ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN -TIC	Código: 3AP-GTI-POL
		Fecha: 16/09/2015
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Versión: 2
		Página: 1 de 16

Objetivo: El presente documento pretende establecer estándares de seguridad informática que sirvan de base para la protección y aseguramiento de los activos tanto tecnológicos como de la información.

Alcance: Las políticas aquí definidas aplican a todos los funcionarios públicos de planta permanente, planta temporal, contratistas y otras personas relacionadas con terceros, que utilicen de manera itinerante los recursos informáticos del Instituto distrital de las artes - IDARTES.

Fecha de Aprobación	Responsable del Documento	Ubicación
	Área de Sistemas	Página Intranet: http://comunicarte.idartes.gov.co/idartes

HISTÓRICO DE CAMBIOS		
Versión	**Fecha de Emisión**	**Cambios realizados**
01	Enero 2014	Emisión Inicial
02	Septiembre 2015	Se realizan cambios en cuanto al manejo de contraseñas y actualización del servicio de correo bajo la plataforma Google.

Oficinas Participantes
Subdirección Administrativa y Financiera Área de Sistemas Oficina Asesora de Planeación

Revisó:	Validó:	Aprobó:
Jenny Peña Durán Profesional Universitario Oficina Planeación	**Edgar Cipagauta** Profesional Universitario Área Sistemas **Orlando Barbosa Silva** Subdirector Administrativo y Financiero	**Orlando Barbosa Silva** Jefe (E) Oficina Asesora de Planeación Fecha Aprobación: 15/09/2015

TABLA DE CONTENIDO

8. DEFINICIONES

INTRODUCCION

La información es el activo más importante dentro de toda organización, convirtiéndose a su vez en su patrimonio histórico. Por esta razón es importante protegerla y son las políticas de seguridad de la información, la clave para identificar los procesos y sus activos de la información dependientes.

Se consideran activos de la información los siguientes elementos:

- La información en sus múltiples formatos (papel o digital, texto, imagen, audio o video).
- Los equipos e infraestructura tecnológica que soportan esta información.
- Los usuarios que utilizan la información y que tienen el conocimiento de los procesos institucionales a nivel misional o administrativo.

GENERALIDADES

Los servicios de la red institucional son de uso exclusivo operativo, misional y para gestiones administrativas relacionados con la actividad del IDARTES.

Los servicios de correo electrónico, internet, intranet y las aplicaciones, son de uso exclusivo en el desarrollo de las funciones y actividades del IDARTES, por lo tanto queda restringido el uso para otros fines como los comerciales o personales.

La ley 1581 de 2012 y el Decreto 1377 de 2013, implementa el Régimen General de Protección de Datos Personales, el cual desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar todo tipo de información recogida o que haya sido objeto de tratamiento de datos personales en bancos o bases de datos y en general en archivos de entidades públicas y/o privadas. Para dar cumplimiento a lo previsto en esta normatividad, IDARTES, tras la vinculación como funcionario o contratista, queda autorizada para manejar y mantener dicha información personal, la cual es recopilada en diferentes bases de datos, para el desarrollo de sus funciones o actividades. Dicha información puede ser conocida, actualizada y rectificada por cada persona en el momento que lo requiera. En caso que la persona decida No Autorizar a IDARTES el tratamiento de su información personal, deberá realizar los trámites correspondientes en la oficina de Talento Humano si es funcionario o la Oficina Jurídica si es contratista, para determinar el cumplimiento de sus funciones u obligaciones contractuales.

No se debe entregar datos o reproducir total o parcialmente la información generada por el servicio a personas ajenas del IDARTES o que no sean parte del proceso administrativo o misional correspondiente.

Se prohíbe la descarga de archivos, transmisión o almacenamiento que pudiera ser considerado pornográfico, difamatoria, racista, videos, música, etc. o que atente contra las buenas costumbres o principios, excepto que el trabajo lo amerite.

Todo usuario de la red institucional del IDARTES gozará de privacidad limitada sobre su información o la información que provenga de sus acciones. IDARTES podrá monitorear la actividad para evitar que ésta se vea involucrada en actos ilícitos o contraproducentes para la seguridad de la red institucional, sus servicios o cualquier otra red ajena a la entidad.

Los usuarios tendrán el acceso a Internet siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones establecidas en la presente política de seguridad.

1. MANEJO Y SEGURIDAD DE INFORMACION EN MEDIOS EXTRAIBLES

Teniendo en cuenta que la información es el activo más importante de toda organización, desde todas las áreas se debe velar por la seguridad del producto final, en la manipulación de dispositivos extraibles y medios de almacenamiento masivo como discos duros y demás medios que permitan una copia no permitida de la información.

1.1. Manejo de memorias USB:

Se recomienda no conectar a los computadores, dispositivos externos como USB, Discos Duros externos USB, Tarjetas SD, Celulares o cualquier otro dispositivo, ya que además del riesgo de contener virus o software malicioso que puede afectar la máquina, también puede extraer información no autorizada; por lo tanto, es responsabilidad de cada persona o usuario por la información o daños que esta cause. En caso de requerir compartir archivos entre dos o más equipos o usuarios, puede solicitar el ingreso ó creación de carpetas compartidas las cuales ya se encuentran funcionales y distribuídas por dependencias.

1.2. Manejo de discos duros autorizados:

Los discos duros deben permanecer desocupados, ya que la función de estos es la de transferencia de información y no la de almacenamiento masivo. Para ello la información debe estar siempre respaldada en la estación de trabajo de origen, se copia en su destino y se debe eliminar del disco duro, que tan solo es el medio de transferencia de la información, para su conservación permanente se debe solicitar su respaldo según el procedimiento "Copias de seguridad y restauración".

Los discos duros de propiedad del Instituto deben permanecer en la medida de lo posible en las sedes de donde han sido asignado con el objeto de prevenir daños en su estructura y con ello la pérdida de información.

1.3. Manejo de dispositivos móviles:

Los dispositivos móviles del IDARTES se han adquirido específicamente para facilitar el desarrollo de actividades laborales relacionadas con la entidad y el uso para propósitos personales debe ser ocasional, racional y no debe obstaculizar las actividades laborales.

La instalación, configuración, modificación o eliminación de software sobre los dispositivos móviles recae bajo la responsabilidad del usuario que tiene la asignación del área.

No descargar ningún software que no se encuentre licenciado o que indique claramente que es de licencia libre.

1.4. Manejo computadores portátiles:

Los computadores portátiles del IDARTES se han adquirido específicamente para facilitar el desarrollo de actividades laborales. Su uso debe estar relacionado con las actividades del área o proceso al cual ha sido asignado y el uso para propósitos personales debe ser ocasional, racional y no debe obstaculizar las actividades laborales habituales.

Los equipos portátiles deben permanecer en las instalaciones del IDARTES, durante los días y horarios hábiles de trabajo y están autorizados para salir de las instalaciones, solo en el caso de utilizarlo en labores de la entidad con el respectivo permiso del área de Almacén.

En caso de licencia o vacaciones del funcionario, el equipo portátil debe quedar a disposición del área a la cual fue asignado.

La instalación, configuración, modificación o eliminación de software aplicativo sobre los equipos portátiles es responsabilidad exclusiva del área de Sistemas y no puede ser modificada bajo ninguna excusa directamente por el usuario.

Si el usuario sospecha que hay infección por un virus, debe inmediatamente llamar al área de sistemas, no utilizar el computador y desconectarlo de la red.

El área de sistemas tiene la potestad para remover, sin notificar al funcionario, cualquier software que no esté autorizado por la Subdirección Administrativa y Financiera.

La configuración e instalación de hardware de los equipos portátiles del IDARTES, debe ser solicitada y ejecutada exclusivamente por el área de sistemas.

Se debe mantener desactivada la red inalámbrica en caso de que no esté siendo utilizada, con el fin de no utilizar un punto de conectividad a la red de más y congestionando así el access point.

Es responsabilidad de cada funcionario hacer copias de seguridad de la información almacenada en el equipo portátil. Si no está seguro del proceso debe comunicarse con el área de Sistemas.

Es responsabilidad del funcionario reportar inmediatamente al área de Sistemas, cualquier daño, desconfiguración ó pérdida del dispositivo móvil que le ha sido asignado.

Todo dispositivo móvil personal que se requiera conectar a la red del IDARTES, debe cumplir las normas de seguridad solicitadas por el área de Sistemas.

1.5. Manejo equipos de visitantes:

Los computadores o cualquier otro dispositivo que permita conexión a la red a través de la tarjeta

inalámbria "Wifi" o tarjeta de red, sólo están autorizados a conectarse a la red de internet llamada "visidartes", cuya clave será suministrada en el área de sistemas. En caso de requerir acceso a un servidor de la intranet, debe realizar la solicitud a través del Jefe de su dependencia o supervisor del contrato, por medio del GLPI.

2. SEGURIDAD EN LOS SERVIDORES Y SISTEMAS DE INFORMACIÓN

2.1. Seguridad en los equipos servidores

La seguridad de los equipos de administración de red y de infraestructura están protegidos de ataques externos desde la nube por el equipo utilizado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas (firewall), en cual permite limitar, cifrar y descifrar el tráfico entre diferentes ámbitos sobre un conjunto de reglas. En la actualidad el instituto cuenta con el software de firewall PfSense el cual es de licencia GPL.

Cabe aclarar que un firewall correctamente configurado brinda la protección necesaria a la red, pero que en ningún caso debe considerarse suficiente toda vez que todos los días se crean nuevos códigos maliciosos con el fin de violar la seguridad. Para ello debe trabajarse de la mano con la sensibilización de los funcionarios.

Sólo el personal de sistemas y administradores de los diferentes sistemas de información están autorizados para ingresar o conectarse al sistema operativo de los servidores, con un usuario diferente al administrador o root, con el fin de realizar tareas de administración y mantenimiento.

En caso que una empresa externa requiera realizar alguna configuración en los servidores, sólo el personal de sistemas debe ingresar con el usuario y contraseña correspondiente, sin suministrar las claves a personal no autorizado.

El administrador de red, en conjunto con el responsable de cada servidor o sistema de información, deben aplicar las actualizaciones vigentes y parches de seguridad al sistema operativo, sin que esto afecte el funcionamiento normal de las aplicaciones. Si no están seguros de la actualización o del impacto que ésta pueda causar, se debe recrear un ambiente alterno para realizar previamente las respectivas pruebas.

Se deben implementar herramientas en los servidores, que permitan su monitoreo, con el fin de conocer su rendimiento, capacidad de almacenamiento, registro de logs y consumo de red.

La administración de los servidores ubicados en la Secretaría de Cultura, recreación y Deporte, para los sistemas de información SiCapital del que el Instituto era provisto del ERP y el SIS de Convocatorias, están a cargo de dicha entidad.

2.2. Seguridad en los sistemas de información

El área de sistemas deberá mantener actualizado el inventario de todos los sistemas de información existentes en la entidad.

Los sistemas de información administrativos del IDARTES, se trabaja a través de los módulos del ERP SiCapital, siendo accesibles para los usuarios a través de la página de inicio de la Intranet. La administración funcional del sistema de información está a cargo de los contratistas especializados en esta plataforma facilitada por la Secretaría de Hacienda Distrital a través de convenio interadministrativo suscrita con el IDARTES. Los servidores en los que se encuentra alojado este ERP, son revisados y administrados por los funcionarios del área de sistemas de la entidad.

Los sistemas de información alojados en los servidores físicos de IDARTES, como Orfeo, GLPI, Zimbra, Pfsense, koha, PMB y demás que hacen parte del inventario de sistemas de información, su administración está a cargo del administrador de red de IDARTES.

A todos los sistemas de información se le debe actualizar sus paquetes, librerías y servicios a la última versión disponible. Si estas actualizaciones pueden provocar el fallo de alguna funcionalidad, se deben aplicar las actualizaciones en un ambiente alterno, donde se hagan las respectivas pruebas y ajustes al código fuente de ser necesario, para luego instalarlas en el ambiente de producción.

3. ADMINISTRACIÓN DE USUARIOS

Cada persona, funcionario o contratista deber tener su correspondiente usuario de red, usuario de correo electrónico y usuario para las diferentes aplicaciones que requiera para el desarrollo de sus funciones o actividades contractuales.

Es responsabilidad de cada Jefe de área y Supervisor de Contrato, realizar la respectiva solicitud de creación y actualización de la cuenta de usuario a través del GLPI, como lo indica el procedimiento "Administración de Usuarios".

3.1. Desactivación temporal de la cuenta de red:

En situaciones especiales como permisos, vacaciones, incapacidades ó despidos del personal, podrá ser enviado un GLPI por parte del Jefe solicitando el bloqueo temporal de las cuentas del funcionario en cuestión, formalizando a la brevedad.

Ante situaciones de grave riesgo para la disponibilidad o continuidad del servicio, se podrá cambiar la contraseña de una cuenta de red. Esto podría impedir al usuario el acceso al resto de los servicios basados en las credenciales de la Intranet.

4. SEGURIDAD DE LAS CUENTAS DE CORREO ELECTRÓNICO

El correo electrónico institucional es una herramienta importante para la gestión y desarrollo de las funciones y actividades de los funcionarios y contratistas de IDARTES, por lo tanto se le debe dar un uso razonable y responsable, atendiendo las siguientes recomendaciones:

4.1. Tamaño de los buzones de correo electrónico:

La capacidad máxima para los buzones de correo GMAIL es de 5 GB. Cuando el sistema detecta que la ocupación del buzón de correo es superior al 90% automáticamente envía una notificación al usuario, con el fin de que pueda tomar las medidas pertinentes para no generar un bloqueo en su cuenta.

Dichas medidas consisten en la utilización del software de descargado de correo THUNDERBIRD, el cual permite descargar el volumen del correo a una estructura de carpetas en el disco duro de su estación de trabajo local. Si no descarga el correo y una vez alcanzado el 100% de la cuota asignada, todos los mensajes son rechazados por el sistema, siendo necesario que el usuario vacíe el buzón para restablecer la recepción normal de mensajes.

4.2. Suspensión de cuentas de correo electrónico:

Se suspenderán aquellas cuentas de correo que no han sido consultadas durante un periodo continuado de tres meses, generando que el usuario no pueda acceder a los correos almacenados en dicha cuenta.

El uso inapropiado o el abuso en el servicio de correo electrónico puede ocasionar la desactivación temporal o permanente de las cuentas. Las acciones en este sentido se pueden llevar a cabo en función de las posibles repercusiones en el buen funcionamiento del servicio. La desactivación de la cuenta implica la imposibilidad de enviar y recibir nuevos correos mientras no vuelva a ser activada.

Ante situaciones de grave riesgo para la disponibilidad o continuidad del servicio de correo, los adminisradores de la plataforma podrán cambiar la contraseña de una cuenta de correo. Esto podría impedir al usuario enviar o recibir correos en su cuenta corporativa hasta que se investigue encuentre el origen y mitigación del problema causado.

4.3. Envío de correos electrónicos masivos:

El envío de correos masivos se canalizarán a través del funcionario de la Oficina de Comunicaciones, diligenciando el formato destinado para la publicación de información en masa. Solo esta Oficina tiene la facultad de la utilización del servidor PHPList para el envió de correos masivos. Al interior de la entidad, solo las personas autorizadas tienen autorización para el envio de correos a todo el dominio.

4.4. Cuentas de correo electrónico externas:

Está prohibido el uso y realizar la vinculación o reenvío del correo institucional a otros servicios de correo como cuentas personales gmail, yahoo, outlook o cualquier otro servidor de correo que no corresponda al servicio de correo de IDARTES.

4.5. Problemas de seguridad en el correo electrónico:

Son múltiples los problemas de seguridad que pueden afectar al correo electrónico, entre los que cabe destacar:

4.5.1. Robo de identidad. Phishing y scams:

Si se recibe un correo de origen desconocido consulten inmediatamente con el área de Sistemas, o levanten un ticket a través de la mesa de ayuda (Helpdesk). Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos a correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, etc). Si dicho archivo pide o contiene un formato para diligenciar con sus datos de usuario, claves y/o datos personales, no lo diligencie por ningún motivo. Puede ser víctima de robo de identidad a través de la técnica de captura de datos personales llamada phishing. Cabe recordar que el área de Sistemas de IDARTES nunca requerirá este tipo de información a través del correo institucional.

4.5.2. Propagación de virus y spam:

El correo electrónico es un vehículo ideal para la propagación de virus y sobre todo los gusanos que utilizan técnicas de spam para infectar un PC en combinación de virus y spam. Las últimas generaciones de virus se han creado para ayudar a los spammers que han incorporado código malicioso en su spam.

Cualquier correo electrónico de contenido inapropiado o sospechoso, debe ser filtrado y enviado a la *lista negra* para evitar su propagación.

4.5.3. Ataques con direcciones falsificadas:

Consiste en inundar el servidor de un dominio real con los errores generados por una máquina atacada al procesar spam para distribuirlo a miles destinatarios. El spammer coloca como dirección receptora de estos errores un dominio real y un usuario aleatorio. Esto provocará problemas de ancho banda, colapso del servidor (colas, disco etc.).

4.5.4. Generación innecesaria de tráfico SMTP:

El envío y encaminamiento de un simple mensaje de correo electrónico implica el uso de varios recursos: conexiones SMTP, consultas DNS, procesamientos por MTA. Los propios errores de SMTP, el spam, los virus etc., generan informes a direcciones falsificadas provocando confusión en los usuarios y generando un exceso de tráfico.

Teniendo en cuenta lo anterior se especifican las siguientes recomendaciones generales para el manejo apropiado de la contraseña y uso general del correo:

- La contraseña de acceso al correo no debe ser cedida o facilitada a otros usuarios, siendo responsabilidad del propio usuario su custodia.
- Nunca se debe guardar las contraseñas, en ningún tipo de archivo digital ni físico como un papel, agenda, etc.
- Las contraseñas se deben mantener confidenciales en todo momento.
- Cambie su contraseña si se piensa que alguien más la conoce y si ha tratado de dar mal uso de ella.
- Seleccione contraseñas que no sean fáciles de adivinar.
- Cambia tus contraseñas regularmente.
- Nunca utilizar la opción de almacenar contraseñas en su navegador de Internet.
- No utilizar contraseña con números telefónicos, nombre de familia o similares ya que son fáciles de adivinar por terceros.
- No utilice el correo institucional para obtener información personal, comercial o de labores diferentes a las de su trabajo, para esto debe utilizar su correo personal.
- Utilizar el correo electrónico como una herramienta de trabajo y no como nuestra casilla personal de mensajes a amigos y familiares.

- No enviar archivos de gran tamaño a compañeros de oficina o área. Estos se deben transmitir a través de carpetas compartidas, si no la tiene, se debe solicitar al área de sistemas.

- No utilizar para enviar cadenas de comentarios, chistes y demás material que no aporte en el proceso laboral.

- Los correos no deben contener información que pudiera ser interpretados como ámbito de ataque, discriminación o ilegalidad. Todo lo que escriba bajo el dominio de la organización, es en representación de la misma y las palabras podrían ser utilizadas de formas no previstas. Por eso, antes de enviar, relea el correo y proceda a corregir de ser necesario, tratando de aclarar cualquier frase ambigüa o que se preste a suspicacias.

- El acceso a las cuentas personales debe ser el mínimo durante nuestra jornada laboral.

4.6. Seguridad de la contraseña:

Se recomienda crear una contraseña de fácil recordación pero que cumpla con las siguientes sugerencias:

- Cree una contraseñas fuerte que contienen números y letras.
- Utilice una contraseña que tenga por lo menos 8 caracteres.
- No socialice ni comparta su clave bajo ningún motivo.
- Se aconseja que su cuntraseña incluya símbolos como: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ con el objeto de hacerla más segura.

Como recomendación general de seguridad, se debe cambiar periódicamente las claves.

5. MANEJO DE ACCESO A INTERNET

El acceso a internet se encuentra protegido por filtros para disminuir sitios peligros que contenga código maliciosos o que se encuentren ajenos al servicio, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.

No navegar por sitios no confiables o no autorizados por el área de Sistemas y las Directivas del instituto.

No suministrar información institucional o personal en sitios desconocidos.

Queda prohibido el uso de sitios de radios online debido al ancho de banda que consume este servicio.

Queda prohibido el uso de intercambio de archivos (Ares, eMule, Torrents, Limewire, etc.).

Queda prohibido el uso de sitios de chat (Messenger, chat, etc.).

Queda prohibido el uso de internet para actividades ilícitas y/o fraudulentas que no solo exponen la seguridad corporativa sino también la imagen organizacional.

Queda prohibido la descarga que no cumpla con la normativa vigente de copyright y similar.

Se prohíbe el acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.

No compartir sus claves para ingresar a sitios que lo requiera como bancos o correo personal.

No permitir que el navegador de internet recuerde la contraseña automáticamente.

Queda prohibido participar en juegos de entretenimiento en línea asi como realizar compras online desde la red del Instituto.

Si no está navegando por internet, se sugiere cerrar todas las ventanas abiertas de su explorador.

Cualquier archivo que se reciba o descargue de internet deberá revisarse con el antivirus para asegurar que no tenga virus.

El área de Sistemas tiene la facultad de suspender el servicio de navegación en internet bajo circunstancias que así lo requiera (Virus, mal uso de internet, trafico sospechoso, etc.).

Si requiere navegar en algún sitio bloqueado el procedimiento es el de enviar la solicitud a través de la mesa de ayuda GLPI o por el correo electrónico al Subdirector Administrativo y Financiero, por parte del Jefe de área, justificando dicho acceso.

4.1. Manejo de redes sociales:

El área bloquea todo tipo de sitio relacionado con redes sociales, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus. Si algún funcionario por motivos de trabajo requiera acceder a ello, su Jefe de área o Gerencia debe enviar la solicitud formal al Subdirector Administrativo y Financiero por correo electrónico y al área de Sistemas a través de la mesa de ayuda GLPI, adjuntando el nombre del funcionario, área al que pertenece y motivo del acceso.
Cabe destacar que cualquier foto subida o comentario en facebook, twitter, Instagram o en alguna red social es responsabilidad exclusiva del que la emite y no compromete a IDARTES, a no ser que la misionalidad de su cargo así lo exija.

5. CLAVES DE ACCESO

El cambio de claves de acceso inalámbrico de todas las sedes debe ser cambiada periódicamente, por parte del área de sistemas máximo cada seis (6) meses, de manera ordinaria ó de inmediato ante casos que de forma extraordinaria así lo ameriten.

El cambio de claves de salida de llamadas a telefonia móvil desde el conmutador, debe ser cambiada periódicamente cada seis (6) meses de manera ordinaria o de manera extraordinaria se realizaría de forma inmediata ante casos que así lo ameriten.

Las claves de administrador de los equipos de escritorio y portátiles adscritos al IDARTES, deben ser protegidas y conservadas únicamente por el área de Sistemas y deben ser cambiadas periódicamente cada seis (6) meses de manera ordinaria o en caso extraordinario cuando el personal adscrito al área cambie.

Las claves de servidores solo deben ser de uso privativo de los profesionales con rol de administrador de red y deben ser cambiadas con una periodicidad de un (1) año ó cuando el personal con esos roles cambie.

6. SEGURIDAD FISICA

6.1. Ingreso al área de sistemas

El acceso al área de Sistemas esta verificado de manera inicial por el guarda de la recepción, quien permite o no el ingreso a dicha área. Para lograr ingresar a la zona en que está ubicada la infraestructura tecnológica se debe pasar por una puerta de vidrio templado que se encuentra seguida después de la sala de operadores. Sólo el área de Sistemas puede autorizar el ingreso a ésta área.

6.2. Bloqueo de estaciones de trabajos

Para generar una cultura de seguridad y prevenir hurto o acceso no permitido a la información y/o a su correo, se recomienda bloquear la sesión de usuario cada vez que se retire de su estación de trabajo, así sea por poco tiempo.

6.3. Escritorio limpio

Todos los escritorios o mesas de trabajo deben permanecer limpios, libre de objetos como portaretratos, juguetes, origami, etc., para proteger documentos en papel y dispositivos de

almacenamiento como CDs, memorias USB y demás medios de almacenamiento, además de proteger los teclados y las estaciones de trabajo con fin de reducir los riesgos de pérdida y daño de la información accidental durante el horario normal de trabajo y fuera del mismo.

7. CAPACITACIÓN

Todos los funcionarios y contratistas de IDARTES y de ser necesario empresas externas que desempeñen actividades en la entidad, deben ser capacitados y actualizados periódicamente en temas de seguridad, normas y procedimientos de IDARTES. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general.

8. DEFINICIONES

Procedimiento: Detalle de cursos de acción y tareas que deben realizar los usuarios para hacer cumplir las definiciones de las normas.

Estándares técnicos: Conjunto de parámetros específicos de seguridad para cada una de las tecnologías informáticas utilizadas.

Confidencialidad: La información solo puede ser conocida por las personas definidas.

Integridad: La información solo puede se creada y/o modificada por las personas autorizadas.

Disponibilidad: La información esté disponible cuando lo necesite el usuario.

Comité de Seguridad de la Información: Es un equipo integrado por representantes de las diferentes áreas de la organización, destinado a apoyar las iniciáticas de Seguridad de la Información.

Incidentes de Seguridad: Es cualquier evento que comprometa la confidencialidad, integridad y disponibilidad de la información de la organización

Política: Son instrucciones mandatorias que indican la intención de la alta gerencia respecto a la operación de la organización.

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

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.

Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios del IDARTES, pero que por las actividades que realizan en la Entidad, deban tener acceso a Recursos Informáticos.

Ataque cibernético: intento 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 si misma, sea o no protegida por reserva legal.