar los siguientes pasos:

	POLITICAS DE SEGURIDAD DE LA INFORMACION		
	VERSIÓN : 01	CODIGO:	PAGINA: 9 DE 15

- Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo.
- La Dirección de Gestión de Tecnología realizara el cambio de contraseñas cada 3 meses y/o a solicitud de los jefes de área y/o oficina deben solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para el personal que labora en sus áreas, acogiéndose al procedimiento establecidos para tal fin.

10.6 POLITICA DE RESPONSABILIDAD DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

10.6.1 NORMAS DIRIGIDAS A: TODOS LOS USUARIOS

- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
- Los usuarios no deben compartir sus cuentas de usuario y contraseñas con otros usuarios o con personal provisto por terceras partes.

10.7 POLITICA DE PROTECCION FRENTE A SOFTWARE MALICIOSO

La Dirección de Gestión de Tecnología proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.

La Dirección de Gestión de Tecnología debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de National Enterprise of Security S.A. y los servicios que se ejecutan en la misma.

10.7.1 NORMAS DIRIGIDAS A: TODOS LOS USUARIOS

- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento

	POLITICAS DE SEGURIDAD DE LA INFORMACION		
	VERSIÓN : 01	CODIGO:	PAGINA: 10 DE 15

externos o que provienen del correo electrónico.

- Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda, para que a través de ella, la Dirección de Tecnología tome las medidas de control correspondientes.

10.8 POLITICA DE USO DEL CORREO ELECTRONICO

National Enterprise of Security S.A., entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre usuarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

La Dirección de Tecnología debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

10.8.1 NORMAS DIRIGIDAS A: TODOS LOS USUARIOS

- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún usuario o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de National Enterprise of Security S.A.; El correo no debe ser utilizado para actividades personales.
- Los mensajes y la información contenida en los buzones de correo electrónico son de propiedad de National Enterprise of Security S.A. y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- Los usuarios de correo electrónico tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas.

	POLITICAS DE SEGURIDAD DE LA INFORMACION		
	VERSIÓN : 01	CODIGO:	PAGINA: 11 DE 15

- No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

10.9 POLITICA DE USO ADECUADO DE INTERNET

National Enterprise of Security S.A. consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionara los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias.

La Dirección de Tecnología debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

La Dirección de Tecnología debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

La Dirección de Tecnología debe monitorear continuamente el canal o canales del servicio de Internet.

La Dirección de Tecnología debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

La Dirección de Tecnología debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

10.9.1 NORMAS DIRIGIDAS A: TODOS LOS USUARIOS

- Los usuarios del servicio de Internet deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo asignados para el desempeño de sus labores.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento
- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Twitter, Youtube, Hotmail, Kazaa, MSN, Yahoo, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio.

	POLITICAS DE SEGURIDAD DE LA INFORMACION		
	VERSIÓN : 01	CODIGO:	PAGINA: 12 DE 15

- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.
- La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la Dirección de Tecnología, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

10.10 POLITICA DE USO DE PERIFERICOS Y MEDIOS DE ALMACENAMIENTO

La Dirección de Tecnología debe establecer las condiciones de uso de periféricos y medios de almacenamiento.

10.10.1 NORMAS DIRIGIDAS A: TODOS LOS USUARIOS

- Los usuarios de los recursos tecnológicos deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la Dirección de Tecnología.
- Los usuarios de los recursos tecnológicos son responsables por la custodia de los medios de almacenamiento asignados.
- Los usuarios no deben utilizar medios de almacenamiento personales en los equipos de cómputo de National Enterprise of Security S.A.

10.11 POLITICA DE USO PARA CONEXIONES REMOTAS

La Dirección de Tecnología establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas en los equipos de cómputo de National Enterprise of Security S.A.; Así mismo, suministrara las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

10.12 POLITICA DE COPIAS DE RESPALDO DE LA INFORMACION

National Enterprise of Security S.A. certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de la Dirección de Tecnología, encargada de la generación de

	POLITICAS DE SEGURIDAD DE LA INFORMACION		
	VERSIÓN : 01	CODIGO:	PAGINA: 13 DE 15

copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, National Enterprise of Security S.A. velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

La Dirección de Tecnología, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

La Dirección de Tecnología, a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

10.13 POLITICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

En cumplimiento de la Ley 29733, por la cual se dictan disposiciones para la protección de datos personales, National Enterprise of Security S.A. a través de la Dirección de Tecnología, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales National Enterprise of Security S.A., como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, National Enterprise of Security S.A. exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a terceras partes sin autorización.

10.13.1 NORMAS DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

- Las áreas que procesan datos personales de empleados, clientes, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir,

	POLITICAS DE SEGURIDAD DE LA INFORMACION		
	VERSIÓN : 01	CODIGO:	PAGINA: 14 DE 15

almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades.

- Las áreas que procesan datos personales de empleados, clientes, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
- Las áreas que procesan datos personales de empleados, clientes, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

10.13.2 NORMAS DIRIGIDAS A: TODOS LOS USUARIOS

- Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.
- Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico, entre otros.

10.14 POLITICA DE GESTION DE LOS INCIDENTES DE SEGURIDAD DE INFORMACION

Lineamientos para asegurar que el personal afectado comunique oportunamente a la Dirección de Tecnología, los eventos o debilidades asociados con la seguridad de información.

El personal debe alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en las políticas de seguridad.

10.15 POLITICA DE CUMPLIMIENTO

Lineamientos para asegurar el cumplimiento de las políticas de seguridad de información por todos colaboradores y/o terceras partes.

Enterprise of Security S.A. se reserva el derecho de tomar medidas administrativas y acciones, conforme a lo que establece el Reglamento Interno de Trabajo.

10.16 POLITICA DE RESPONSABILIDAD POR LOS ACTIVOS

National Enterprise of Security S.A. como propietario de la información física así como de la información generada, procesada, almacenada y transmitida, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

	POLITICAS DE SEGURIDAD DE LA INFORMACION		
	VERSIÓN : 01	CODIGO:	PAGINA: 15 DE 15

La información, archivos físicos, los sistemas, los servicios y los equipos (estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros) propiedad de National Enterprise of Security S.A., son activos de la empresa y se proporcionan a los Trabajadores, colaboradores y terceros autorizados, para cumplir con los propósitos del negocio.

Toda la información sensible de National Enterprise of Security S.A., así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la Dirección de Tecnología.

11. SANCIONES PARA LAS VIOLACIONES A LAS POLITICAS DE SEGURIDAD DE INFORMACION

La Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los trabajadores, colaboradores, personal externo y otros. Por tal razón, es necesaria que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

