POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. OBJETIVO

Establecer lineamientos o normas frente a la seguridad de la información que se gestiona en el despacho de la Curadora urbana 1 de Funza y todos sus funcionarios y contratistas, teniendo en cuenta los requisitos legales, operativos y tecnológicos necesarios para la prestación de los servicios en la Entidad.

2. ALCANCE

La política de seguridad reglamenta la protección y uso de los activos dispuestos por la Curadora Urbana para el funcionamiento del Despacho y, está dirigido a todo el personal de la oficina o usuarios que posean algún tipo de contacto con estos.

Los funcionarios de la Curaduría deben diligenciar un acuerdo de confidencialidad y reserva, el cual, refiere al cumplimiento de las políticas de seguridad que se describen, con el propósito de garantizar la protección de la información que se obtiene a través de los tramites o procesos realizados.

Los usuarios de la información se clasifican así:

a) Curador: es el actor principal por cuanto es el directamente responsable de la custodia de la información y del resguardo de su seguridad, que se genera dentro de las instalaciones, así como, la información que es entregada a algún funcionario de su oficina.
b) Personal de la Oficina: empleados o colaboradores de planta que han suscrito un contrato laboral.
c) Contratistas: Se definen como contratistas, a las personas que han suscrito un contrato de prestación de servicios.
d) Entidades de Control - Procuraduría General de la Nación, Superintendencia de Notariado y Registro, entre otras.

3. NORMATIVIDAD

Para la implementación de la estrategia de seguridad de la información, la Curaduría se regirá por lo dispuesto en el marco jurídico y normativo aplicable, el cual, se conforma por las siguientes, además de las que las complemente, modifiquen o sustituyan.

Decreto-Ley 960 de 1970, Ley 527 de 1999.
Decreto-Ley 019 de 201, Resolución 5633 de 2016 de la Registraduría Nacional del Estado Civil
Resolución 14681 de 2015

Instrucción Administrativa 03 de 2017 de la Superintendencia de Notariado y Registro.

4. DEFINICIONES

- Activo: Cualquier bien que tenga valor para la organización.
- Acuerdo de Confidencialidad: Es un documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de la oficina.
- Contraseña: Clave de acceso a un recurso informático.
- Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.
- Política: Toda intención y directriz.
- Protector de pantalla: Programa que se actia a voluntad del usuario, automáticamente después de un tiempo en el que no ha habido actividad.
- Recursos informáticos: Son aquellos elementos de tecnología de Información tales como: computadores, servidores de aplicaciones y de datos, computadores de escritorio, computadores portátiles, elementos de comunicaciones, elementos de almacenamiento de información, programas y datos.

5. POLÍTICAS DE SEGURIDAD INFORMÁTICA

Son normas de obligatoriedad por parte de todo el personal de planta y contratista de la Curaduría Urbana No. 1 de Funza, que se encuentran dentro de la oficina y se han clasificado así:

- Políticas de contraseñas.
- Política de escritorio limpio y pantalla.
- Política de administración de los recursos informáticos.
- Políticas de internet y correo electrónico.
- Políticas de administración de la red.
- Políticas de cumplimiento
- Políticas de acceso físico

5.1 Políticas de contraseñas

5.1.1 Confidencialidad

La contraseña que tendrá el personal de la oficina para el acceso a la utilización de los servicios tecnológicos es personal, confidencial e intransferible. Cada usuario debe velar porque sus contraseñas no sean vistas o aprendidas por otras personas.

5.1.2 Características de la contraseña

Las contraseñas deben contener o cumplir con las siguientes características: incluir mayúsculas, minúsculas y caracteres especiales. El tamaño será validado por el sistema en el momento de generar la contraseña para impedir que sea un tamaño menor. La contraseña no debe contener nombres propios, ni palabras del diccionario, deben ser una mezcla de número, letras y caracteres especiales.
Todo el personal creara la contraseña al ingresar a la oficina y realizaran su cambio por lo menos cada seis meses.

5.1.3 Almacenamiento de las contraseñas

Ninguna contraseña debe ser guardada de forma legible en archivos “batch”, scripts, macros, teclas de función de terminal, archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas. Ningún usuario está autorizado para tener su contraseña en cualquier medio impreso.

5.1.4 Sospecha de compromiso de la contraseña

Toda contraseña deberá ser cambiada de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.

5.1.5 Revelación de contraseñas

En ninguna circunstancia está permitido que el personal de la oficina revele su contraseña a empleados o terceras personas. La contraseña es personal no beben ser digitada en presencia de terceras personas, así sean personal de equipo de trabajo. Todos los computadores y demás recursos tecnológicos que se encuentran dentro de la oficina contaran con un sistema de control de acceso.

5.2 Política de escritorio limpio y pantalla

El escritorio del equipo de trabajo asignado al personal debe estar despejados y ordenados, de tal forma que la información sensible o privada se encuentre resguarda y bajo llave evitando mantenerla a la vista de terceras personas. Es responsabilidad de cada persona del equipo de trabajo mantener y resguardar la confidencialidad de la información que maneja.

Se debe aplicar un solo fondo de pantalla para las estaciones de trabajo ubicadas dentro de la oficina este no debe ser alterado o cambiado.

5.2.1 Bloqueo estación de trabajo

Las estaciones o equipos de trabajo del personal tendrán activado un bloqueo automático de estación el cual se activará luego de un periodo de ausencia o inactividad de 5 minutos.

5.2.2 Control criptográfico

La Curadora y el personal designado de la Administración para gestionar firma digital o mecánica, debe realizarlo de forma exclusiva, personal e intransferible y se debe procurar que realice todos los procesos correspondientes en las plataformas durante todo el tiempo que labore en la oficina.

El personal o administrador de los tokens deben proteger la confidencialidad, integridad e inviolabilidad de la contraseña suministrada por el ente emisor. En caso de robo o pérdida informar inmediatamente al área certificadora para efectuar el bloqueo.

5.3 Política de administración de los recursos informáticos

5.3.1 Asignación y uso de los recursos informáticos

El uso del computador personal y demás recursos informáticos por parte de los empleados, contratistas y demás usuarios de la información de la Curaduría, deben someterse a todas las instrucciones técnicas que imparta el encargado de los recursos tecnológicos y de la seguridad de la información por indicación de la Curadora. El personal realizara cada tres meses una limpieza de los archivos, temporales, cookies, datos en cache, etc.

5.3.2 Prohibición instalación de software y hardware en los computadores.

La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de cómputo o demás recursos informáticos solo puede ser realizada por el personal delegado por la Curadora.

5.3.3 Bloqueo de puertos

Los equipos asignados a la oficina tendrán el bloqueo de puertos, brindando seguridad y resguardo a la información que se encuentra alojada en los computadores.

5.3.4 Control de recursos informáticos entregados a los funcionarios

Según contrato laboral firmado por el personal al momento de vincularse, diligenciara el acuerdo de confidencialidad (personal).

5.3.5. El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados.

Todo el personal es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien fue otorgada. Los usuarios no deben permitir que otros interesados realicen labores bajo su identidad. De forma similar, los funcionarios no deben realizar actividades bajo la identidad de alguien más.

La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del funcionario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de la oficina.

5.3.6 Software de identificación de vulnerabilidades

Los equipos de cómputo tendrán antivirus activo siempre.

5.3.7 Límite de intentos consecutivos de ingreso al sistema.

Todas las contraseñas por defecto que incluyen equipos deberán ser cambiadas siguiendo los lineamientos de la política “Contraseñas fuertes”.

5.3.8 Respaldo de la información

Para salvaguardar la integridad y seguridad de los trámites e información que se maneja dentro de la Curaduría, estos reposarán en un área establecida bajo las medidas adoptadas por la Curadora. Adicional se realizará la digitalización de la información y podrán ser consultados o validados desde la herramienta “drive”.

5.3.9 Clasificación de la información

Todos los activos de la Curaduría estarán claramente identificados y se realizara un inventario actualizado. Los funcionarios y contratistas deben recogerán la información que se imprima inmediatamente para evitar la divulgación confidencial.

La información que se gestione dentro en la Curaduría debe estar relacionada directamente con los tramites que se presten en esta. Los funcionarios y los contratistas no deben realizar la divulgación de ninguno de los trámites que se adelanten en la Entidad a terceros, y deben proporcionar el resguardo, confidencialidad e integridad de la información privada o sensible que se maneja.

5.4 Políticas de internet y correo electrónico

5.4.1 Prohibición de uso de internet para propósitos personales.

El uso del internet está limitado exclusivamente para propósitos laborales. Los usuarios serán notificados.

5.4.2 Intercambio de información a través de internet

La información sensible o privada que los funcionarios y contratistas de la Curaduría, requieran enviar por internet, se debe transmitir con la mayor seguridad posible entre las dos partes.

5.4.3 Preferencia por el uso del correo electrónico

Toda comunicación a través de correo electrónico de funcionarios y contratistas se debe realizar desde los correos corporativos correspondiente.

5.4.4 Chequeo de virus en archivos recibidos en correo electrónico.

Los funcionarios y contratistas deben asegurar que todos los archivos descargados de Internet sean chequeados por un software de detección de virus informático, antes de ser transferidos a los computadores.

5.5 Políticas de administración de la red

5.5.1 Servicios de red

Se debe garantizar que el servicio de red utilizado dentro de la Curaduría, se encuentre disponible y operando adecuadamente según los parámetros establecidos por la Curadora.

5.1.1 Protección de vulnerabilidades

Los equipos que se utilicen dentro de la Curaduría tendrán activo un antivirus de protección.

5.1.2 Sincronización de reloj

Todos los equipos de la oficina deben ser sincronizados según la zona horaria establecida para Colombia-Bogotá, los cuales no deben ser alterados, ni modificados en caso de presentarse alguna alteración con el sistema inmediatamente informar al personal asignado

5.1.3 Control de recurso móvil entregados

Al generar la entrega de móviles al personal de la oficina, se firmará el formato de entrega, este será para uso exclusivo de la Curaduría, en caso de robo o perdida se informar inmediatamente a la Curadora.

5.6 Políticas de cumplimiento

5.6.1 Cumplimiento de la norma

Todo los funcionarios y contratistas que se encuentren dentro de la Curaduría deben cumplir con los estándares de normas y controles vigentes, antes de realizar el ingreso al área establecida.

5.6.2 Medidas por incumplimiento de la política de seguridad

Cualquier incumplimiento de una política de seguridad de la información, estándar, o procedimiento es un argumento válido para que sea tomada como llamado de atención.

5.6.3 Cumplimiento con la seguridad de la información

Todos los funcionarios y contratistas deben cumplir y acatar las políticas y los procedimientos en materia de protección y seguridad de la información.

5.6.4 Declaración de reserva de derechos del despacho de la Curadora

La Curadora usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada en computadores y sistemas de información. Para mantener estos objetivos la Curadora se reserva el derecho y la autoridad de: 1. Restringir o revocar los privilegios de cualquier persona del equipo de trabajo; 2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados; y, 3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de la Curaduría. Esta autoridad se puede ejercer con o sin conocimiento de los funcionarios y contratistas, bajo la responsabilidad del técnico designado y la Curadora.

5.7 Políticas de acceso físico

5.7.1 Carné del personal

Los funcionarios y contratistas durante la permanencia en la Curaduría deben portar el carné de esta.

5.7.2 Acceso a zonas restringidas

Los funcionarios y contratistas que se encuentra dentro de la Curaduría no podrán dejar ingresar a personal externas a zonas restringidas.

5.7.3 Robo o perdida de identificación

En caso de robo o pérdida del carné se debe informar inmediatamente a la Curadora.

5.7.4 Los privilegios de acceso a los recursos informáticos cuando termine el periodo de la Curadora

Todos los privilegios sobre los recursos informáticos otorgados al personal serán eliminados en el momento de la culminación del periodo de la Curadora.

5.7.5. Orden de salida de activos

Todos los activos que afecten la seguridad de la información de la Curaduría como medios de almacenamiento, CD, USB, Discos Duros, entre otros, y que necesiten ser retirados de la Entidad, deben ser autorizados por la Curadora.