CONTROL VERSIÓN

ELABORÓ	REVISÓ	APROBÓ
Samuel Córdoba **CISO**	Johely López A. **Gerente Administrativa y Financiera**	Pedro Pabón **Gerente General**
VERSIÓN	1.0	
ACTUALIZACIÒN	Creación del documento	

1. OBJETIVO GENERAL

La política de control de acceso tiene como propósito asegurar que solo usuarios, sistemas o procesos puedan acceder a la información y otros activos asociados, garantizando la confidencialidad, integridad y disponibilidad de los de los activos de información, mediante controles preventivos y medidas de ciberseguridad, adecuándolos a los requisitos comerciales y las normativas vigentes.

2. ALCANCE

Esta política se aplica a todos los empleados, contratistas, terceros y cualquier otra entidad que requiera acceso a los activos de información y sistemas de la organización.

3. PRINCIPIO DE NECESIDAD DE SABER

Mediante este principio se establece que una persona, sistema o proceso solo debe tener acceso a la información que necesita específicamente para desempeñar sus funciones o cumplir con sus responsabilidades.

El acceso a la información se limitará únicamente a aquella que sea estrictamente necesaria para que un usuario realice las funciones que le han sido asignadas.

Los permisos de acceso serán asignados en función de los roles y responsabilidades específicas de cada usuario, de acuerdo con la descripción de su puesto o contrato de trabajo. Cada acceso será revisado periódicamente para asegurarse de que los permisos concedidos siguen siendo adecuados y necesarios para las funciones actuales del usuario.

4. PRINCIPIO DE PRIVILEGIO MÍNIMO

Cada usuario, sistema o proceso debe tener únicamente los permisos mínimos necesarios para realizar sus tareas. Todo acceso estará generalmente prohibido por defecto, excepto cuando se haya otorgado expresamente mediante un proceso de solicitud y autorización formal.

En caso de acceso temporal para tareas específicas, este será habilitado únicamente por el tiempo necesario y deshabilitado inmediatamente después.

Los permisos de acceso serán revisados regularmente, para asegurar que se mantengan alineados con las funciones operativas de loa usuario. Cualquier cambio de función o rol dentro de la organización requerirá una revisión y ajuste de los permisos.

5. DIRECTRICES DE CONTROL DE ACCESO

Control de acceso a la informacion

El acceso se realiza de acuerdo a los niveles de clasificación de confidencialidad del activo de información. Estos niveles, junto con los roles y permisos asignados a los usuarios o entidades que solicitan el acceso, determinan quién puede acceder a qué información, en qué circunstancias y con qué tipo de acciones permitidas (como lectura, escritura, modificación o eliminación). Este proceso garantiza que solo el personal autorizado tenga acceso a la información estrictamente necesaria para el desempeño de sus funciones, aplicando el principio de mínimo privilegio para proteger la confidencialidad, integridad y disponibilidad de los datos.

5.1. Control de acceso para Servicios en la nube

- Los activos de información de tipo servicio en la nube son: AWS, Azure DevOps, Microsoft 365, SharePoint, Siigo, GLPI, HubSpot, AWS S3.
- La Organización debe establecer control de acceso basado en roles (RBAC) que permita implementar roles y permisos para usuarios, según su función dentro de la organización.
- Requerir autenticación de dos factores para acceder a los servicios en la nube, de acuerdo con los activos de información que lo permiten.
- Asegurarse de que los datos en reposo y en tránsito que lo requieran estén cifrados.
- Revisar y auditar los accesos de los usuarios regularmente para asegurar que solo los usuarios autorizados tengan acceso.
- Configurar el registro de eventos de acceso y el monitoreo de actividad sospechosa o anómala.
- Garantizar que se cumplan las políticas de uso aceptable que se definan para estos activos, cómo se deben usar estos servicios y los datos que contienen.

5.2. Control de acceso en Sharepoint

Solo los usuarios autorizados podrán acceder a los datos y funcionalidades de SharePoint mediante autenticación segura, alineada con los roles y permisos definidos según sus responsabilidades laborales. Se implementan medidas de control, como autenticación multifactor y acceso por grupos determinados para garantizar la información se pueda visualizar, editar o gestionar, por personas autorizadas.

5.3. Control de acceso para Herramientas de desarrollo

- Los activos de información de tipo herramientas para el desarrollo son: GitHub, SonarQube, IDEs (Entornos de Desarrollo), aplicaciones de software.
- Establecer permisos granulares en repositorios para controlar quién puede ver, modificar o aprobar cambios.
- Configurar autenticación multifactor y usar tokens o claves SSH para GitHub.
- Mantener entornos de desarrollo, pruebas y producción separados, con diferentes niveles de acceso.
- Controlar el acceso a los entornos de desarrollo y a las aplicaciones de software mediante políticas de seguridad específicas y autenticación centralizada.

5.4. Control de acceso a Redes sociales y mensajería

- Los activos de información de este tipo son WhatsApp Business y redes sociales
- Confirmar las personas y áreas que tienen permitido de WhatsApp Business y redes sociales corporativas.
- Se debe limitar el acceso a cuentas de redes sociales y WhatsApp Business a personas no autorizadas.
- Se debe activar autenticación multifactor si es posible.
- Monitorear el uso de redes sociales para identificar actividades que puedan comprometer la seguridad de la información.
- Asegurar que las comunicaciones en WhatsApp Business estén cifradas de extremo a extremo.

5.5. Herramientas de seguridad

- En esta categoría están los activos de información como LastPass o KeePass Password Safe.
- Configurar políticas en los activos de información para la generación, almacenamiento y uso de contraseñas seguras.
- Asegurar que todos los usuarios utilicen **Autenticación Multifactor (MFA)** para acceder a LastPass.
- Revisar regularmente los accesos y las contraseñas compartidas para garantizar que solo personas autorizadas puedan acceder.
- Establecer políticas de rotación y caducidad de contraseñas, así como evitar el uso de contraseñas repetidas.

6. VIGENCIA

Esta Política es aplicable para todos los funcionarios, contratistas y terceros, a partir de momento de su publicación, será revisada anualmente y actualizada según corresponda y comunicada por los medios establecidos por la Organización a todos los trabajadores y partes interesadas.

7. CONSECUENCIA DE INCUMPLIMIENTO

Cualquier violación o incumplimiento a la presente política es calificada como grave y constituye justa causa para dar por terminado el contrato laboral o contractual vigente.

PEDRO ELÍAS PABÓN LOZANO
Gerente General