POLÍTICA DE ACCESO A LAS TECNOLOGÍAS DE LA INFORMACIÓN

SERVICIUDAD E.S.P
DOSQUEBRADAS

Elaboró	Revisó	Aprobó
Harrison González Santa	**Wilson Arias Castaño**	**Mauricio Andrés Rodas T**
Técnico grado 3 sistemas	Profesional especializado	Subgerente Planeación (e)
Fecha: 26/11/2021	Fecha: 29/11/2021	Fecha: 29/11/2021

TABLA DE CONTENIDO

INTRODUCCIÓN

Para SERVICIUDAD E.S.P, La Política de Acceso a las Tecnologías de la Información genera sinergia en escenarios de confianza sobre la operación de la infraestructura tecnológica, permitiendo como resultado conectar eficientemente las necesidades priorizadas con las capacidades institucionales y los retos plasmados en los planes de desarrollo a los cuales se encuentra alineada la Entidad.

La Política de Acceso a las Tecnológicas de la Información utiliza mecanismos de transformación basados en el uso adecuado de las TIC, como soporte a todos y cada uno de los proyectos que conforman el Portafolio de Servicios de la Dirección de la Oficina de TI.

1. DEFINICIONES

Acceso: El nivel y la extensión de la funcionalidad de un servicio o los datos que un usuario tiene derecho a utilizar.

Identidad: Información acerca de los usuarios que verifica su estado dentro de la Entidad.

Derechos Son los privilegios que toman en cuenta la configuración real que se le provee a los usuarios con el acceso a un servicio, o grupo de servicios. Los derechos típicos, o niveles de acceso, incluyen: Leer, escribir, ejecutar, cambiar y borrar

Sistema de información: Es el conjunto de instrucciones, órdenes y reglas que un equipo de cómputo debe ejecutar, orientados al tratamiento y administración de datos e información.

Proceso: Es un conjunto de actividades que constituyen una cadena de valor para un producto o un servicio.

Recurso: Factores de tipo humano, financiero, funcional y técnico, que al combinarse tienen la capacidad de generar valor en la prestación de los servicios.

Tecnología de la Información (TI): Herramienta de gestión para el almacenamiento, comunicación y procesamiento de información a través del uso y apropiación de la tecnología.

Usuario: Colaboradores, contratistas, pasantes universitarios y SENA, personal temporal y otras personas relacionadas a terceras partes, que accedan a las tecnologías para desarrollar sus funciones y actividades asignadas.

Validación: Una Actividad que asegura que un Servicio de TI, Proceso, Plan u otro Entregable nuevo o cambiado satisface las necesidades del Negocio.

2. NORMATIVIDAD RELACIONADA

ISO 27001: Norma de la Seguridad de la Información

Ley Estatutaria 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 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 1008 de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Ley 1341 de 2009: Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC- se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. Esta Ley promueve el acceso y uso de las TIC a través de su masificación, garantiza la libre competencia, el uso eficiente de la infraestructura y el espectro, y en especial, fortalece la protección de los derechos de los usuarios.

3. OBJETIVO

Ofrecer directrices para brindar garantías de acceso, validación y soporte a los usuarios que requieran el uso de tecnologías de información como apoyo de sus funciones al interior de cada uno de sus procesos.

4. ALCANCE

La Política de Acceso a las Tecnologías de la información de SERVICIUDAD E.S.P está dirigida a todos aquellos usuarios que hagan uso de componentes tecnológicos para el desempeño de sus actividades, teniendo en cuenta la validación, control y soporte de acceso requerido por parte de éstos.

5. PRINCIPIOS

Los principios definidos para la Política de Acceso a las Tecnologías de Información de SERVICIUDAD E.S.P son:
Ciberseguridad: Es la práctica de defender y proteger la infraestructura tecnológica de ataques maliciosos que afecten la integridad y privacidad de la información.
Transparencia de Acceso: Es la práctica ética de cada usuario para ingresar bajo sus credenciales personalizadas y asignadas por la Dirección de la Oficina de TI.

Accesibilidad: Posibilidad de los usuarios para acceder a las Tecnologías de la información, de acuerdo a requerimientos funcionales para desempeñar las actividades de los procesos.

Disponibilidad del recurso: Prestación de los medios al usuario para acceder a las Tecnologías de la Información en el momento oportuno y requerido para el desempeño de actividades institucionales.

Prioridad al Acceso: Prestación de los medios al usuario de acuerdo al impacto de los requerimientos y necesidades solicitadas por éstos.

Comunicación: Capacidad de orientar a los usuarios hacia la disponibilidad de herramientas de tecnologías de la información, incluidas en el portafolio de servicios de TI.

6. ELEMENTOS DE LA POLÍTICA

La Política de Acceso a las Tecnologías de Información de SERVICIUDAD E.S.P consta de:

6.1. ASPECTOS GENERALES

La política descrita velará por el adecuado cumplimiento de los siguientes aspectos:

a. **Para el acceso a las TI del usuario interno:** Desarrollo y soporte de una infraestructura tecnológica bajo adecuados estándares de calidad, que permita ofrecer los servicios de la Dirección de la Oficina de TI, que se encuentran en el portafolio para la sostenibilidad de dicha infraestructura. La Dirección de la Oficina de TI, deberá adoptar mecanismos de calidad que estandaricen las iniciativas de incidencias y requerimientos para la mejora continua en la prestación de los servicios de TI en la Entidad.

b. **Educación Y Entrenamiento en accesos:** Periódicamente habrá espacios de formación continua para romper la brecha de resistencia al cambio frente a la utilización de todos los servicios de TI de la Entidad, conforme a lo establecido en la política de Gobierno Digital del Estado colombiano.

6.2. RECURSO HUMANO

La Entidad considera a las personas como usuarios claves para el uso y apropiación de herramientas tecnológicas. Se pueden identificar los siguientes tipos de usuario:

a. **Colaboradores directos e indirectos**, que participan en la ejecución de los servicios de TI en la Entidad.

b. **Clientes y proveedores**, autorizados para el acceso a los recursos de tecnología de la Entidad.

c. **Demás terceros**, autorizados por la Entidad, para acceder a las herramientas tecnológicas

De este modo, los aspectos anteriormente mencionados deberán estar direccionados por:

6.3. CON RELACIÓN AL ACCESO A LAS TECNOLOGÍAS

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a. Todos los usuarios deben tener acceso delimitado a las herramientas tecnológicas requeridas para el desarrollo de las actividades dentro de los procesos asignados.

b. En el caso de personas ajenas a la Entidad, los Subgerentes de área y el Director de la Oficina de TI, son los responsables de autorizar el acceso requerido y delimitado, de acuerdo con el trabajo realizado por estas personas, con previa justificación.

c. Para dar acceso a las herramientas tecnológicas se tendrán en cuenta los roles y funciones de los usuarios al interior de la Entidad.

d. El otorgamiento de acceso a los sistemas de Información está regulado mediante las normas/reglas y procedimientos definidos para tal fin.

e. Todos los privilegios para el uso de los sistemas de información de la Entidad deben terminar inmediatamente después del retiro del colaborados. Por su parte, los Proveedores o terceras personas solamente deben tener el acceso, durante el periodo del tiempo requerido y aprobado para llevar a cabo las labores asignadas.

f. Mediante el registro de eventos de los diversos recursos informáticos integrados en la plataforma tecnológica, se hará disponible la ejecución de un seguimiento de los accesos realizados por los usuarios a los sistemas de información de la Entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información.

g. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información que brindan las herramientas tecnológicas, se deberán documentar y realizar las acciones tendientes a su solución.

6.4. ACCESO AL SERVICIO DE INTERNET Y CUENTAS DE CORREO ELECTRÓNICO.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a. Para hacer uso de este tipo de herramientas se debe gestionar el acceso directamente con la Dirección de la Oficina de TI por escrito y por intermedio de la Subgerencia del área del usuario solicitante.

b. El servicio de Internet y correo electrónico estará disponible únicamente para propósitos institucionales y corporativos concernientes a la Entidad.

c. Está estrictamente prohibido cualquier uso con fines comerciales, políticos, particulares o cualquier otro diferente al laboral que dio origen a la habilitación del servicio.

d. Está prohibido transmitir material que viole la regulación de la Entidad y en general de la República de Colombia; esto incluye: derechos de autor, amenazas, mensajes ofensivos, mensajes en cadena, mensajes intencionales que no contengan información o que contengan basura informática, material obsceno o información protegida por secreto comercial.

e. El usuario de Internet o cuenta de correo no tiene permitido acceder o intentar acceder a la cuenta o a los datos de otros usuarios.

f. Cualquier evidencia de acceso no autorizado a la cuenta o a los datos tiene que ser informada inmediatamente a la Dirección de la Oficina de TI

6.5. GESTIÓN DE ACCESOS Y CONTRASEÑAS

6.5.1. Gestión de Accesos

Al momento del ingreso del nuevo colaborador, la Subgerencia a la cual se encuentra adscrito de manera oficial, envía un correo electrónico a la Dirección de la Oficina de TI con el nombre del usuario, cédula, cargo, rol a desempeñar y requerimientos tecnológicos para ejecutar sus actividades. Con base a la información suministrada el director de la Oficina de TI genera y notifica las credenciales de acceso.

6.5.2. Gestión de Contraseñas

Para la gestión de contraseñas a través del controlador de dominio, se definen los siguientes parámetros:

La contraseña debe cumplir con los siguientes requisitos mínimos:

- No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.
- Tener una longitud mínima de 10 caracteres
- Incluir caracteres de tres de las siguientes categorías:
  - Mayúsculas (de la A a la Z)
  - Minúsculas (de la a a la z)
  - Dígitos de base 10 (del 0 al 9)
  - Caracteres no alfanuméricos (por ejemplo,!, $, #, %)

- Estos requisitos de complejidad se exigen al cambiar o crear contraseñas.

- Longitud mínima de la contraseña **10 caracteres**
  - Esta configuración de seguridad determina el número mínimo de caracteres que debe contener la contraseña de un usuario.

- Vigencia máxima de la contraseña **72 días**
  - Esta configuración de seguridad determina el período de tiempo (en días) en que puede usarse una contraseña antes de que el sistema solicite al usuario que la cambie.

- Vigencia mínima de la contraseña **1 día.**
  - Esta configuración de seguridad determina el período de tiempo (en días) en que puede usarse una contraseña antes de que el usuario pueda cambiarla.

6.5.3. ALMACENAMIENTO DE CONTRASEÑAS

Todas las contraseñas de los sistemas operativos de servidores, servicios de TI, bases de datos y dispositivos de red deberán ser cambiadas en periodos máximo de 72 días o sino el sistema hace un reinicio de contraseñas al día 73.
Cuando un funcionario sale o cambia de rol, el director de la oficina de TI inmediatamente hace los cambios de contraseñas, por ser administrador de los sistemas de información puede restablecer las contraseñas.

6.6. POLÍTICAS DE ACCESO FÍSICO

6.6.1. REPORTE DE PÉRDIDA O ROBO DE IDENTIFICACIÓN

Todo colaborador debe reportar con la mayor brevedad, cualquier sospecha de pérdida o robo de carnets de identificación y tarjetas de acceso físico a las instalaciones.

6.6.2. ORDEN DE SALIDA PARA EQUIPOS ELECTRÓNICOS

Ningún equipo electrónico podrá salir de las instalaciones de SERVICIUDAD E.S.P sin una orden de salida otorgada por el personal adecuado o sin haber sido registrado en el momento de su ingreso.

6.6.3. ORDEN DE SALIDA DE ACTIVOS

Todos los activos que afecten la seguridad de la información de SERVICIUDAD E.S.P como medios de almacenamiento, CDs, DVDs., entre otros, y que necesiten ser retirados de la Entidad, deben presentar autorización diligenciada por medio del formato de Autorización de salida de activos dispuesto para estos casos.

6.6.4. REVOCACIÓN DE PRIVILIGECIOS DE ACCCESO POR TERMINACIÓN LABORAL

Cuando exista una terminación laboral, el usuario deberá devolver los objetos de acceso físico a las instalaciones (carnés, tarjetas de acceso, etc.) y a su vez todos sus privilegios de acceso a las herramientas tecnológicas, esta devolución deberá realizarse al área respectiva y con copia a la Dirección de Oficina de TI.

6.6.5. INGRESO DE EQUIPOS DE GRABACIÓN Y FOTOGRAFÍAS AL CUARTO DE SERVIDORES.

Cualquier miembro de SERVICIUDAD E.S.P y/o tercero debe estar autorizado por el área de seguridad de la información para ingresar con equipos donde puedan obtener información, estos pueden ser (video cámaras, celulares, cámaras fotográficas etc.).

6.7. POLÍTICAS DE ACCESO REMOTO

a. Los Usuarios que requieran acceder de manera remota a sistemas de información y recursos informáticos de la Entidad, deberán solicitar el permiso de trabajo desde casa por medio del formato de teletrabajo, aprobado y firmado por el jefe de área al cual pertenece el usuario solicitante. Con base a este formato, el director de la Oficina de TI Instala la VPN como método de conexión para garantizar el acceso requerido.

b. En La modalidad de trabajo en casa como método de acceso remoto a componentes tecnológicos de la Entidad, el usuario debe hacer uso de su propio recurso informático para conectarse y desarrollar sus actividades, la Entidad brinda garantías de conexión al escritorio remoto, por medio de la instalación de la VPN con el fin de que el usuario pueda acceder al equipo directamente.

7. RESPONSABLE

Los responsables de velar por el cumplimiento de la Política de Acceso a las Tecnologías de la Información son el director de la Oficina de TI y Control Interno, los cuales tendrán las siguientes responsabilidades:

- Realizar procesos de socialización y sensibilización a los colaboradores de la Entidad, sobre la importancia de cumplir con los parámetros de acceso a la Tecnologías de la Información en aras de velar por la seguridad de la información de la Entidad.
- Realizar planes de mejora a partir de los hallazgos identificados y registrados en procesos de auditoría, con respecto al acceso por parte de los usuarios a las Tecnologías de la Información.
- Realizar las debidas sanciones disciplinarias de acuerdo al acceso inadecuado a las Tecnologías de la Información.

8. SANCIONES POR INCUMPLIMIENTO DE LA POLÍTICA

a. Cuando se trate de una falta que afecte directamente el normal funcionamiento del recurso tecnológico por acceso inadecuado o infrinja leyes del ámbito jurídico, se aplicarán también todas las normas vigentes, informando por escrito al Área del usuario infractor y la Oficina de control interno Disciplinario para tomar las medidas y sanciones correspondientes.

b. Cuando por consecuencia de una violación de las normas se suspenda el acceso de las herramientas tecnológicas a un usuario, para reactivar los servicios la Subgerencia de área del usuario infractor, debe solicitar por escrito el levantamiento del acceso ante la Dirección de la Oficina de TI, con validación previa de la Oficina de Control Interno.

c. La reincidencia de una falta SIMPLE la convierte en GRAVE.

CONSIDERACIONES FINALES

Por todo lo anterior, se solicita la gestión de todos los colaboradores de SERVICIUDAD E.S.P para conservar un ambiente seguro en los sistemas de información y recursos informáticos de la Entidad, informando de cualquier irregularidad observada en los procesos que se lleve en los sistemas de información o el acceso de los recursos informáticos.