

	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

1. POLITICA

Esta Política de Seguridad de la Información tiene como propósito establecer los principios, directrices y controles necesarios para proteger la **confidencialidad, integridad y disponibilidad** de la información y los activos informáticos de la empresa. El alcance de esta política abarca a todo el personal, proveedores, contratistas y terceros que tengan acceso a los sistemas y datos de la empresa, así como a todos los equipos, software y redes.

1.1 MARCO NORMATIVO

9ONCE SEGURIDAD LTDA basa sus directrices de seguridad de la información en cumplimiento con el siguiente marco normativo colombiano e internacional aplicable:

- **Ley Estatutaria 1581 de 2012:** Por la cual se dictan disposiciones generales para la **protección de datos personales** y se regula el "hábeas data".
- **Decreto Reglamentario 1377 de 2013:** El cual reglamenta la Ley 1581 de 2012 y establece los procedimientos para el tratamiento de datos personales, incluyendo la necesidad de tener una política de tratamiento de la información.
- **NTC-ISO 27001:** Norma técnica colombiana que adopta la ISO/IEC 27001, estableciendo los requisitos para un **Sistema de Gestión de la Seguridad de la Información (SGSI)**. Su implementación ayuda a gestionar los riesgos de seguridad y garantizar la confidencialidad, integridad y disponibilidad de la información.
- **BASC V6.02 (o versiones posteriores):** Enfoque en la gestión de riesgos para la seguridad en la cadena de suministro y la prevención de actividades ilícitas. Su implementación fortalece la seguridad física y de la información, especialmente en empresas con operaciones logísticas o de comercio exterior.

1.2. OBLIGACIONES DE LOS USUARIOS

Todos los empleados de la empresa 9 -Once Seguridad Ltda., que debido a sus funciones debe manipular y utilizar equipos y servicios tecnológicos, independiente de su jerarquía dentro de la empresa, deben firmar formato donde acepte, condiciones de confidencialidad y manejo de información digital generada en sus funciones, el manejo adecuado de los recursos informáticos de 9 Once Seguridad Ltda., así como el apego a las normas y políticas.

	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

Es responsabilidad de los usuarios de equipos y servicios tecnológicos de 9 Once Seguridad Ltda., cumplir las políticas de seguridad informática.

1.3. ENTRENAMIENTO Y CAPACITACION

Parte de los objetivos de las políticas de información, es la presentación de fácil entendimiento para todo el personal, por medio de capacitaciones personalizadas para la sensibilización del personal.

Estas deben incorporar en entrenamiento sobre amenazas de ciberseguridad, Malware y otro tipo de amenazas que ponga en riesgo la seguridad del entorno de 9once seguridad.

1.3. POLITICAS Y NORMAS DE SEGURIDAD FISICA Y AMBIENTAL

1.3.1. POLITICA

Los mecanismos de control de acceso físico deben asegurar que las áreas restringidas de la compañía 9 Once Seguridad Ltda., den acceso solamente a personal autorizado para salvaguardar la seguridad de los equipos e información de la compañía.

1.3.2. MANEJO DE LA INFORMACION

Todos los usuarios deberán reportar de forma inmediata los riesgos reales y potenciales que presenten en el área física en que desempeñan sus funciones, para los equipos de cómputo o de comunicación que hacen uso, como por ejemplo fugas de agua, conato de incendio, cortos eléctricos etc.

Todos los medios de almacenamiento de información de tipo extraíble (pen drive o USB, CD, DVD, discos extraíbles) asignados por la compañía 9 Once Seguridad Ltda., en función de las tareas del usuario son responsabilidad de este, junto con información contenida en los mismos, aun cuando no se utilicen.

La información almacenada en los ordenadores asignados a los funcionarios de la compañía 9 Once Seguridad Ltda., son responsabilidad de estos, el evitar fugas o perdidas de información dentro de los equipos es obligación del usuario.

 <p>Sistema Integrado de Gestión</p>	<p>POLITICA SEGURIDAD DE LA INFORMACIÓN</p>	<p>01-E-06</p>
		<p>FECHA: 14-10-2026</p>
		<p>V. 4</p>

1.3.3. CONTROL DE INGRESO DE EQUIPO

Cualquier persona que acceda a la compañía 9 Once Seguridad Ltda., deberá registrar al momento de su ingreso: equipos de cómputo, equipos de comunicaciones (exceptuando teléfonos móviles o celulares) y herramientas que no sean propiedad de 9 Once Seguridad Ltda., de manera que se mantenga control sobre el tráfico de los equipos computacionales y de computación que entran y salen de la compañía.

Las computadoras personales o portátiles asignados o cualquier otro activo de comunicación e información podrán salir de la compañía 9 Once Seguridad Ltda., previa autorización de la autoridad respectiva.

1.3.4. TRASLADO, PROTECCIÓN Y UBICACIÓN DE EQUIPOS

La reubicación o movimiento de equipos de computación y comunicación, la instalación y desinstalación de dispositivos, el retiro de sellos tanto de garantía como de licenciamiento de sistema operativo o de programas de herramientas ofimáticas son atributos del personal de Tecnología de la compañía 9 Once Seguridad Ltda., este tipo de tareas se realizarán previa autorización de la Dirección Administrativa y con apoyo de esta.

Todo usuario es responsable de los equipos tecnológicos computacionales y de comunicación asignados en la ubicación autorizada por la Coordinación de tecnología, y el uso de los equipos será de uso exclusivo de las funciones para la compañía 9 Once Seguridad Ltda.

En caso de necesitarlo, es responsabilidad del usuario solicitar capacitación necesaria para el manejo de herramientas informáticas relacionadas con su labor de forma que se reduzca el riesgo de daño o malfuncionamiento de los equipos y herramientas por mal uso o desconocimiento, optimizando al mismo tiempo el uso de las herramientas informáticas.

Toda la información obtenida y desarrollada en base a las funciones de los usuarios se guardará en los directorios asignados en el servidor de archivos, O en las respectivas unidades de red, de manera que los datos puedan identificarse de manera rápida y en una sola ubicación lógica para facilitar el proceso de recuperación o respaldo de archivos.

 <p>Sistema Integrado de Gestión</p>	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

La ingesta de alimentos y/o bebidas mientras se operan los equipos de computación y comunicación está prohibida.

La colocación de cualquier objeto sobre los equipos computacionales o la ubicación de obstáculos o cosas que obstruyan los orificios de ventilación (ubicados en la fuente y parte lateral de los CPU y monitores de los computadores) están prohibidas.

Los cables de conexión de los equipos computacionales a la red eléctrica, a la red de datos y el cable de conexión telefónica deben protegerse, el usuario cuidará que estos cables no sean pisados, aplastados o pinchados por personas u objetos.

Cuando se requiera cambiar la ubicación de varios equipos de cómputo (reestructuración, remodelación, cambio de lugar de unidades, etc) se deberá notificar a la Coordinación de tecnología este particular con un mínimo de 48 horas de anticipación para prever las medidas a aplicarse para realizar el cambio de la manera más rápida y eficaz, todos estos movimientos y reubicaciones deben estar autorizados por la Dirección Administrativa.

Está prohibido que los usuarios abran o desarmen los equipos de computación y de comunicación asignados por la compañía 9 Once Seguridad Ltda.

1.3.5. MANTENIMIENTO DE EQUIPOS

Los servicios de mantenimiento y reparación se llevarán a cabo solamente por el personal de tecnología de la compañía 9 Once Seguridad Ltda., o personal autorizado por la misma unidad, es responsabilidad del usuario solicitar información e identificación de la persona o personas designadas antes de permitir el acceso al equipo asignado.

En caso de ser necesario el traslado del equipo para diagnóstico y reparación, los usuarios deberán hacer respaldos de la información que consideren crítica o relevante para sus funciones; de esta manera se asegura que la pérdida involuntaria de información que podría suceder como efecto de la reparación pueda subsanarse.

1.3.6. PERIFÉRICOS Y DISPOSITIVOS ESPECIALES

Los usuarios cuyos equipos computacionales están equipados con grabadores para CD, DVD o ambos utilizarán estos dispositivos exclusivamente para archivos de respaldo de documentos originales y copias de software autorizadas solamente por el personal de tecnología de la compañía 9 Once Seguridad Ltda., vía contrato.

 <p>Sistema Integrado de Gestión</p>	<p>POLITICA SEGURIDAD DE LA INFORMACIÓN</p>	<p>01-E-06</p>
		<p>FECHA: 14-10-2026</p>
		<p>V. 4</p>

El uso indebido de estos dispositivos para copias no autorizadas por el autor (“piratas”) de cualquier programa de ordenador o software es responsabilidad del usuario bajo cuyo resguardo esté el equipo computacional.

1.3.7. DAÑO DEL EQUIPO

El daño por negligencia, maltrato o descuido del usuario en los equipos de computación y comunicación asignados será cubierto por el responsable previa verificación del inconveniente por parte del personal de tecnología de la compañía 9 Once Seguridad Ltda., en función del daño se podrá solicitar el valor de la reparación o reposición del equipo o dispositivo.

1.4 POLÍTICAS Y NORMAS DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

1.4.1. POLÍTICA

Los funcionarios de la compañía 9 Once Seguridad Ltda., que utilizan equipos de computación y comunicación deben ocupar mecanismos tecnológicos para la protección y privacidad de la información que manejan y generan.

La protección de la información también compete a la prevención de código maliciosos al computador asignado, ya sea este virus, gusano, caballo de troya (troyanos) u otros.

1.4.2. USO DE MEDIOS DE ALMACENAMIENTO

No se admite el uso de archivos compartidos entre los equipos asignados que no correspondan a lo estrictamente laboral, el envío y recepción de documentos importantes se hará vía correo electrónico para que quede constancia del envío y de las partes relacionadas; de esta manera se asegura control sobre el flujo de comunicaciones interno de la compañía.

La información de los colaboradores, deberá ser almacenados de forma centralizada en las unidades de Red, asignadas para tal fin; si esta información se encuentra en ubicaciones distintas, será Única y Exclusivamente responsabilidad

	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

del colaborador su uso y manipulación. Proceso de Tecnología de la Información y Comunicación, no se hará responsable por Perdidas o daños en la misma).

Todos los medios de almacenamiento de información de tipo extraíble (pen drive o USB, CD, DVD, discos extraíbles) asignados por la empresa en función de las tareas de los colaboradores, son responsabilidad del mismo, junto con información contenida, aun cuando no se utilicen. (Según aplique).

El uso de medios de almacenamiento extraíbles en los equipos de la empresa está bloqueado mediante directivas de grupo (GPO). Solo se habilita por excepción autorizada por la Gerencia, por el tiempo aprobado y con registro en el 06-F-20 Matriz Control de accesos TI, según el 06-PR-04 Procedimiento Bloqueo de Dispositivos USB.

1.4.3. INSTALACIÓN DE SOFTWARE

Todos los usuarios que debido a sus actividades requieran el uso de software propietario, deberán justificar el uso de este y solicitar la Autorización a el personal de tecnología de la compañía 9 Once Seguridad Ltda., a través de un oficio firmado por el director del departamento del usuario, indicando en que equipo o equipos (de existir varias licencias adquiridas) deberá instalarse el programa en cuestión y el período de tiempo estimado de uso.

La instalación de cualquier tipo de programa en computadores, servidores o cualquier otro equipo conectado a la red de la compañía 9 Once Seguridad Ltda., sin la autorización del personal de tecnología de la compañía, está prohibida.

1.4.4. IDENTIFICACIÓN DEL INCIDENTE

En el caso que un usuario sospeche o tenga conocimiento pleno sobre un incidente de seguridad informática deberá reportarlo de inmediato al personal de tecnología de la compañía, justificando con claridad porque lo ocurrido se considera como incidente de seguridad informática.

De existir la sospecha de que información ha sido revelada, modificada, alterada o borrada sin autorización del usuario se deberá también notificar el incidente al director de la Unidad respectiva.

	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

Cualquier incidente relacionado con la utilización de equipos computacionales y de comunicación deben reportarse al personal de tecnología de la compañía 9 Once Seguridad Ltda.

1.4.5. ADMINISTRACIÓN DE LA CONFIGURACIÓN

Está prohibido el alterar la configuración del equipo asignado por cualquier motivo, el establecer redes de área local, **conexiones remotas internas o externas**, el intercambio de información a través del protocolo FTP o cualquier otro protocolo de transferencia de datos tampoco está permitido sin la autorización previa del personal de tecnología de la compañía 9 Once Seguridad Ltda.

1.4.6. SEGURIDAD PARA LA RED

El uso del equipo computacional asignado para exploración de los recursos compartidos de la infraestructura de la compañía 9 Once Seguridad Ltda., y las aplicaciones que la misma presta con el objetivo de hallar vulnerabilidades, sin autorización previa del personal de tecnología de la compañía se considera un ataque a la seguridad de la red.

1.4.7. USO DEL CORREO ELECTRÓNICO

El correo electrónico institucional es personal e intransferible, cada usuario mantiene su propia cuenta y está prohibido el utilizar cuentas asignadas a otras personas para enviar o recibir mensajes de correo.

El uso de cuentas de correos en servidores externos (Hotmail, Gmail, etc) para comunicaciones institucionales está prohibido a menos que exista autorización de la Coordinación de tecnología.

Tanto los mensajes enviados y recibidos, así como los archivos adjuntos que salen y entran a los buzones institucionales se consideran propiedad del 9 Once Seguridad Ltda. Los mensajes enviados por correo electrónico se consideran como una comunicación privada y directa entre el emisor y el receptor.

9 once Seguridad Ltda., se reserva el derecho al acceso y análisis de todos los mensajes y archivos adjuntos enviados a través del correo institucional, al existir

	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

sospecha de envío de información que comprometa la seguridad de la red, o cualquier otra acción no autorizada.

El usuario debe utilizar el correo electrónico exclusivamente para desempeñar las funciones que le fueron asignadas por su cargo, empleo o comisión; cualquier otro uso del correo electrónico está prohibido.

Queda prohibido suplantar, falsear o suprimir la identidad de un usuario de correo electrónico.

Queda prohibido el interceptar, revelar o ayudar a interceptar o revelar a terceros las comunicaciones por correo electrónico. El empleo del correo electrónico considera el uso de lenguaje apropiado, evitando palabras ofensivas o altisonantes que afecten la honra y estima de terceros.

1.4.8. CONTROLES CONTRA CÓDIGO MALICIOSO

Para evitar la inducción de código malicioso dentro de los equipos computacionales, el personal hará uso sólo del software o programas de instalados y validados personal de tecnología de la compañía 9 Once Seguridad Ltda.

Los usuarios de la infraestructura tecnológica de 9 Once Seguridad Ltda., deben verificar que toda información contenida en medios de almacenamiento extraíbles como, CD, DVD o memorias USB esté libre de códigos maliciosos, esto a través del software antivirus autorizado e instalado en cada equipo de cómputo por personal de tecnología de la compañía 9 Once Seguridad Ltda.

Debe verificarse la presencia o no de código malicioso en todos los archivos adjuntos comprimidos (en formato .zip o .rar) enviados por personal externo o interno ejecutándose el programa antivirus autorizado antes de ejecutarse la descompresión.

El usuario que genere, compile, escriba, copie, propague o ejecute programas o aplicaciones en cualquier código o lenguaje de computadora que estén diseñados para auto-replicarse, dañar o borrar datos o impedir el funcionamiento de aplicaciones y programas autorizados o componentes del equipo computacional como memorias o periféricos será sancionado por la autoridad competente como ataque contra la seguridad informática de 9 Once Seguridad Ltda.

	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

Cualquier usuario que sospeche la infección de su equipo computacional de virus, troyano o cualquier otro código malicioso deberán dejar de usar inmediatamente el equipo y anunciar al personal de tecnología de la compañía 9 Once Seguridad Ltda. Para la toma de acciones respectivas de re-establecimiento del equipo y eliminación del código malicioso.

Los usuarios a quienes se han asignado equipos portátiles están en el deber de solicitar periódicamente al personal de tecnología de la compañía la actualización del software antivirus.

Los usuarios no deben cambiar o eliminar las configuraciones de las consolas de antivirus instaladas en cada equipo computacional para prevenir la propagación de código malicioso. Los códigos maliciosos son cada vez más complejos, por lo que ningún usuario debe intentar erradicarlos por sí mismo.

1.4.9. USO DEL INTERNET

El acceso a Internet provisto para el personal de 9 Once Seguridad Ltda a través de equipos computacionales es exclusivo para el desarrollo de las actividades relacionadas con las necesidades del puesto y función que desempeña.

Todos los accesos de Internet deben ser provistos a través de los canales previstos para el efecto, de necesitarse una conexión a Internet especial de características diferenciadas esta debe ser notificada y autorizada por personal de tecnología de la compañía.

Los usuarios de internet que sospechen la ocurrencia de un incidente de seguridad informática deben reportarlo inmediatamente al personal de tecnología de la compañía con los justificativos respectivos sobre las sospechas para la verificación del incidente. Todo usuario de Internet en 9 Once Seguridad Ltda., al aceptar el servicio está aceptando que:

- Las actividades realizadas en Internet serán sujeto de monitoreo.
- Conocen la prohibición al acceso de páginas no autorizadas
- Conocen la prohibición de descarga de software y archivos de música o video sin la autorización del personal de tecnología.
- La utilización del Internet es para el desempeño de su función y cargo en 9 Once Seguridad Ltda., y no para propósitos personales.

	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

1.5. POLÍTICAS Y NORMAS DE CONTROLES DE ACCESO LÓGICO

1.5.1. POLÍTICA

Cada usuario se responsabilizará por el mecanismo de acceso lógico asignado, esto es su identificador de usuario y password necesarios para acceder a la información e infraestructura de comunicación de 9 Once Seguridad Ltda., es responsabilidad de cada usuario la confidencialidad de los mismos.

El acceso a la información que fluye dentro de la infraestructura tecnológica d 9 Once Seguridad Ltda., se otorga en base a las funciones del usuario, se deberán otorgar los permisos mínimos necesarios para el desempeño del cargo o rol.

1.5.2. CONTROLES DE ACCESO LÓGICO

La coordinación de tecnología de la información, garantizara la revisión periódica de los accesos asignados a los usuarios, con el fin de efectuar controles, de seguridad de la información

Todos los usuarios de equipos computacionales son responsables de la confidencialidad del identificador de usuario y el password de su equipo, así como de aplicaciones especiales que requieran el mismo control de acceso lógico.

Todos los usuarios deberán autenticarse con los mecanismos de control de acceso lógico antes de tener acceso a los recursos de la Infraestructura tecnológica de 9

Once Seguridad Ltda.

No está permitido a los usuarios el proporcionar información a personal externo sobre los mecanismos de control de acceso a los recursos e infraestructura tecnológica de 9 Once Seguridad Ltda., salvo el caso de autorización expresa del generador de la información y la personal de Tecnología.

El identificador de usuario dentro de la red es único y personalizado, no está permitido el uso del mismo identificador de usuario por varios miembros del personal.

 <p>Sistema Integrado de Gestión</p>	<p>POLITICA SEGURIDAD DE LA INFORMACIÓN</p>	<p>01-E-06</p>
		<p>FECHA: 14-10-2026</p>
		<p>V. 4</p>

El usuario es responsable de todas las actividades realizadas con su identificador de usuario, por tanto, no debe divulgar ni permitir que terceros utilicen su identificador, al igual que está prohibido usar el identificador de usuario de otros.

1.5.3. ADMINISTRACIÓN DE PRIVILEGIOS

Todo cambio en roles, funciones o cargo que requiera asignar al usuario atributos para acceso a diferentes prestaciones de la infraestructura tecnológica de 9 Once Seguridad Ltda., debe ser notificado al personal de Tecnología por el Director correspondiente a la unidad o la autoridad que ordena el cambio.

1.5.4. EQUIPO DESANTENDIDO

El usuario que deja su lugar de trabajo por cualquier razón debe dejar bloqueado su terminal o equipo computacional precautelando la seguridad de la información a través del mecanismo de control de acceso lógico.

1.5.5. ADMINISTRACIÓN Y USO DE PASSWORDS

Es obligación del usuario cambiar la clave por defecto asignada por el personal de tecnología de 9 Once Seguridad Ltda.

Los passwords son individuales, está prohibido que varios usuarios compartan un password.

Cuando un usuario olvide, bloquee o extravíe su password deberá solicitar al personal de tecnología para que se le realice la acción que le permita ingresar un nuevo password, y el momento de recibirlo deberá personalizar uno nuevo.

Está prohibido mantener ayudas escritas o impresas referentes al password en lugares donde personas no autorizadas pueden descubrirlos.

La revelación del password o contraseña a terceros responsabiliza al usuario que prestó su password de todas las acciones que se realicen con el mismo.

Los usuarios deberán observar las siguientes guías para la construcción de su contraseña:

- La contraseña tendrá mínimo ocho (8) caracteres, sin longitud máxima, y combinará mayúsculas, minúsculas, números y caracteres especiales.

 <p>Sistema Integrado de Gestión</p>	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

- Deben ser difíciles de adivinar, es decir no deben estar relacionados con nombre del empleado, fechas de nacimiento, lugar o cargo o estado dentro del trabajo.

Las contraseñas se cambiarán cada noventa (90) días, y de inmediato cuando se sospeche que otra persona la conoce. No se podrán repetir las últimas cinco (5) contraseñas.

Los cambios o desbloqueo de password solicitados por el usuario al personal de tecnología serán notificados posteriormente al solicitante y al superior inmediato de manera que se pueda detectar cualquier cambio no solicitado.

La cuenta se bloqueará después de tres (3) intentos fallidos de inicio de sesión. El correo corporativo y las cuentas administrativas usarán autenticación de múltiples factores (MFA).

Estos requisitos se configuran de forma centralizada mediante directivas de grupo (GPO) de Windows Server, según el 06-PR-05 Procedimiento Gestión de Contraseñas por GPO, y los restablecimientos de contraseña se registran en el 06-F-16 Control cambio de contraseñas.

1.5.6. CONTROL DE ACCESOS REMOTOS

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con la autorización y un mecanismo de control de acceso seguro autorizado por el dueño de la información y la del personal de tecnología de 9 Once Seguridad Ltda.

1.5.7. REALIZACION DE SIMULACROS

La coordinación de tecnología tendrá la obligación simulacros periódicos mínimo 1 vez durante cada 12 meses y ejercicios prácticos en el ámbito de la seguridad de las tecnologías de la información con el fin de evaluar la efectividad de las medidas de seguridad implementadas

1.6. POLÍTICAS Y NORMAS DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

1.6.1. POLÍTICA

El personal de tecnología de 9 Once Seguridad Ltda., emitirá y revisará el cumplimiento de las políticas y normas de seguridad informática que permitan realizar acciones correctivas y preventivas para el cuidado y mantenimiento de los equipos que forman parte de la infraestructura de la compañía.

1.6.2. DERECHOS DE PROPIEDAD INTELECTUAL

Las leyes de propiedad intelectual prohíben la reproducción de programas de ordenador o software sin autorización escrita del autor, ya sea este adquirido o desarrollado en el Instituto.

Los sistemas desarrollados por personal interno o externo bajo la supervisión de del personal de tecnología de 9 Once Seguridad Ltda.

1.6.3. VIOLACIONES DE SEGURIDAD INFORMÁTICA

Se prohíbe el uso de herramientas de hardware o software que alteren o eviten los controles de seguridad informática, a menos que exista autorización expresa del personal de tecnología.

Está prohibido realizar pruebas a los controles efectuados por el personal de tecnología, ninguna persona puede probar o intentar comprometer los controles internos a menos que cuente con la aprobación del personal de tecnología o sea un órgano interno de control.

La búsqueda de vulnerabilidades o fallas de seguridad informática está reservada para el personal de tecnología, está prohibida la realización de pruebas de este tipo para cualquier usuario no autorizado.

La propagación de código malicioso de forma intencional para probar el desempeño de la red de parte de usuarios no autorizados está prohibida totalmente.

1.7. POLÍTICAS RESPALDO DE INFORMACIÓN BACK UP

1.7.1 PROPÓSITO Y ALCANCE

 Sistema Integrado de Gestión	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

Esta política establece las directrices para la **creación, gestión y restauración** de copias de seguridad del servidor principal, con el fin de proteger la **integridad, disponibilidad y confidencialidad** de los datos críticos de la empresa. La política aplica a todo el personal y a los sistemas involucrados en el proceso de respaldo de datos.

1.7.2. MODELO DE COPIA DE SEGURIDAD 3-2-1

El modelo de copias de seguridad adoptado se basa en la regla 3-2-1:

- **Copia 1 (Fuera del Sitio):** Una copia de seguridad **comprimida y encriptada** se sube a **Dropbox Business** diariamente. Esta copia sirve como el respaldo principal y se almacena en la nube, fuera de las instalaciones físicas.
- **Copia 2 (Medio Físico):** Una segunda copia de seguridad se guarda en un **disco duro externo**. Este disco se almacena en una **caja fuerte** dentro de la oficina para protegerlo contra robos o daños físicos.
- **Copia 3 (Medio Físico Externo):** Una tercera copia de seguridad se guarda en un **segundo disco duro externo** y se almacena en una **ubicación externa** a la oficina, en la casa del Gerente, para proteger los datos en caso de un desastre mayor que afecte las instalaciones.

1.7.3. PROCEDIMIENTOS DE COPIA DE SEGURIDAD

1. **Frecuencia:** Las copias de seguridad se realizarán **diariamente** fuera del horario laboral para minimizar el impacto en el rendimiento del servidor.
2. **Automatización:** El proceso de respaldo será **automatizado** mediante un software de terceros **Cobian backup** para asegurar su consistencia y fiabilidad.
3. **Compresión y Encriptación:** Todas las copias de seguridad se deben **comprimir y encriptar** utilizando algoritmos robustos (por ejemplo, AES-256) para proteger los datos en tránsito y en reposo. Las claves de encriptación deben guardarse de forma segura y separada de las copias de seguridad.
4. **Verificación:** mensualmente, se debe realizar una **verificación de la integridad** de las copias de seguridad para asegurar que los archivos no estén corruptos y sean restaurables, la cual se realizara antes de ejecutar la copia de seguridad en el disco duro externo y consignado en el 06-F-02 Control Backup V1.
5. **Rotación de Medios:** Se implementará un **esquema de rotación** para los discos duros externos (Rotación mensual para la copia interna / caja fuerte y

 <p>Sistema Integrado de Gestión</p>	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

semestral para la copia externa / residencia de representante legal) para garantizar la existencia de múltiples puntos de restauración en el tiempo.

1.7.4. RETENCIÓN DE DATOS

- **Dropbox:** Se mantendrán las copias de seguridad de los **últimos 30 días**.
- **Discos Duros Externos:** Se conservarán las copias de seguridad de las **últimas 6 meses** en el medio de la caja fuerte y las de los **últimos 6 meses** en la ubicación externa.

1.7.5. PROCEDIMIENTOS DE RESTAURACIÓN

1. **Pruebas de Restauración:** Se realizarán **pruebas de restauración Semestrales** para validar el proceso y el tiempo de recuperación (RTO - Recovery Time Objective).
2. **Incidentes:** En caso de pérdida o corrupción de datos, el equipo de TI debe seguir el **plan de recuperación de desastres** para restaurar la información a partir de la copia de seguridad más reciente y no dañada.

1.7.6. RESPONSABILIDADES

- **Equipo de TI:** Es responsable de la **implementación, monitoreo y mantenimiento** del sistema de copias de seguridad.
- **Gerencia:** Es responsable de **aprobar y auditar** el cumplimiento de esta política.

1.7.7. AUDITORÍA Y REVISIÓN

Esta política se **revisará anualmente** o cuando haya cambios significativos en la infraestructura de TI o en los requisitos de seguridad.

1.8. SEGURIDAD DE LA INFORMACIÓN EN TORNO AL TALENTO HUMANO

En tratamiento de los datos personales, antes, durante y después de la relación laboral, se regirá por las siguientes reglas:

- 9Once Seguridad informará a las personas interesadas en participar en un proceso de selección, las reglas aplicables al tratamiento de los datos personales

 <p>Sistema Integrado de Gestión</p>	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

que suministre el interesado durante el respectivo proceso de selección, así como de aquellos datos que se obtengan durante la realización de este, los interesados firmarán el formato de autorización de datos destinado para ello.

- El tratamiento de los datos suministrados por los interesados en las vacantes de 9ONCE SEGURIDAD y los obtenidos del proceso de selección, será únicamente el informada en la autorización al aspirante.
- La empresa realizará estudios de antecedentes disciplinarios, previos a la contratación de nuevo personal para la empresa.
- La empresa contará con un proceso de eliminación de las hojas de vida de los candidatos (titulares) sobre los que ya no se tenga interés en conservar contacto.
- Una vez seleccionada un aspirante para ocupar un cargo en 9Once Seguridad, se celebrará el respectivo contrato de trabajo, acuerdo de confidencialidad y se le asignará cuando el cargo lo requiera, un usuario con un perfil definido relacionado directamente con el cargo a desempeñar, el cual le permitirá el acceso a la información personal tratada por la empresa, cuando el cargo así lo requiera.
- Seleccionado el candidato para el cargo, la empresa almacenará los datos personales del trabajador en una carpeta identificada con el nombre de cada persona. A esta carpeta solo tendrá acceso el proceso de Gestión Integral y Talento Humano, Gestión Administrativa y Dirección y planeación con la finalidad de gestionar la relación laboral entre la empresa y el empleado.
- Para cuando 9Once Seguridad, requiera contratar servicios externos para el tratamiento de datos durante la relación contractual con los trabajadores, podrá requerirse la transferencia de datos personales a un tercero que se denominará Encargado, Para este caso, la empresa seguirá los lineamientos para la selección de Encargados en la transmisión de datos personales contenidos en esta política.
- Con la finalización del contrato, la empresa solicitará la entrega formal de perfiles y contraseñas que le hayan sido asignadas durante la ejecución del contrato de trabajo.
- Terminada la relación laboral, 9Once Seguridad, igualmente procederá a almacenar los datos personales de sus extrabajadores en un archivo general, sometiendo tal información a medidas y niveles de seguridad altas, atendiendo la calidad de los datos que dicho archivo puede contener.

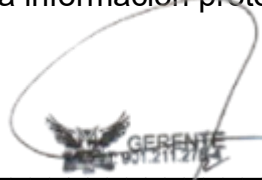
 <p>Sistema Integrado de Gestión</p>	POLITICA SEGURIDAD DE LA INFORMACIÓN	01-E-06
		FECHA: 14-10-2026
		V. 4

1.8.1. CONFIDENCIALIDAD CON TERCEROS

9ONCE SEGURIDAD para el desarrollo de las relaciones contractuales con proveedores y contratistas recurrentes o, que tengan acceso a información sensible o confidencial, exigirá a los terceros la aceptación de los acuerdos de confidencialidad definidos por la organización. Los acuerdos establecen el compromiso de salvaguardar la información, velar por su correcto uso, impedir el uso no autorizado de dicha información y guardar reserva. Se debe estipular a su vez la información que es objeto de protección dentro del acuerdo y su temporalidad.

Los acuerdos deben incluirse dentro de los contratos celebrados entre la organización y terceros, como parte integral del contrato o firmarse como un acuerdo independiente.

La aceptación de las condiciones de confidencialidad es indispensable para conceder al tercero el acceso a la información protegida.



Carlos Uriel Falla Guzmán
Gerente General