Agencia Nacional de Defensa Jurídica del Estado

POLÍTICA DE SEGURIDAD INFORMÁTICA

UNIDAD ADMINISTRATIVA ESPECIAL
AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO
AGOSTO DE 2014

La utilización creciente de las Tecnologías de la Información y las Comunicaciones -TIC-, genera beneficios para las entidades, organismos y órganos de control, mejorando el cumplimiento de la misión y la prestación de servicios a la ciudadanía. Sin embargo, por ser la información el activo más importante de la organización, es necesario protegerla frente a los posibles riesgos derivados del uso de las nuevas tecnologías, para garantizar la seguridad de la información, en aspectos tales como disponibilidad, confiabilidad, accesibilidad e integridad de la misma.

Estos tres principios se definen así:

DISPONIBILIDAD: La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizada para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La alta disponibilidad de sistemas objetivo debe ser garantizada en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

Garantizar la disponibilidad implica también la prevención de cualquier tipo de ataques informáticos, como tales como la **Denegación del Servicio (DoS)**.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen diferentes mecanismos para cumplir con los niveles de servicio que se requieran; tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web etc., mediante el uso de Clústers o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, entre otros. La gama de posibilidades dependerá de lo que se requiere proteger y el nivel de servicio que se quiera proporcionar.

CONFIDENCIALIDAD: Es la propiedad de la información por la que se garantiza que ésta pueda ser accesible únicamente a personal autorizado para ello. La confidencialidad ha sido definida por la Organización Internacional de Estandarización (ISO) en la norma ISO-17799 como "garantizar que la información es accesible sólo para aquellos autorizados a tener acceso" y es una de las piedras angulares de la seguridad de la información. La confidencialidad es uno de los objetivos de diseño de muchos criptosistemas, lo cual es posible en la práctica gracias a las técnicas de criptografía moderna.

INTEGRIDAD: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene

adjuntándole otro conjunto de datos de comprobación de la integridad, siendo la firma digital uno de los pilares fundamentales de la seguridad de la información.

La definición de esta Política de Seguridad Informática (PSI) está enfocada a la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida) en la Agencia Nacional de Defensa Jurídica del Estado. Para ello se realizó una investigación sobre los estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La Política de Seguridad Informática comprende software, bases de datos, metadatos, archivos y toda aquella información adicional que la organización valore (activo de información) y signifique un riesgo si ésta llega a manos de personas no autorizadas. Este tipo de información se conoce como información privilegiada o confidencial.

DEFINICIONES

Entiéndase para el presente documento los siguientes términos:

Activos de información: Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.
Amenaza: Es un evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
Ataque informático: intentó de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.
Brecha de seguridad: Deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.
Criptografía de llave publica: Es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.
Cifrar: quiere decir transformar un mensaje en un documento no legible que requiere ser descifrado que es el proceso contrario. Los sistemas de cifrado se llaman "sistemas criptográficos".
Certificado Digital: Un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.
Confidencialidad: Aseguramiento de que la información es accesible sólo para quienes están autorizados.
Disponibilidad: Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando se requiera.

Desastre: Interrupción de la capacidad de acceso a información y procesamiento de la misma, a través de equipos de cómputo necesarios para la operación normal de un negocio.

Impacto: Medir la consecuencia al materializarse una amenaza.
Información: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.
Integridad: Salvaguardia de la exactitud y completitud de la información y sus métodos de procesamiento.
Política: son instrucciones mandatorias que indican la intención de la alta gerencia respecto a la operación de la organización.
Riesgo: Posibilidad de que se produzca un impacto determinado en un Activo, en un Dominio o en toda la Organización.
Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.
Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.
Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios de la Agencia, pero que por las actividades que realizan en la Entidad, deban tener acceso a Recursos Informáticos.
Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

OBJETIVOS DE LA POLITICA DE SEGURIDAD INFORMÁTICA GENERAL

General

Proteger los activos informáticos frente a los posibles riesgos derivados del uso de las nuevas tecnologías, para garantizar la seguridad en aspectos tales como disponibilidad, confiabilidad, accesibilidad e integridad de los mismos en la Agencia Nacional de Defensa Jurídica del Estado.

Específicos

- Establecer un entorno seguro sobre los activos informáticos de la Agencia.

- La Política de Seguridad Informática, surgen como una herramienta organizacional para concientizar a cada uno de los miembros de la organización sobre la importancia y sensibilidad de la información y servicios críticos tanto misionales como de apoyo.

La política descrita en este documento refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad de

la información; pero ante todo siempre hay que tener en cuenta que la seguridad comienza y termina con el recurso humano.

PRINCIPIOS ORIENTADORES DE LA POLITICA DE SEGURIDAD INFORMÁTICA

Principio de Confidencialidad:

1. Principio de acceso al equipo de cómputo: Se debe crear un usuario y contraseña para el acceso y manejo del equipo de cómputo; esta información debe ser entregada en el momento que el usuario recibe el activo.
2. Principio de contraseña de usuario registrado en el dominio: La contraseña de acceso debe tener un mínimo de 8 caracteres los cuales deben incluir, letras en mayúscula, minúscula, números y caracteres especiales.
3. Principio de manejo de la contraseña: La contraseña se debe cambiar periódicamente, como mínimo cada 40 días.
4. Principio de manejo de la información en un equipo de cómputo: La información deberá estar situada en la carpeta de **Mis Documentos**, estableciendo un orden cronológico. Se advierte que no se debe almacenar información de los usuarios en carpetas de la unidad C: \, ya que esto permitiría el acceso a esta información por parte de todos los usuarios que ingresen al equipo.

Principio de Integridad:

1. Principio de salvaguardar la información: Se realizará Backup de los diferentes Sistemas de Información en el servidor que este estipulado para este fin, el cual se programará de acuerdo a los diferentes sistemas y usuarios.
2. Principio de manejo de la información de los equipos de cómputo: En el instante que un usuario sea reasignado, traslado o se termine su contrato con la Agencia, éste deberá relacionar la información que deja en el equipo al jefe inmediato mediante documento y copia de la información en medio físico. Por otra parte, si requiere la información en otro medio deberá solicitarlo al área encargada de dicha tarea; ya que esta información es un activo de información de la entidad.

Principio de Disponibilidad:

1. Principio de escaneo de la información en los equipos de cómputo:
Se debe generar un mecanismo de detección de virus en todos los equipos de cómputo de la Agencia, con el fin de proteger la información y garantizar su disponibilidad e integridad. Este sistema Antivirus que deberá estar programado para hacer escaneos en tiempo real, analizando discos extraíbles como Memorias USB, CD-ROM, etc., será administrado por el área encargada y se encontrará en el Servidor perteneciente al Dominio con su respectiva consola de administración.
2. Principio de creación de perfiles: Consiste en la asignación de permisos diferenciados para el manejo de los diferentes aplicativos con que cuente la Agencia; para este proceso el XXX será la encargada de dar autorización de acceso a los diferentes sistemas de la Agencia.

3. Principio de creación de usuarios: Para la creación de un usuario en los aplicativos de la Agencia, el área solicitante remitirá correo electrónico al encargado de esta función relacionando el nombre del funcionario que recibirá el usuario y las opciones del módulo que sean requeridas por éste se mostrarán en el menú.

Principio de Seguridad de la Red:

1. Principio de Seguridad de la Información: La organización deberá contar con un Servidor Firewall para la administración del canal de internet y de datos el cual debe tener los Servicios de: Protección contra Intrusos, Filtrado Web, HTTP Proxy, Antivirus, Antispyware, Antispam y Encriptación Mail, con el fin de garantizar la estabilidad y el buen uso del canal de internet.
2. Principio de Creación de los Perfiles en el Servidor Firewall: De acuerdo a la misión de la Agencia, se deben crear 3 o más perfiles asignándolos por categorías, los cuales serán orientados de la siguiente manera:

- **Perfil Administrativo:** Este perfil contendrá a la parte Administrativa de la organización y estará conformado por los líderes de las áreas y/o funcionarios de actividad misional.
- **Perfil de Sistemas:** Este perfil contendrá al personal del área de sistemas, el cual estará enfocado a la descarga de información e instalación de actualizaciones de los equipos de la organización.
- **Perfile de Usuarios Generales:** Este perfil contendrá toda la parte operativa y misional de la agencia.

3. Principio de Asignación de Perfiles en el Servidor Firewall: Para la asignación de los perfiles a los funcionarios de cada área se contemplarán las labores y ubicación en el organigrama de la organización.

Principios de Manejo del Activo de la Información:

1. **Principio de Instalación del Equipo de Cómputo:**

Todo equipo de cómputo (Portátiles, Estaciones de Trabajo, tabletas, Servidores e Impresoras), que esté o sea conectado a la red de la Agencia, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe de sujetarse a las normas y procedimientos de instalación que emite la entidad y/o el encargado de TIC.
El responsable del activo deberá avisar al encargado de Tic y/o Activos Fijos de la organización con el fin de dar cumplimiento con las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos internos del activo.

La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, a los encargados correspondientes, como sería el encargado de Tic y/o Activos Fijos de la organización.

2. Principio de Mantenimiento de Equipo de Cómputo.

El encargado de TIC deberá tener un registro del inventario de todos los equipos de la organización.

También estará encargado del mantenimiento preventivo y correctivo de los equipos por motivos de pérdida de información o daño en otros equipos, para la organización queda estrictamente prohibidos dar mantenimiento a equipos de cómputo que no sean propiedad de la Agencia.

Todo equipo de cómputo (Portátiles, Estaciones de trabajo, tabletas, Servidores y demás relacionados), que sean propiedad de la organización deberá procurarse su actualización continua, esto con el fin de conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

ESTRATEGIA

La instancia para decidir sobre temas de seguridad informática en la Agencia es el Comité Institucional de Desarrollo Administrativo. La estructura de este comité es:

La Resolución 191 de 19 de Julio 2013, la cual define la creación del Comité Institucional de Desarrollo Administrativo de la Agencia Nacional de Defensa Jurídica del Estado, el cual es integrado por los siguientes miembros:

1. El director de la Agencia Nacional de Defensa Jurídica del Estado o su delegado.
2. El secretario General de la Agencia Nacional de Defensa Jurídica del Estado, quien lo presidirá.
3. El director de Gestión de Información.
4. El Director de Políticas y Estrategias para la Defensa Jurídica.
5. El Director de Defensa Jurídica.
6. El jefe de Oficina Asesora Jurídica.
7. El jefe de la Oficina de Control Interno será invitado permanente con voz pero sin voto.
8. El jefe de la Oficina Asesora de Planeación, quien será el Secretario Técnico y asistirá a las reuniones con voz pero sin voto.

Parágrafo 1°. Invitados. Serán invitados ocasionales los funcionarios que por su condición jerárquica, funcional o conocimiento técnico deban asistir, según el caso concreto. Igualmente el Comité, por medio de su Secretaria Técnica, podrá invitar a sus sesiones a las personas o funcionarios que requiera para la mejor comprensión de sus asuntos materia de consideración, quienes asistirán a las sesiones con voz pero sin voto. Las

invitaciones efectuadas a los servidores públicos serán de obligatoria aceptación y cumplimiento.
Parágrafo 2°. La asistencia de los directores técnicos de la Agencia será obligatoria en relación con la Política Misional y de Gobierno.
Parágrafo 3°. El Comité Institucional de Desarrollo Administrativo sustituirá a todos los comités de la Agencia, que tengan relación con el Modelo y no sean obligatorios por mandato legal.

PUBLICACIÓN Y VIGENCIA

La POLÍTICA DE SEGURIDAD INFORMÁTICA rige a partir de su adopción mediante acto administrativo por parte de la Dirección General, y deroga todas las disposiciones que le sean contrarias.

Elaboró	Revisó	Aprobó
Mauricio Galarza Vejarano Asesor Secretaria General	Mauricio Galarza Vejarano Asesor Secretaria General	Isabel Abello Albino Secretaria General