



**artesanías
de colombia**

**POLÍTICA DE SEGURIDAD DE LA
INFORMACION**

CODIGO: POLDPC03
Documento vigente a partir de:
2015/04/21

VERSIÓN:1

Página 1

POLÍTICA DE SEGURIDAD DE LA INFORMACION ARTESANÍAS DE COLOMBIA



 <p>artesanías de colombia</p>	<p>POLÍTICA DE SEGURIDAD DE LA INFORMACION</p>		<p>CODIGO: POLDPC03 Documento vigente a partir de: 2015/04/21</p>
	<p>VERSIÓN:1</p>	<p>Página 2</p>	

TABLA DE CONTENIDO

1. PREAMBULO	3
2. DISPOSICIONES GENERALES	3
2.1. DEFINICIONES	3
2.2. POLITICA DE SEGURIDAD	4
2.3. POLÍTICAS DE COPIA DE SEGURIDAD (BACKUPS).....	8
2.4. POLÍTICAS PARA CLASIFICACIÓN DE LA INFORMACIÓN	11

 <p>artesanías de colombia</p>	<p>POLÍTICA DE SEGURIDAD DE LA INFORMACION</p>		<p>CODIGO: POLDPC03 Documento vigente a partir de: 2015/04/21</p>
	<p>VERSIÓN:1</p>	<p>Página 3</p>	

1. PREAMBULO

La información es un activo en las organizaciones, por tanto, se deben tomar todas las medidas necesarias, para mantener y preservar información íntegra, oportuna y consistente, disponer de mecanismos de protección sobre los sistemas de información y recursos tecnológicos, a través de políticas automatizadas, controles de acceso, seguimiento y control permanente, en conjunto con todas las personas que hacen parte de la organización.

Esta política operativiza la declaración de valor con este mismo nombre y reemplaza el Instructivo “Módulo de seguridad” del proceso Gestión TICS, al ser de un mayor nivel institucional por su transversalidad.


2. DISPOSICIONES GENERALES

2.1. DEFINICIONES

BACKUP: Copia de seguridad, copia de respaldo o backup (su nombre en inglés) en tecnologías de la información, corresponde a una copia de los datos originales, para disponer de un medio para recuperarlos en caso de su pérdida, en el futuro.

Existen algunos tipos de backup:

- **Incremental:** Realiza copia de seguridad de los bloques que han sufrido algún cambio, requiere alto nivel de integración con el sistema de ficheros y el software de copias de seguridad.

 artesanías de colombia	POLÍTICA DE SEGURIDAD DE LA INFORMACION		CODIGO: POLDPC03 Documento vigente a partir de: 2015/04/21
	VERSIÓN:1	Página 4	


- Diferencial: Selecciona las variaciones de información de un backup respecto de un backup anterior.
- Total o Full: Copia de seguridad que incluye toda la información original.

2.2. POLITICA DE SEGURIDAD

Artesanías de Colombia, para lograr mantener la seguridad de la información, establece mecanismos como son: copias de seguridad y clasificación de los datos de las aplicaciones o software de la entidad, control de acceso a los recursos a través de seguridad perimetral y segmentación de la red. Para disminuir los riesgos que puedan atentar contra la privacidad, integridad, oportunidad y consistencia de la información se han implementado controles y herramientas de tecnología, de procesos de Ingeniería Social y controles físicos, que involucran el compromiso de todas las personas que interactúan con la infraestructura tecnológica de la organización, incluyendo a usuarios, administradores, visitantes, etc. Se describen a continuación:

Protección de la red interna (LAN)

Para minimizar riesgos de ataques por virus, spyware y malware por los mismos usuarios internos dentro de la LAN, se optó por implementar Endpoint Protection la solución antivirus corporativo de Symantec Corporate Edition. En el plan de gestión de tecnología anual, se incluye la actualización de esta herramienta y en la medida que el presupuesto asignado lo permita, cada año se actualiza.

 artesanías de colombia	POLÍTICA DE SEGURIDAD DE LA INFORMACION		CODIGO: POLDPC03 Documento vigente a partir de: 2015/04/21
	VERSIÓN:1	Página 5	


Adicionalmente, cada uno de los puntos de red tiene bloqueos para evitar múltiples equipos en un único puerto.

La totalidad del parque TI de la Entidad se ha actualizado a ambientes administrables de última generación (Windows X). Con esta medida las claves de administración se reservan para los funcionarios de tecnología, asignado solo claves de usuarios estándar a los funcionarios de los puestos de trabajo; controlando la instalación de software no licenciado.

Para mayor seguridad y capacidad en cuanto a estructura tecnológica, la infraestructura y plataforma tecnológica de la Entidad está implementada en Windows Server 20XX (Server 2008R2 y Server 2012), y toda la plataforma a nivel de cliente, basada en Windows X (Windows 7 y Windows 8) se conecta la plataforma de la Entidad a través del Directorio Activo (LDAP).

Con el advenimiento de la tecnología Wireless y sus grandes ventajas para la interconexión de equipos en red y comunicaciones en general, Artesanías de Colombia ha implementado esta tecnología, con la configuración de redes inalámbricas, las permiten atender usuarios internos que requieren acceso a los recursos corporativos y diferenciarlos de los usuarios tipo INVITADO, los cuales tiene acceso restringido.

Se han implementado enfoques y tecnologías VLAN (segmentación de la LAN). La segmentación se realiza por áreas funcionales, de tal manera que se permiten/restringen el acceso a los recursos corporativos, de acuerdo a las herramientas que requieren.

 artesánías de colombia	POLÍTICA DE SEGURIDAD DE LA INFORMACION		CODIGO: POLDPC03 Documento vigente a partir de: 2015/04/21
	VERSIÓN:1	Página 6	

Autenticación (usuarios y contraseñas)

Autenticación, mediante registro de usuarios y claves. Con esta medida se garantiza que solo los usuarios autorizados tengan acceso a los recursos de red, internet, sistemas de información y aplicativos en general que requieran para su labor diaria. Para ello se tiene asignado usuarios con sus respectivas claves, perfiles y permisos.

Con la utilización de LDAP de Windows Server 2012 se implementa las políticas que para autenticación de usuarios tiene este ambiente de trabajo, en especial para usuarios de aplicaciones, entre otros políticas: tamaño y complejidad en la conformación de claves, periodicidad en el cambio de claves, histórico de claves y número de intentos fallidos en la autenticación, entre otros más que se requieran.

En las aplicaciones (ERP, iSolucion, etc.) los usuarios tienen la opción de cambiar de manera manual la clave para ingresar y registrarse a estos mismos aplicativos. Algunos aplicativos tienen autenticación integrada con windows, lo que significa que la aplicación utiliza el mismo usuario y contraseña que solicita windows en el ingreso del computador.

A nivel de Windows los usuarios deben cambiar estas claves, mínimo cada mes, aplica otras políticas como validación de contraseñas históricas, entre otras mejoras establecidas por el área de sistemas.

Control de flujo eléctrico



Para evitar posibles pérdidas de información por caídas intempestivas del fluido eléctrico, es necesario el uso de UPS, actualmente la entidad cuenta con una UPS de 20KVA que permite dar autonomía eléctrica a los puestos de trabajo, cuando se interrumpe el fluido eléctrico, adicionalmente, elimina los picos de voltaje que pueden afectar los equipos.


Para el Centro de Datos, se instalaron dos UPS's de 6 y 3 KVA cada una. La UPS de 6 KVA, que para mayor autonomía tiene un banco adicional de baterías, soportan los servidores y la de 3 KVA los equipos de telecomunicaciones.

Seguridad perimetral

Para minimizar riesgos de ataques externos, además de virus, spyware, y demás software maligno que se bajan vía Internet, se implementaron Corta Fuegos (Firewall y/o UTM) a nivel de hardware propietario. Además de estos controles, estos equipos tienen las siguientes ventajas:

- Firewall: Inspección de contenido
- Antivirus, protege contra virus vía Internet.
- Anti Spam, previene contra correo basura.
- Detención y prevención de intrusos: evita ataques por Internet y que hackers ingresen a la red corporativa vía Internet.
- Políticas de horario, permite asignar horarios para acceso a los usuarios.
- Antigrayware: bloqueo de spyware y demás malware
- Filtrado de contenido: Filtrado y bloqueo por URL, sitios, palabras.

Ingeniera social

 artesánias de colombia	POLÍTICA DE SEGURIDAD DE LA INFORMACION		CODIGO: POLDPC03 Documento vigente a partir de: 2015/04/21
	VERSIÓN:1	Página 8	

Son todos los procesos que se han llevado al interior de la Empresa, para concientizar a los funcionarios (usuarios de las TIC) y prevenirlos contra la manipulación, que por diferentes medios y formas (correo electrónico, Web, entre otros) puedan ser objetos de hackers, con el fin de conseguir información confidencial que violen las políticas de seguridad informática definida en los puntos anteriores. Para ello se han llevado charlas, información vía mail o en intranet.

Controles físicos


Para prevenir ataques físicos ya sea de los mismos funcionarios de la Empresa así como de visitantes y personas externas, se implementaron controles físicos para el acceso al centro de datos.

2.3. POLÍTICAS DE COPIA DE SEGURIDAD (BACKUPS)

Dependiendo del tipo de información, Artesanías de Colombia estableció la siguiente política para copia de seguridad de la información:

Información procedente de los aplicativos que automatizan los procesos

Esta copia es responsabilidad y debe ser realizada por la oficina de sistemas. A partir de diciembre de 2014, con la instalación del sistema cloud backup, las copias de seguridad se realizan a través de herramientas de tecnología que utilizan internet, generando una copia de respaldo, en un servidor ubicado en un centro de datos en internet, fuera de las instalaciones de Artesanías de Colombia

 artesanías de colombia	POLÍTICA DE SEGURIDAD DE LA INFORMACION		CODIGO: POLDPC03 Documento vigente a partir de: 2015/04/21
	VERSIÓN:1	Página 9	

Aplicativos de los cuales se realiza copia de seguridad de la base de datos, en formato Filemaker, SQLServer, MySQL u Oracle:

- ERP (ZBOX)
- iSolucion
- Gestion Documental TQM
- Intranet


Mientras la administración técnica del software se encuentre en el área de sistemas, los nuevos sistemas de información se adhieren a la política de backup definida.

Periodicidad y tipo de copia de seguridad

Copia de seguridad total: Se realiza cada 15 días, a las 10:00 de la noche. Esta copia se hace con el sistema de Cloud Backup y se transmite por internet al centro de datos contratado, fuera de las instalaciones de Artesanías de Colombia. La base de datos se copia cifrada, que significa que su contenido únicamente esta visible a través de procesos de seguridad de información que convierten los datos en texto legible para las aplicaciones.

Copia de seguridad diaria e incremental: Se realiza todos los días (domingo a domingo) a las 10:00 de la noche. Esta copia se hace con el sistema de Cloud Backup y se transmite por internet al almacenamiento externo contratado.

Retención

 <p>artesanías de colombia</p>	<p>POLÍTICA DE SEGURIDAD DE LA INFORMACION</p>		<p>CODIGO: POLDPC03 Documento vigente a partir de: 2015/04/21</p>	
	<p>VERSIÓN:1</p>		<p>Página 10</p>	

La información de las copias de seguridad totales, tienen un periodo de retención de 10 años. La información de las copias de seguridad incrementales tiene un periodo de retención de 30 días.

Restauración


Ante desastres, saboteos y otras eventualidades se entra a llevar a cabo el siguiente proceso:

Para las bases de datos de las aplicaciones, se realiza un proceso de restauración de la base de datos de una fecha específica y disponible del sistema de backups. Para que la información esté disponible para un usuario final, esta debe ser interpretada por su aplicativo o software asociado, por lo cual, es necesario realizar la configuración del backup en un ambiente de pruebas, de acceso restringido.

Fuentes externas de datos

Para productos tecnológicos, cuya información administra y almacena un proveedor externo, como son: Google Apps, Dropbox, entre otras, los procesos de backup corresponden a los acuerdos de servicio realizados con el proveedor o el fabricante. Estos acuerdos normalmente se aceptan en el contrato, publicado a través de páginas web.

Para productos cuya información original, se encuentra almacenada en una plataforma tecnológica fuera de Artesanías de Colombia, propiedad de un tercero,

 <p>artesanías de colombia</p>	POLÍTICA DE SEGURIDAD DE LA INFORMACION		CODIGO: POLDPC03 Documento vigente a partir de: 2015/04/21
	VERSIÓN:1	Página 11	

por ejemplo: SIART, CENDAR, SIEAA, las copias de seguridad deben garantizar como mínimo la periodicidad diaria con retención de 30 días y una copia mensual con retención mínimo de 5 años, mientras el contrato y el contexto lo permita.


2.4. POLÍTICAS PARA CLASIFICACIÓN DE LA INFORMACIÓN

Como se mencionó al inicio de este documento, la información es el activo más valioso de las Empresas y entidades en general. Por lo tanto Artesanías de Colombia mantiene la siguiente clasificación de la información:

- **Información Pública:** Es la información institucional de interés general que produce la Empresa, y que por su condición de entidad de economía mixta debe publicar. Esta información es producida por diferentes áreas. Entre otra información la siguiente:

Información de invitaciones públicas y licitaciones: Esta información es producida por diferentes áreas y se produce con la asesoría y control de la Oficina Jurídica. Según las políticas de copia de seguridad, con las excepciones ahí detalladas, e independientemente de la oficina que la produzca y de la oficina jurídica, además de las copias en los respectivos equipos y puestos de trabajo, se debe hacer una copia en disco DVD-RW y se entregado al coordinador del área.

Información sobre contratos que realiza la Empresa durante los diferentes años.

 <p>artesanías de colombia</p>	POLÍTICA DE SEGURIDAD DE LA INFORMACION		CODIGO: POLDPC03 Documento vigente a partir de: 2015/04/21
	VERSIÓN:1	Página 12	

Información de la estructura orgánica de la Empresa y sus directivos.

Información que la Directiva presidencial 002, Agenda de Conectividad y Gobierno en Línea exige que se publique.


Esta información es pública en el portal de la Empresa:
www.artesantiasdecolombia.com.co

- Información privada: Es la información misional y demás requerida y necesaria para el funcionamiento y operación de la Empresa. Esta información es producida por los diferentes puestos de trabajo y la diferentes áreas, entre otras la siguiente:

Información de proyectos: Esta información es producida por la Subgerencia de Desarrollo. Esta información se almacena en el servidor propio del edificio donde están ubicados estos puestos de trabajo. La copia de seguridad se debe hacer desde ese equipo.

Información comercial. Obviamente es producida por las áreas que dependen de esta Subgerencia: Almacenes, compras, ventas nacionales e internacionales.

Información administrativa y financiera: Producida por sus respectivas áreas: presupuesto, tesorería, contabilidad, recursos humanos, servicios generales etc.

 <p>artesanías de colombia</p>	<p>POLÍTICA DE SEGURIDAD DE LA INFORMACION</p>		<p>CODIGO: POLDPC03 Documento vigente a partir de: 2015/04/21</p>
	<p>VERSIÓN:1</p>	<p>Página 13</p>	

Información Diseño: Producida por los Laboratorios de Diseño, por su tipo gráfica y tamaño es una información muy pesada y de gran volumen, por tanto según política de copia de seguridad, se debe depurar, y comprimir en la medida que sea posible, para respaldar solo la información que sea relevante y evitar guardar información innecesaria y redundante. Como ya se ha venido mencionando se debe hacer copia en disco DVD-RW y discos externos, y entregar una copia al coordinador.

- Información Sensible: La información privada, en especial la información de Diseño, y demás áreas misionales, es información sensible para la Empresa, por ello existen algunas políticas para su preservación y seguridad.

Se cuenta con toda una política de seguridad, descrita antes en este documento, para su preservación y administración: antivirus, corta fuegos, procesos para evitar la Ingeniería Social, proceso de autenticación de usuarios y controles físicos entre otros.

Política para copias de seguridad, igualmente descrita al principio de este documento, de manera que en caso de siniestros, accidentes, errores humanos o saboteos se pueda recuperar la información.

La información de Diseño, por su valor misional, procesamiento y custodia, es una de las más sensibles de la Entidad. Por esta razón, con miras a minimizar el riesgo de saqueo y/o sabotaje, en el contrato de cada diseñador existe una cláusula de confidencialidad y buen uso sobre la información que se les entrega y producen. Este misma cláusula debería existir en los contratos de cada uno de los funcionarios de las demás áreas misionales.

Por tecnologías, procesos y políticas de autenticación de usuarios, solo los funcionarios autorizados tienen acceso a la información privada y sensible de la Empresa

Por procesos, charlas, capacitaciones y en especial mensajes de correo electrónico para concientizar y sensibilizar a los funcionarios sobre los ataques de Ingeniería Social, se ha hecho una política agresiva en este sentido para evitar que los usuarios de los recursos y herramientas TIC confíen y entreguen sus claves de acceso a personas o funcionarios ajenos al proceso que maneja, y para el cual está autorizado. Igualmente para evitar que vía Internet y sus herramientas (Web y correo electrónico), delaten y difundan este tipo de información.

Con las herramientas que proveen los sistemas operativos, Windows X, se creó la política para que cada puesto de trabajo comparta y de permisos (en diferentes niveles, según sea el caso) sobre la información que deba o se requiera sea compartida con otros usuarios o puestos de trabajo. Mediante procesos para combatir la Ingeniería Social se ha hecho mucho énfasis en este tema y evitar que los puestos de trabajo exponga toda la información a toda la red corporativa.

Importante: Es responsabilidad de todos los funcionarios de la entidad tomar las precauciones necesarias, difundidas a través de la oficina asesora de planeación y las de conocimiento general, para proteger la red, como son: No ingresar a sitios sospechosos, no entregar información privilegiada de acceso, como son usuarios o contraseñas, no suministrar información específica de seguridad a terceros,



**artesanías
de colombia**

**POLÍTICA DE SEGURIDAD DE LA
INFORMACION**

CODIGO: POLDPC03
Documento vigente a partir de:
2015/04/21

VERSIÓN:1

Página 15

controlar el acceso de personas ajenas a la entidad, informar al área técnica sobre correos electrónicos o páginas web sospechosas, evitar ingresar a sitios donde soliciten usuario y contraseña a través de búsquedas en motores como Google, yahoo, etc, deben ingresar directamente por la dirección de la página previamente conocida, compartir la clave de acceso o red de datos con compañeros de trabajo, dado que el usuario de red y de acceso a las aplicaciones es personal e intransferible, evitar el uso de contraseñas fáciles de adivinar por otras personas, entre otras.

Elaboró/Actualizó	Revisó	Aprobó:
Angela Milena Dorado Egas Especialista de proyecto Oficina asesora de planeación e información	Johanna Paola Andrade S Profesional Oficina asesora de planeación e información	Andrea García Jefe Oficina asesora de planeación e información