1. OBJETIVO

Definir las directrices para:

a) asegurar el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados;

b) permitir la identificación única de individuos y sistemas que acceden a la información de la Universidad y otros activos asociados y permitir la asignación adecuada de derechos de acceso;

c) asegurar la autenticación de entidades correcta y evitar errores en los procesos de autenticación;

d) asegurar que solo los usuarios autorizados, los componentes de software y los servicios se proporcionen con derechos de acceso con privilegios;

e) asegurar que el acceso a la información y otros activos asociados se defina y autorice de acuerdo con los requisitos de negocio;

f) evitar la introducción de funciones no autorizadas, los cambios no intencionados o malintencionados y mantener la confidencialidad de la propiedad intelectual;

g) asegurar que un usuario o una entidad se autentique de forma segura cuando se conceda acceso a sistemas, aplicaciones y servicios.

2. ALCANCE

Las presentes directrices aplican a todos los funcionarios administrativos, docentes, estudiantes (pasantes, judicantes, practicantes), contratistas y/o terceros de la Universidad Surcolombiana.

3. DEFINICIONES

Los términos y definiciones aplicables para esta guía son los establecidos en la norma NTC ISO IEC 27000.

Propietario del activo de Información: persona (cargo) o grupo de trabajo designado por la Entidad que tiene la responsabilidad de determinar los controles y

acciones para asegurar la confidencialidad, integridad y disponibilidad a la información y otros activos asociados, teniendo en cuenta la política y directrices de seguridad y privacidad de la información aplicables relacionadas

Entidad: puede representar a un usuario humano, así como a un elemento técnico o lógico (por ejemplo, una máquina, un dispositivo o un servicio)

MAC: control de acceso obligatorio.

DAC: control de acceso discrecional.

RBAC: control de acceso basado en roles.

Contraseñas o frases de acceso: son un tipo de información de autenticación que se utiliza habitualmente y son un medio común de verificar la identidad de un usuario. Otros tipos de información de autenticación son las claves cifradas, los datos almacenados en tokens de hardware (tarjetas inteligentes) que producen códigos de autenticación y datos biométricos, como escaneos de iris o huellas dactilares.

Derechos de acceso con privilegios: son derechos de acceso proporcionados a una identidad, una función o un proceso que permite realizar actividades que los usuarios o procesos típicos no pueden realizar.

4. MARCO DE REFERENCIA

La gestión de riesgos y oportunidades en la Universidad Surcolombiana considera para su labor, los lineamientos definidos en las directrices y políticas institucionales, además de las consideraciones definidas en:

- La norma ISO 31000:2018– Gestión del riesgo. Principios y directrices.
- La norma ISO IEC 27005:2022 – Gestión de riesgos para la seguridad de la información.
- Los lineamientos definidos en los documentos del Sistema de Gestión de Seguridad y Privacidad de la Información.
- Los requisitos aplicables a la gestión del riesgo, detallados en el estándar ISO IEC 27001:2022 y la ISO IEC 27701:2025
- Código de Práctica para Controles de Seguridad de la Información - GTC ISO IEC 27002:2022 Tecnología de la Información. Técnicas de Seguridad.

- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- Guía de Administración de riesgos y el diseño de controles en entidades públicas
- CONPES de Seguridad Digital (CONPES 3854 de 2016 y actualizaciones)
- Modelo de Seguridad y Privacidad de la Información – MSPI (MinTIC)
- Política de Gobierno Digital (Decreto 1078 de 2015 y actualizaciones)
- Modelo Integrado de Planeación y Gestión – MIPG (DAFP)
- FURAG (Formulario Único de Reporte de Avance de la Gestión)
- Ley 1581 de 2012 y Decreto 1377 de 2013
- Lineamientos y guías de la Superintendencia de Industria y Comercio.

5. GENERALIDADES

Estas directrices son la declaración general que establece la Universidad para asignar accesos a la información, información de identificación personal -IIP- y demás activos asociados a su tratamiento y protección, con base en los siguientes controles de acuerdo a las normas:

ISO/IEC 27001:2022

A.5.15 Control de acceso
A.5.16 Gestión de identidad
A.5.17 Información de autentificación
A.5.18 Derechos de acceso
A.8.2 Derechos de accesos privilegiados
A.8.3 Restricción del acceso a la información
A.8.4 Acceso al código fuente
A.8.5 Autenticación de seguridad

ISO/IEC 27701:2025

A.3.8 Gestión de identidades
A.3.9 Derechos de acceso

6. DIRECTRICES

6.1 CONTROL DE ACCESO

Los propietarios de la información y otros activos asociados deben determinar la seguridad de la información y los requisitos institucionales relacionados con el control de acceso.

Estos requisitos y la directriz específica del tema deben considerar lo siguiente:

a) determinar qué entidad requiere qué tipo de acceso a la información y otros activos asociados;

b) seguridad de las aplicaciones;

c) el acceso físico, que debe estar soportado por los controles de entrada apropiados;

d) difusión y autorización de la información (el principio de necesidad de conocer) y niveles de seguridad de la información y clasificación de la información;

e) restricciones al acceso privilegiado;

f) segregación de tareas;

g) la legislación, los reglamentos y las obligaciones contractuales pertinentes relativas a la limitación del acceso a datos o servicios;

h) segregación de las funciones de control de acceso (solicitud de acceso, autorización y administración de acceso);

i) autorización formal de solicitudes de acceso;

j) la gestión de los derechos de acceso;

k) registro

Las reglas de control de acceso deben implementarse definiendo los derechos y restricciones de acceso apropiados a las entidades. Para simplificar la gestión del control de acceso, se pueden asignar roles específicos a los grupos de entidades.

Al definir e implementar las reglas de control de acceso, se debe tener en cuenta lo siguiente:

a) coherencia entre los derechos de acceso y la clasificación de la información;

b) coherencia entre los derechos de acceso y las necesidades y requisitos de seguridad del perímetro físico;

c) considerar todos los tipos de conexiones disponibles en los entornos distribuidos, para que las entidades solo tengan acceso a la información y otros activos asociados, incluidos los servicios de red que estén autorizados.

Los principios generales en el contexto del control de acceso más utilizados son:

a) necesidad de saber: a una entidad solo se le concede acceso a la información que requiere para realizar sus tareas (diferentes tareas o funciones significan una información diferente de necesidad de saber y, por lo tanto, diferentes perfiles de acceso);

b) necesidad de uso: a una entidad solo se le asigna acceso a la infraestructura de tecnología de la información cuando existe una necesidad clara.

Al definir las reglas de control de acceso se debe tener en cuenta:

a) establecer reglas basadas en la premisa del menor privilegio, "todo está generalmente prohibido a menos que esté expresamente permitido", en lugar de la regla más débil, "todo está generalmente permitido a menos que esté expresamente prohibido";

b) los cambios en las etiquetas de información que se inician automáticamente mediante las instalaciones de procesamiento de información y los iniciados a discreción del usuario;

c) los cambios en los permisos de usuario se realizan automáticamente por el sistema de información y los permisos especiales verificados por un administrador;

Las reglas de control de acceso deben estar respaldadas por procedimientos documentados y la definición de responsabilidades.

6.2 GESTIÓN DE IDENTIDAD

Los procesos utilizados en el contexto de la gestión de identidades deben asegurar

que:

a) las identidades asignadas a personas, permiten responsabilizarlas de las acciones realizadas con esta identidad específica;

b) las identidades asignadas a varias personas (por ejemplo, identidades compartidas) solo se permiten cuando son necesarias por motivos operativos y están sujetas a aprobación y documentación específicas;

c) las identidades asignadas a entidades no humanas están sujetas a una aprobación debidamente segregada y a una supervisión independiente continua;

d) las identidades se desactivan o eliminan de forma oportuna si ya no son necesarias, si sus entidades asociadas se eliminan o ya no se utilizan o si la persona vinculada a una identidad ha abandonado la organización o ha cambiado el rol;

e) en un dominio específico, se debe evitar la asignación de varias identidades a una sola entidad;

f) se mantienen registros de todos los eventos significativos relacionados con el uso y la gestión de las identidades de usuario y de la información de autenticación.

La Universidad cuenta con los procedimientos AP-TIC-PR-09 USUARIOS Y CUENTAS DE CORREO ELECTRÓNICO y AP-TIC-PR-10 CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN, APLICACIONES Y SERVICIOS para la gestión de administración de usuarios.

Las directrices para la creación de identidades asignadas a personas se definen en la AP-TIC-DR-XX DIRECTRICES PARA EL USO ADECUADO DE CUENTA DE USUARIO Y DE CORREO ELECTRÓNICO INSTITUCIONAL.

Cabe anotar que se requiere vinculación contractual activa para que este procedimiento se lleve a cabo. Para los casos excepcionales se debe llevar a cabo los procedimientos AP-TIC-PR-09 USUARIOS Y CUENTAS DE CORREO ELECTRÓNICO y AP-TIC-PR-10 CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN, APLICACIONES Y SERVICIOS, teniendo en cuenta:

a) confirmar los requisitos institucionales para establecer una identidad;

b) verificar la identidad y el estado de vinculación de una entidad antes de asignarle una identidad lógica;

c) establecer, configurar y activar la identidad

d) proporcionar o revocar derechos de acceso específicos a la identidad, sobre la base de las decisiones de autorización o derecho apropiadas

6.3 INFORMACIÓN DE AUTENTICACIÓN

6.3.1 Asignación de información de autenticación

El proceso de asignación y gestión debe asegurar que:

a) las contraseñas personales o los números de identificación personal generados automáticamente durante los procesos de autenticación secreta temporal, son únicas para cada persona y los usuarios deben cambiarlos después del primer uso;

b) se establecen procedimientos para verificar la identidad de un usuario antes de proporcionar información de autenticación, de sustitución o temporal

c) la información de autenticación, incluida la información de autenticación temporal, se transmite a los usuarios de forma segura a través de correo electrónico;

d) la información de autenticación predeterminada, predefinida o proporcionada por los proveedores se cambia inmediatamente después de la instalación de sistemas o software;

e) se mantienen registros de eventos de asignación y gestión de la información de autenticación, se otorga confidencialidad y se aprueba el método de mantenimiento de registros.

6.3.2 Responsabilidades del usuario

Cualquier persona que tenga acceso o utilice la información de autenticación debe asegurarse de que:

a) la información de autenticación secreta, como las contraseñas, se mantiene confidencial, no debe compartirse con nadie y la información de autenticación secreta utilizada en el contexto de identidades vinculadas a varios usuarios o vinculadas a entidades no personales, se comparte únicamente con personas autorizadas;

b) la información de autenticación afectada o comprometida se cambia inmediatamente tras la notificación o cualquier otra indicación de un compromiso;

c) cuando se utilizan contraseñas como información de autenticación, se seleccionan contraseñas seguras según buenas prácticas recomendadas, por ejemplo:

   1) las contraseñas no se basan en algo que otra persona pueda adivinar u obtener fácilmente al utilizar información relacionada con la persona (por ejemplo, nombres, números de teléfono, fechas de nacimiento, entre otros);

   2) las contraseñas no se basan en palabras de diccionario o sus combinaciones;

   3) utilizar frases de contraseña fáciles de recordar e incluir caracteres alfanuméricos y especiales;

   4) las contraseñas tienen una longitud mínima;

d) las mismas contraseñas no se utilizan en distintos servicios y sistemas;

6.3.3 Sistema de gestión de contraseñas

Cuando se utilizan contraseñas como información de autenticación, el sistema de gestión de contraseñas debe:

a) permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para solucionar los errores de entrada;

b) aplicar contraseñas seguras de acuerdo con las recomendaciones de buenas prácticas;

c) forzar a los usuarios a cambiar sus contraseñas en el primer inicio de sesión;

d) aplicar los cambios de contraseña según sea necesario, por ejemplo, después de un incidente de seguridad o cambio de funciones u obligaciones;

e) no mostrar contraseñas en la pantalla al introducirlas;

f) almacenar y transmitir contraseñas en forma protegida.

El cifrado de contraseñas y el hash deben realizarse de acuerdo con las técnicas cifradas aprobadas para contraseñas.

6.4 DERECHOS DE ACCESO

6.4.1 Provisión y revocación de derechos de acceso

El proceso de aprovisionamiento para asignar o revocar derechos de acceso físicos y lógicos otorgados a la identidad autenticada debe incluir:

a) obtención de la autorización del propietario de la información y otros activos asociados para el uso de la información y otros activos asociados;

b) consideración de los requisitos de la Institución, la política, directrices y las reglas específicas sobre el control de acceso;

c) asegurar que se eliminan los derechos de acceso cuando alguien no necesita acceder a la información y a otros activos asociados, en particular garantizando que los derechos de acceso de los usuarios que se han desvinculado se inactiven de forma oportuna; ver AP-TIC-DR-XX DIRECTRICES PARA EL USO ADECUADO DE CUENTA DE USUARIO Y DE CORREO ELECTRÓNICO INSTITUCIONAL

d) verificar que el nivel de acceso concedido se ajuste a las directrices específicas del tema sobre control de acceso y sea coherente con otros requisitos de seguridad de la información, como la separación de funciones;

e) asegurar que los derechos de acceso se activen solo después de que los procedimientos de autorización se hayan completado correctamente;

f) mantener un registro de accesos otorgados a un identificador de usuario para acceder a la información y otros activos asociados;

g) modificar los derechos de acceso de los usuarios que han cambiado de roles o funciones;

h) eliminar o ajustar los derechos de acceso físicos y lógicos, que se pueden realizar mediante la eliminación, revocación o sustitución de claves, información de autenticación o tarjetas de identificación;

i) mantener un registro de los cambios en los derechos de acceso lógicos y físicos de los usuarios.

El usuario de los aplicativos institucionales de los funcionarios y/o contratistas será inactivado al finalizar el día de terminación del contrato o desvinculación de la Institución, ver AP-TIC-DR-XX DIRECTRICES PARA EL USO ADECUADO DE CUENTA DE USUARIO Y DE CORREO ELECTRÓNICO INSTITUCIONAL.

6.4.2 Revisión de los derechos de acceso

En las revisiones periódicas de los derechos de acceso físicos y lógicos se debe tener en cuenta lo siguiente:

a) los derechos de acceso de los usuarios después de cualquier cambio en la Institución (cambio de funciones, ascenso, descenso) o terminación del vínculo laboral y/o contractual;

b) autorizaciones para derechos de acceso con privilegios.

6.4.3. Consideración antes del cambio de funciones o terminación del vínculo laboral

Los derechos de acceso de un usuario a la información y otros activos asociados deben revisarse, ajustarse y/o eliminarse antes de cualquier cambio o cese del empleo basándose en la evaluación de factores de riesgo como:

a) si la terminación o el cambio es iniciado por el usuario o por la dirección y el motivo de la terminación;

b) las responsabilidades actuales del usuario;

c) el valor de los activos actualmente accesibles.

Se debe considerar la inclusión de cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal intenta acceder sin autorización.

6.5 DERECHOS DE ACCESO PRIVILEGIADO

En la asignación de derechos de acceso privilegiado se debe considerar lo siguiente:

a) identificar a los usuarios que necesitan derechos de acceso con privilegios para cada sistema o proceso;

b) asignación de derechos de acceso con privilegios a los usuarios según sea necesario y evento por evento, de acuerdo con la directriz de control de acceso específica de cada tema;

c) mantener un proceso de autorización y un registro de todos los privilegios asignados;

d) definir e implementar los requisitos para la expiración de los derechos de acceso privilegiado;

e) tomar medidas para asegurar que los usuarios conozcan sus derechos de acceso privilegiado

f) los requisitos de autenticación para los derechos de acceso con privilegios son superiores a los requisitos para los derechos de acceso normales (segunda contraseña);

g) establecer reglas específicas para evitar el uso de ID de usuario de administración genéricos (como “root”), dependiendo de las capacidades de configuración de los sistemas. Administrar y proteger la información de autenticación de dichas identidades;

h) conceder acceso temporal con privilegios solo durante el período de tiempo necesario para implementar cambios o actividades aprobadas (actividades de mantenimiento o algunos cambios críticos a través de una ventana de mantenimiento), en lugar de conceder derechos de acceso con privilegios de forma permanente;

i) registrar todo acceso privilegiado a los sistemas con fines de auditoría;

j) no compartir o vincular identidades con derechos de acceso con privilegios a varias personas, asignando a cada persona una identidad independiente que permita asignar derechos de acceso con privilegios específicos. Las identidades se pueden agrupar para simplificar la gestión de los derechos de acceso con privilegios;

Las funciones de administrador del sistema normalmente requieren derechos de acceso con privilegios. El uso inapropiado de los privilegios del administrador del sistema es un riesgo y un factor importante que contribuye a las fallas o incumplimiento de los sistemas.

6.6 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN

El acceso a la información y a otros activos asociados, debe restringirse de conformidad con las directrices establecidas sobre temas específicos. Se debe tener en cuenta los siguientes requisitos de restricción de acceso:

a) no permitir el acceso a información confidencial por identidades de usuario desconocidas o anónimas.

b) el acceso público o anónimo solo debe concederse a ubicaciones de almacenamiento que no contengan información confidencial;

c) proporcionar mecanismos de configuración para controlar el acceso a la información en sistemas, aplicaciones y servicios;

d) controlar a qué datos puede acceder un usuario concreto;

e) controlar qué identidades o grupos de identidades tienen acceso, como lectura, escritura, eliminación y ejecución;

f) proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones, datos de aplicaciones o sistemas confidenciales.

Las técnicas y procesos de gestión de acceso dinámico para proteger la información confidencial que tiene un alto valor para la Universidad deben considerarse cuando:

a) necesita un control detallado sobre quién puede acceder a dicha información durante qué período y de qué manera;

b) desea compartir dicha información con personas ajenas a la Institución y mantener el control sobre quién puede acceder a ella;

c) desea gestionar dinámicamente, en tiempo real, el uso y la distribución de dicha información;

d) desea proteger dicha información contra cambios, copias y distribución no autorizados;

e) quiere controlar el uso de la información;

Las técnicas de gestión dinámica de acceso deben proteger la información a lo largo de su ciclo de vida (es decir, creación, procesamiento, almacenamiento, transmisión y eliminación), incluyendo:

a) establecer reglas sobre la gestión del acceso dinámico basadas en casos de uso específicos considerando:

1) conceder permisos de acceso basados en la identidad, el dispositivo, la ubicación o la aplicación;

2) aprovechar el esquema de clasificación (ver ES-GSPI-MR-04 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN DOCUMENTAL, ES-GSPI-MR-05 MATRIZ DE INVENTARIO Y CLASIFICACION DE ACTIVOS DE LA INFORMACIÓN) para determinar qué información necesita protegerse con técnicas de gestión de acceso dinámico;

Los sistemas de gestión de acceso dinámico deben proteger la información mediante:

a) solicitud de autenticación, credenciales adecuadas o un certificado para acceder a la información;

b) restricción del acceso a un plazo de tiempo especificado (después de una fecha determinada o hasta una fecha determinada);

c) uso del cifrado para proteger la información;

d) registro de quién accede a la información;

6.7 ACCESO AL CÓDIGO FUENTE

El acceso al código fuente, a los elementos asociados y a las herramientas de desarrollo debe controlarse rigurosamente. Para el código fuente, esto se puede lograr al controlar el almacenamiento central de dicho código, preferiblemente en el sistema de gestión del código fuente.

Se deben considerar las siguientes directrices para controlar el acceso a las bibliotecas de los códigos fuente a fin de reducir el riesgo de modificación o alteración de los programas informáticos, ver GUIA BUENAS PRÁCTICAS PARA EL MANEJO DE REPOSITORIO Y VERSIONAMIENTO EN GITHUB:

a) administrar el acceso al código fuente del programa y a las bibliotecas de origen del programa según los procedimientos establecidos;

b) conceder acceso de lectura y escritura al código fuente en función de las necesidades de la Institución y gestionar para abordar los riesgos de alteración o uso indebido, de acuerdo con los procedimientos establecidos;

c) actualizar el código fuente y los elementos asociados y conceder acceso al mismo de acuerdo con el procedimiento, procedimientos de control de cambios y realizarlo solo después de recibir la autorización adecuada;

d) no conceder a los desarrolladores acceso directo al repositorio de código fuente, sino a través de herramientas de desarrollo que controlen las actividades y autorizaciones en el código fuente;

e) mantener listas de programas en un entorno seguro, donde el acceso de lectura y escritura debe gestionarse y asignarse de forma adecuada;

f) mantener un registro de todos los accesos y de todos los cambios realizados en el código fuente.

6.8 AUTENTICACIÓN DE SEGURIDAD

La solidez de la autenticación debe ser adecuada para la clasificación de la información a la que se va a acceder. Cuando se requiere autenticación y verificación de identidad sólidas, se utilizan métodos de autenticación alternativos a las contraseñas, como certificados digitales, tarjetas inteligentes, tokens o medios biométricos.

El procedimiento para iniciar sesión en un sistema o aplicación debe diseñarse para minimizar el riesgo de acceso no autorizado, considerando lo siguiente:

a) no mostrar información confidencial del sistema o de la aplicación hasta que el proceso de inicio de sesión se haya completado correctamente para evitar que un usuario no autorizado reciba asistencia innecesaria;

b) validar la información de inicio de sesión solo cuando se completen todos los datos de entrada;

c) protección contra intentos de inicio de sesión forzada en nombres de usuario y contraseñas después de un número predefinido de intentos fallidos o que bloquee al usuario después de un número máximo de errores

d) provocar un evento de seguridad si se detecta un posible intento o incumplimiento de los controles de inicio de sesión (enviar una alerta al usuario y a los administradores del sistema cuando se ha alcanzado un número determinado de intentos de contraseña incorrectos);

e) visualización o envío de la siguiente información al finalizar un inicio de sesión correcto:

1) fecha y hora del inicio de sesión anterior correcto;

2) detalles de cualquier intento de inicio de sesión incorrecto desde el último inicio de sesión correcto;

f) no mostrar una contraseña en texto no cifrado al introducirla

g) no transmitir contraseñas en texto no cifrado a través de una red para

evitar ser capturadas por un programa de rastreador de red;

h) finalizar sesiones inactivas después de un período definido de inactividad

i) restringir los tiempos de duración de la conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo y reducir la oportunidad de acceso no autorizado.

7. RESPONSABILIDADES Y AUTORIDADES

Los funcionarios administrativos, docentes, estudiantes, pasantes, judicantes, contratistas y/o terceros deben cumplir con la política y directrices de seguridad y privacidad de la información definidas por la Universidad Surcolombiana; así mismo, deben reportar a los propietarios de la información y otros activos asociados las violaciones a la política, directrices y/o cualquier inconsistencia o irregularidad que pueda ser generada por los usuarios.

Los líderes de procesos y propietarios de la información y otros activos de la información deben revisar periódicamente los riesgos que se identifiquen sobre el uso inadecuado de los activos.

8. DOCUMENTOS RELACIONADOS Y REGISTROS

AP-TIC-DR-02 DIRECTRICES PARA EL USO ADECUADO DE CUENTA DE USUARIO Y DE CORREO ELECTRÓNICO INSTITUCIONAL
AP-THU-DR-01 DIRECTRICES PARA EL CONTROL DE PERSONAS
AP-THU-DA-03 ROLES, RESPONSABILIDADES Y AUTORIDADES DE LA INSTITUCIÓN.
AP-TIC-PR-09 USUARIOS Y CUENTAS DE CORREO ELECTRÓNICO
AP-TIC-PR-10 CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN, APLICACIONES Y SERVICIOS
ES-GSPI-MR-04 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN DOCUMENTAL
ES-GSPI-MR-05 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN
GUÍA BUENAS PRÁCTICAS PARA EL MANEJO DE REPOSITORIO Y VERSIONAMIENTO EN GITHUB
GUÍA CONFIGURACIÓN DE ACCESO POR VPN CLIENT TO SITE

CONTROL DE CAMBIO		
VERSIÓN	DOCUMENTO Y FECHA DE APROBACIÓN	DESCRIPCION DE CAMBIO
01	EV-CAL-FO-17 del 1 de septiembre de 2026	Creación documento

ELABORÓ	REVISÓ	APROBÓ
MARTHA LILIANA HERMOSA TRUJILLO Gestión Seguridad y Privacidad de la Información **Elaboró** DIEGO ANDRES CARVAJAL RUIZ Director Centro de Tecnología Información y Control Documental **Aprobó**	ALVARO TORRENTE LÓPEZ Profesional de apoyo SGC	MAYRA ALEJANDRA BERMEO BALAGUERA Coordinador SGC