POLÍTICA DE SEGURIDAD DE LA INFORMACION ARTESANÍAS DE COLOMBIA

TABLA DE CONTENIDO

1. INTRODUCCION

La información es un activo de los mas importantes en las organizaciones, por tanto, se deben tomar todas las medidas necesarias, para mantener y preservar información integra, oportuna y consistente, disponeniendo 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.

La política general de seguridad y privacidad de información para Artesanías de Colombia, hace parte de los requisitos para avanzar en la implementación del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Establecer y determinar las pautas y lineamientos para la protección de la Información de Artesanías de Colombia, cumpliendo con sus principios fundamentales de Confidencialidad, Disponibilidad e Integridad, además de no repudio, entre otros, y teniendo en cuenta los requisitos legales, operativos, tecnológicos, alineados con el contexto de direccionamiento estratégico y de gestión del riesgo.

2.2. OBJETIVOS ESPECÍFICOS

Artesanías de Colombia, para el cumplimiento de su misión, visión, objetivos estratégicos y alineados a sus valores corporativos, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

- Cumplir con los principios de seguridad de la información: Disponibilidad,

Confidencialidad, e Integridad, a fin de mantener la confianza de usuarios del sector artesanal y la ciudadanía en general

- Lograr que los funcionarios contratistas, pasantes y/o practicantes de la Entidad se comprometan con el apropiado uso y protección de la información, los equipos y tecnologías que la procesan y almacenan, y con todos los activos de información en general.
- Identificar e implementar las tecnologías y controles necesarios para cumplir con estos principios, para proteger
- Proteger la información y en general todos los activos de información de la Entidad.
- Proteger todos los activos tecnológicos que hacen posible el procesamiento y registro y almacenamiento de la información institucional
- Dar cumplimiento a los lineamientos establecidos a la política de Gobierno Digital, y más específicamente al Modelo de seguridad y Privacidad de la Información.

3. DEFINICIONES

Antivirus: Es el software de seguridad informática que detecta, contrala y minimiza los ataques software y contenidos maliciosos (malware) provenientes normalmente de correos electrónicos, de la web y en general de las diferentes herramientas de Internet.

Activo de información: Cualquier tipo de información o sistema relacionado con el tratamiento de la misma que tenga valor para la Entidad. En este sentido, es todo activo que contiene información, la cual posee un valor y se requiere para realizar los procesos misionales, administrativos y operativos de la Institución. Se pueden clasificar de la siguiente manera:

- Datos: Elementos básicos de la información (en cualquier medio o formato) que se generan, acopien, recogen, gestionen, procesen para crear información, La cual es

compartida y/o transmitida y finalmente se destruyen cuando cumpla su vida útil. Ejemplo: hoja en Excel para llevar control de asistencia a un evento o reunión “lista de asistencia.xlsx”

- Aplicativo o programa: Es todo el software que se utiliza para la gestión de la información. Ejemplos: ZBOX, TQM
- Personal: Son los funcionarios de cualquier nivel, los contratistas, pasantes, clientes, usuarios y ciudadanía en general, que estén autorizados y tenga acceso (disponibilidad) por diferentes medios y maneras a los activos de información de una organización.
- Servicios: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios. Ejemplo: Catálogo de servicios, solicitud de vacaciones.
- Tecnología: Son todos los equipos utilizados para gestionar la información y las comunicaciones. Ejemplo: equipo de cómputo, teléfonos, impresoras.
- Instalaciones: Son todos los lugares en los que se alojan los sistemas de información. Ejemplo: Data Center loca; servicios de hosting o de computación en la Nube

BACKUP (Copias de Seguridad): 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.

- 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.
- 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.

Confidencialidad: Significa que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados. Es decir, el acceso a la información por parte únicamente de quienes estén autorizados

Disponibilidad: Es la característica o propiedad de la información de estar disponible para su uso cuando lo requiera una entidad autorizada, en el entendido de entidad a personas procesos o aplicativo.

Integridad: Propiedad de salvaguardar la exactitud y completitud de la información y sus métodos de proceso, los cuales deben ser exactos.

Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. Puede estar almacenada y registrada en diferentes forma y medios, así: medio físico (impresa o registrada en papel), o puede estar almacenada digital o electrónicamente; así mismo puede ser transmitida en medios físicos y en medios electrónicos.

Ingeniería Social: Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten información con clasificación confidencial o superior.

Hardware: Conjunto de componentes que integran la parte material de una computadora o equipo electrónico en general.

LAN: Local Área Network (por sus siglas de ingles), Red de Área Local en español, es el conjunto de computadores dentro de las instalaciones o edificio de una empresa, que están interconectados entre sí para compartir recursos, servicios y herramientas TI, información, almacenamiento, documentos, e impresoras entre otros.

Malware: Es una forma abreviada del término inglés "malicious software" (software

malicioso) y hace referencia a virus, spyware, gusanos, etc. El **malware** está diseñado para causar daños a equipos independientes o conectados en red.

Pólitica: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Mejor practica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema,

los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Seguridad de la Información: Hace referencia a la preservación de los principios fundamentales de la información, es decir. Confidencialidad (principio o propiedad, que establece que la información está disponible o revelada única y exclusivamente a individuos, entidades o procesos autorizados), Integridad (protección de la exactitud e integridad de los activos) y Disponibilidad (propiedad que establece que la información debe poder ser accesible y asequible para los usuarios, procesos y entidades autorizados).

Seguridad Perimetral: En informática, la seguridad perimetral es un método de defensa de red, que se basa en el establecimiento de recursos de seguridad en el perímetro de la red y a diferentes niveles, permitiendo definir niveles de confianza, en el acceso de usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros. El recurso o tecnología de seguridad en el perímetro se conoce como Firewall (Corta fuegos en español), y se puede implementar a nivel de Hardware o de Software.

4. MARCO LEGAL Y/O NORMATIVO

- LEY 23 DE 1982 sobre Derechos de Autor. Congreso de la República.
- CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991; Artículo 15. “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

- LEY 527 DE 1999; por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

- LEY 1266 DE 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- LEY 1273 DE 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- LEY 1474 DE 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

- DECRETO 4632 DE 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.

- LEY ESTATUTARIA 1581 DE 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.

- DECRETO 2609 DE 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".

- DECRETO 2693 DE 2012 Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
- LEY 1712 DE 2014; Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones.

- DECRETO 2573 DE 2014 Por el cual se establecen los lineamientos generales de

la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

- DECRETO 103 DE 2015, por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- Decreto 728 de 2017: Se reglamenta la implementación y puesta al servicio de los ciudadanos el servicio la "Zona WiFi GRATIS para la GENTE", por parte de la Entidades del Estado.

- Política de Gobierno Digital, establecida mediante el Decreto 1008 de 2018, forma parte del Modelo Integrado de planeación y Gestión (MIPG) y se integra con las políticas de Gestión y Desempeño Institucional en la dimensión operativa de Gestión para el Resultado con Valores, que busca promover una adecuada gestión interna de las entidades y un buen relacionamiento con el ciudadano a través de la participación y la prestación de servicios de calidad.

5. POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

5.1. ALCANCE

La Política de Seguridad de la Información aplica a todo la Entidad, es decir a funcionarios de todos los niveles jerárquicos, así como a los contratistas, pasantes y terceros, que tengan acceso a información registrada tanto en medios físicos, como electrónicos y/o digitales

5.2. LINEAMIENTOS DE LA POLITICA DE SEGURIDAD

La dirección de Artesanías de Colombia S.A., entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación el cumplimiento de los requisitos asociados a seguridad de la información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y

visión de la entidad.

Para Artesanías de Colombia, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a la Entidad según como se define en el alcance, a sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de Artesanías de Colombia
- Garantizar la continuidad del negocio frente a incidentes.
- Artesanías de Colombia ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Dentro de las temáticas involucradas se encuentran la gestión de activos, seguridad física

y ambiental, control de accesos, definición de roles y responsabilidades, política de escritorio limpio y todas aquellas que hacen parte del sistema de gestión de calidad en el proceso de Gestión de Tics y corresponden a políticas y guías complementarias.

5.3. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

5.4. SEGURIDAD Y DISPONIBILIDAD DE SERVICIOS E INFORMACIÓN

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, control de acceso a los sistemas de información y recursos de red, parámetros mínimos de seguridad en la nube, definición de roles y responsabilidades. Para disminuir los riesgos que puedan atentar contra la privacidad, integridad, oportunidad y consistencia de la información se han implementado mecanismos y herramientas de tecnología, que previenen y controlan ataques internos y externos contra la infraestructura TIC; así mismo se previene procesos de Ingeniería Social y se implementan controles físicos, que involucran el compromise 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, spywere y malwere por los mismos usuarios internos dentro de la LAN, se optó por implementar Enpoint Protection la solución antivirus corporativo de Symantec Corparate 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.

Adicionalmente, cada uno de los puntos de red tiene activada en los Swtich la opción de bloqueos para prevenir y evitar que múltiples equipos se conecten en un único Puerto, o la conexión de varios dispositivos en un intervalo corto de tiempo (port security).

La totalidad del parque TI de la Entidad se ha actualizado a ambientes administrables de última generación (Windows XX). 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 como ya se mencionó todo el parque TI o la plataforma a nivel de cliente o puestos de trabajo, está basada en Windows XX PRO (Windows 7, Windows 8 y Windows 10), todo con un enfoque de conectividad 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, en 3 niveles

de acceso así: En el primer nivel una zona WiFi corporativa con privilegios que permiten atender usuarios internos que requieren acceso a los recursos corporativos de la Entidad; en un segundo nivel una red WiFi de "INVITADO" que no tiene accesos a los recursos corporativos, es totalmente restringido y solo puede acceder a Internet y sus herramientas, deben ingresar a través de un portal cautivo; y un tercer nivel con una red totalmente abierta que da respuesta al requerimiento la Política de Gobierno Digital, que mediante el Decreto 728 de 2017 ordena a todas las Entidades del Estado implementar y poner al servicio de la ciudadanía una red wifi libre, con el nombre de "Zona wifi GRATIS para la Gente", que tiene totalmente restringido el acceso a la infraestructura corporativa, y solo tiene acceso a Internet.

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. Además, estas tecnologías permiten la segmentar y colocar en un segmento de red totalmente separado, la redes de "INVITADO" y "Zona wifi GRATIS para la Gente", con lo cual se restringe y garantizar el no acceso a la infraestructura TIC institucional.

- **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 otras 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.

Los controles mencionados son heredados por aquellos sistemas de información que hacen uso de autenticación integrada con Windows, siendo este mecanismo el sugerido por el proceso de Gestión de TICs para ser incorporado como requisito en la adquisición de nuevos sistemas de información.

- **Control de flujo eléctrico**

Para evitar posibles pérdidas de información por caídas intempestivas del fluido eléctrico, es necesario el uso de UPS. Para este propósito, actualmente la entidad cuenta con 3 UPS'S de 40, 20 y 5 KVA respectivamente, que permite dar autonomía eléctrica al DATA CENTER y a los puestos de trabajo, cuando se interrumpe el fluido eléctrico, adicionalmente, elimina los picos de voltaje que pueden afectar los equipos. La UPS de 40 KVA está dispuesta para soportar los equipos que hacen parte del DATA CENTER, de tal manera que permita mayor autonomía en caso que haya un fallo de corriente eléctrica, y las UPS´S de 20 y 5 KVA soporta la carga de los equipos del parque TI y/o los puestos de trabajo de la Entidad.

Con la restauración del claustro se instaló una planta eléctrica de 720 KVA, que soporta los sistemas de bomba hidráulicas contra incendios. No obstante, también se tiene previsto conectar los sistemas de UPS a la planta eléctrica de manera que se tenga una mayor autonomía, casos de caídas de fluido eléctrico.

- **Seguridad perimetral**

Para minimizar riegos de ataques externos, además de virus, spywere, 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.
- Antigraywere: bloqueo de spyware y demás malwere
- Filtrado de contenido: Filtrado y bloqueo por URL, sitios, palabras.

- **Ingeniera social**

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 de la información definida en los puntos anteriores. Para ello se han llevado charlas, información vía mail y en intranet.

Lo anterior se socializa con información en Intranet, correo electrónico y con instrucciones directas a los usuarios.

- **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, es así, como el acceso al centro de datos es restringido al personal de TI, y el acceso a la entidad es controlado por personal supervisado por la

Subgerencia Administrativa y Financiera.

La puerta del Centro de Datos además de tener todos los aspectos que se requieren para este tipo de espacios, es anti-pánico; es decir estando con toda la seguridad de chapas y demás, se puede abrir desde adentro, por si alguien quedar encerrado.

El centro de datos dispone de tecnologías para detección de incendios, y se dispone de dos extintores

5.5. GESTIÓN DE INCIDENTES

La Entidad dentro de la política de Gestión de Incidentes incluye la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información, dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.

Todo incidente, evento o vulnerabilidad debe ser reportado al área de Gestión de TICs a través de la mesa de servicios quienes deben analizar técnicamente la trazabilidad del incidente o evento, intentar identificar las causas y aplicar un plan de choque para evitar la proliferación de la falla y un plan de remediación a profundidad.

Cuando los incidentes o eventos reportados son catalogados como un delito, éstos deben ser escalados a la Jefatura de la oficina de planeación y a la Alta dirección, adicionalmente, de acuerdo a las características del incidente puede ser reportado a la unidad de delitos informáticos de la policía nacional. Cuánto éstos involucran infraestructura crítica nacional, deben ser reportados al Ministerio de Tecnologías de la Información y el Comando Conjunto cibernético, a través de CSIRT Gobierno (Equipo de Respuesta ante Emergencias Infotmáticas)

5.6. POLÍTICAS DE COPIA DE SEGURIDAD (BACKUPS)

Dependiendo del tipo de información, Artesanías de Colombia establece los lineamientos en la Política de Seguridad para realizar copias de seguridad.

- **Información procedente de los aplicativos que automatizan los procesos**

Esta copia es responsabilidad y debe ser realizada por la oficina o área de TIC'S. Con la instalación del sistema cloud backup, las copias de seguridad de aplicativos y Bases de Datos se realizan tanto de manera local o interna (In Side), como de manera externa (out side). La copia externa se hace en la Nube, y 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.

De manera local de igual forma se hace a través de una herramienta que toma la información de los aplicativos y Base de Datos, y se llevan a un unidad de almacenamiento ubicado en el Data Center. Estas copias, tanto local como en la nube se llevan a cabo entre las 10 de la noche y 6 de mañana del dia siguiente.

- **Periodicidad y tipo de copia de seguridad**

  La periodicidada de la copia es diariamente 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.

  La Copia de seguridad local se hace diariamente: Se realiza todos los días (domingo a domingo) a las 10:00 de la noche.

- **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, 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.

5.7. 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 establece la clasificación de la información a través del documento “Matriz de activos

de información Institucional" la cual se encuentra publicada en el portal de la entidad y en el Portal de datos abiertos del Estado Colombiano o en la herramienta que lo modifique o sustituya.

5.8. RESPONSABILIDADES DE LOS USUARIOS DE RECURSOS TECNOLÓGICOS Y SISTEMAS DE INFORMACIÓN

Es responsabilidad de cada uno de los funcionarios tener y colocar la copia de seguridad en los medios y elementos definidos para este propósito.

De iugal manera es responsabilidad de los funcionarios de la entidad tomar las precauciones necesarias, difundidas desde la oficina asesora de planeación e información 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, 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.

Cada funcionario es directamente responsable sobre el uso de las credenciales (usuario y contraseña) que le fueran entregados, incluso cuando se encuentra ausente o en vacaciones, dado que la contraseña debe guardar su característica de privacidad y confidencialidad en todo momento.

Cuando se trate de contratistas o terceros, es el supervisor de los mismos, quien debe socializar la Política de Seguridad de la Información y la Política de Control de

Acceso, para ello, directamente el supervisor debe solicitar la creación o eliminación, según sea el caso, de los accesos que se requieran para que el tercero realice sus obligaciones.

6. POLITICA PROTECCION DE DATOS PERSONALE

En relación al Ley 1581 de 2012, Artesanias de Colombia definió, desarrolló e implementó la Poltica de Protección de Datos Personales, la misma se encuentra publicada en el portal institucional de la Entidad.

7. NATURALEZA DEL CAMBIO

Versión	Fecha	Naturaleza del cambio
0		Publicación de la política inicial.
1	21/Abril/2015	Ajuste a la política para incluir lineamientos de Gobierno en Línea
2	30/Marzo/2017	Ajuste a la política para incluir lineamientos de Gobierno en Línea
3	26/Diciembre/2018	Ajuste a la política para incluir la normatividad aplicable
4	10/05/2019	Ajustes para generar versión 2

Elaboró/Actualizó	Revisó	Aprobó:
Medardo Alfonso Castillo O. Profesional de Gestión Oficina asesora de planeación e información	**Leonardo Martin Puentes** Profesional de Gestión Oficina asesora de planeación e información	**María Mercedes Sánchez Gil** Jefe Oficina asesora de planeación e información