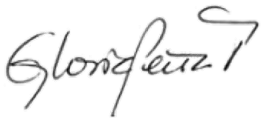
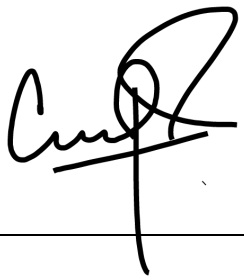
Política de Seguridad de la Información
SOCIEDAD TEQUENDAMA

BOGOTA D.C.

ELABORO	REVISO	APROBÓ
Gloria Peña Jefe Tecnología de la información y comunicaciones	Christian Henrique González Secretario General	Christian Henrique González Secretario General
Firma: 	Firma: 	Firma: 

Contenido

Propósito

La Sociedad Tequendama S.A., procede a adoptar la Resolución 7870 del 26 de diciembre de 2022, por la cual el Ministerio de Defensa Nacional procedió a emitir y adoptar la Política General de Seguridad y Privacidad de la información, seguridad Digital, Ciberseguridad y Continuidad de los servicios tecnológicos en las Unidades Ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y Sociedad adscritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.

Es así como, teniendo en cuenta la importancia que tiene que la Sociedad defina las necesidades de sus grupos de interés, y la valoración de los controles precisos para mantener la seguridad de la información, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la Sociedad, sus objetivos , sus procesos misionales, y que este adaptada a las condiciones específicas y particulares de cada una según corresponda para que sea aprobada y guiada por la Dirección.

Con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información, así como definir políticas frente a la recolección, manejo tratamiento y protección de datos personales y privacidad de todas las personas con el propósito de garantizar y proteger el derecho fundamental de habeas data.

1. Política General de Seguridad de la información

Para la Sociedad Tequendama, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma. Esta política se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Promover la adopción de medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.
- Promover el desarrollo de una cultura de seguridad de la información y ciberseguridad a través de campañas de sensibilización y concientización.
- Gestionar los recursos financieros requeridos para la implementación del (MSPI).
- Ordenar la inclusión, de temas relacionados con seguridad de la información y ciberseguridad, en las materias y cursos de tecnología que se dictan en las escuelas de formación y capacitación de las Fuerzas Militares y Policía Nacional.

La Sociedad adopta la **Política General de Seguridad y Privacidad de la información, Seguridad Digital, Ciberseguridad y Continuidad** de los servicios tecnológicos en las Unidades Ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y Sociedad adscritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.”, con el fin de dar aplicación a las normas, políticas y directivas que sobre el particular ha expedido el Ministerio de Defensa; y la Directiva Permanente 0018 del 19 de junio de 2014 del Ministerio de Defensa Nacional -DIR2014-18- "Políticas de Seguridad de la Información para el Sector Defensa”.

La Secretaría General como responsable y de conformidad con el parágrafo del artículo sexto de la Resolución 7870 del 26 de diciembre de 2022, en relación con la implementación de esta resolución, las siguientes funciones:

- Verificar el cumplimiento de la resolución mencionada y demás normas que la desarrollen, adicionen o modifiquen.
- Promover la adopción de medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.
- Promover el desarrollo de una cultura de seguridad de la información y ciberseguridad a través de campañas de sensibilización y concientización.
- Adoptar la seguridad digital y ciberseguridad con un enfoque preventivo y proactivo, priorizando la protección de datos personales e información sensible de la Sociedad o que goza de reserva legal, al igual que los servicios y sistemas de información e infraestructura críticas.
- Fungir como único canal de comunicación autorizado para hacer pronunciamientos oficiales ante Sociedades externas, medios de comunicación o la ciudadanía, reportará los incidentes que afecten la infraestructura crítica y la Seguridad Nacional ante las autoridades competentes.
- Designar al Responsable de Seguridad de la Información representante de la Alta Dirección para el Modelo de Seguridad y Privacidad de la Información (MSPI), con el fin de apoyar las actividades y controles necesarios para llevar a cabo la implementación y la mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI) en su Sociedad.
- Gestionar los recursos financieros requeridos para la implementación del (MSPI).
- Ordenar la inclusión, de temas relacionados con seguridad de la información y ciberseguridad, en las materias y cursos de tecnología que se dictan en las escuelas de formación y capacitación de las Fuerzas Militares y Policía Nacional.
- Apoyar la creación de los respectivos Equipos de Respuesta a Emergencia Informáticas (CSIRT) y Centros de Operaciones de Seguridad (SOC), con el propósito de apoyar a la gestión de incidentes.

el área de Tecnologías e Información y las Comunicaciones, debe dar cumplimiento de la Resolución 7870 del 26 de diciembre de 2022, para lo cual deberá realizar las siguientes actividades:

- Artículo 18. Adoptar las medidas necesarias para asegurar la transferencia y seguridad de la información, incluyendo la contenida en los mensajes electrónicos.
- Artículo 19. Política General de la estrategia de seguridad digital, liderar la implementación del Modelo de Seguridad y privacidad de la Información (MSPI), articularlo debidamente con el habilitador de seguridad y privacidad de la política de Gobierno Digital, de acuerdo con los lineamientos emitidos en la Resolución 500 del 10 de marzo de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones sus lineamientos, criterios, y gestión de riesgos de la seguridad de la información, seguridad digital y ciberseguridad,

- Artículo 20. implementar los planes y controles para mitigar los riesgos que puedan afectar la seguridad digital y física de acuerdo con el resultado de análisis y evaluación de riesgos, y cumplir con las demás características y responsabilidades establecidas.
- Artículo 21. Política de tratamiento para la gestión de incidentes de Seguridad digital, para lo cual debe gestionar los incidentes de seguridad digital y ciberseguridad y deberá coordinar las tareas de seguridad informática, cumpliendo con los lineamientos y criterios establecidos
- Liderar el relacionamiento en la materia con los Equipos de Respuesta a Emergencias Informáticas (CSIRT) del Ministerio de Defensa, con el fin de coordinar con ellos las capacidades de ciberseguridad y ciberdefensa.
- Artículo 22. Elaborar el análisis del impacto del negocio (BIA) y el plan tecnológico de la Sociedad., asi como la política de continuidad de la operación mediante la la operación y administración de los recursos tecnológicos que soportan la operación, definir e implementar el plan de continuidad tecnológico del negocio, los procedimientos de continuidad y de contingencia para cada una de las plataformas tecnológicas críticas bajo su responsabilidad y cualquier estrategia orientada a generar el diagnóstico inicial, la contención, la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de riesgos de seguridad de la información, seguridad digital y ciberseguridad.

Artículo 22 de la Resolución 7870 del 26 de diciembre de 2022, delegar en el área de Planeación o quien haga sus veces, como el área encargada de liderar el Plan de Continuidad del Negocio de esta sociedad.

De conformidad con lo señalado en el artículo 23 de la Resolución 7870 del 26 de diciembre de 2022, todos los integrantes, contratistas o terceros que hagan uso de los recursos tecnológicos de la Sociedad Tequendama tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable, entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación y, por ende, el cumplimento de la misión . Deberán cumplir con las siguientes directrices:

- Minimizar el riesgo en las funciones más importantes de la Sociedad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de SOCIEDAD TEQUENDAMA
- Garantizar la continuidad del negocio frente a incidentes.
- SOCIEDAD TEQUENDAMA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Finalmente, incluimos la descripción general de otras políticas para el cumplimiento dentro del SGSI; para la gestión de activos, seguridad física y ambiental, control de accesos, etc. Para abordar este punto nos remitimos a la "Guía de políticas específicas de seguridad y privacidad de la información" y mencionar algunas de ellas.

Principios de seguridad.

La Sociedad Tequendama:

- Define, comparte, publica las responsabilidades frente a la seguridad de la información en cabeza de los empleados, proveedores, socios de negocio o terceros.
- Protege la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes)
- Protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- Protegerá su información de las amenazas originadas por parte del personal.
- Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementará control de acceso a la información, sistemas y recursos de red.
- Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Garantizará una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- Garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales

2. Políticas específicas recomendadas para la implementación de controles de seguridad de la información

En este documento presenta algunas recomendaciones de políticas de seguridad de la información para el Modelo de Seguridad y privacidad de la Información para las Sociedades del Estado. Este conjunto de recomendaciones no es exhaustivo, se aconseja que cada Sociedad genere sus documentaciones propias dependiendo de sus características particulares, sus activos de información, sus procesos y los servicios de información que pueda prestar. A continuación se agruparan las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Sociedad.

2.1. Tecnología en la Nube

Tecnologías en la Nube sea confiable y segura

- Los servicios de Tecnologías en la Nube deben aplicar las medidas de seguridad necesarias para garantizar la integridad, disponibilidad y confidencialidad de la

información de la institución, así como cumplir con los requisitos establecidos en la normatividad vigente y con los niveles de seguridad adecuados para los servicios que presta cada Sociedad del Sector Defensa.

- Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y seguridad informática incluyendo los servicios en la nube de la Sociedad Tequendama, deberán estar protegidos mediante herramientas y software de seguridad que prevenga el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos.

2.2. Gestión de Activos

Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información, las políticas relacionadas con gestión de activos deben contemplar como mínimo:

- Identificación y disposición de Activos: Periodicidad de identificación y/o actualización del inventario de Activos de Información, responsable, propietario. Adicionalmente, proceso para realizar de forma segura la correcta la eliminación, retiro, traslado o reuso cuando ya no se requieran los activos. Validación y actualización de los activos para evitar el acceso o borrado no autorizado de la información.
- Clasificación de Activos: Clasificación de los activos de información de acuerdo a la criticidad, sensibilidad y reserva de la misma.
- Etiquetado de la Información: Determinar el mecanismo, responsable y obligatoriedad para el etiquetado o rotulación de Activos.
- Devolución de los Activos: Determinar el instrumento y responsable del cumplimiento, mediante el cual se genera obligatoriedad para que los funcionarios, contratistas y/o terceros realicen la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con la Sociedad.
- Gestión de medios removibles: Usos y permisos que tienen los usuarios y/o funcionarios de la Sociedad frente a los medios removibles, entendiendo como medio removible a todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores (casos en que se autoriza y en los que no, y uso de medios removibles).
- Dispositivos móviles: Determinar los funcionarios, contratistas o terceros que pueden tener acceso a las redes inalámbricas, quiénes pueden realizar instalación de chats corporativos y/o correos electrónicos de la Sociedad mediante el uso de este tipo de dispositivos, adicionalmente debe describir las responsabilidades que deben tener los funcionarios, contratistas o terceros frente al uso de la información almacenada en los dispositivos móviles así como como los controles de seguridad que la Sociedad utilizará para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información.

2.3. Correo electrónico

Normativa de uso de correo electrónico. Esta normativa ayudará a garantizar que los integrantes de la Sociedad sean conscientes de sus responsabilidades al utilizar el correo electrónico, de lo que pueden y no pueden hacer, y de que estos términos estén acordados y

firmados. Por lo tanto, un integrante puede ser considerado responsable si hubiera una violación de estos términos.

Esta normativa deberá ser aceptada por todos los empleados antes de incorporarse al puesto de trabajo

Políticas:

- En caso de que se envíe un correo electrónico que no se considere de contenido apropiado de acuerdo con la política en materia de correo electrónico, sería el integrante, y no la Sociedad, quien asumiría la responsabilidad de cualquier daño o demanda que se presente como resultado de su envío de un correo electrónico inapropiado.
- Tener una buena política en materia de correo electrónico puede ayudar a la ciberseguridad. Los comunicados a todo el personal relacionados con Phishing deben ser revisados y tenidos en cuenta para evitar daños significativos para la Sociedad.
- Los bienes de cómputo no pueden ser utilizados con fines personales, estos se emplearán de manera exclusiva y bajo la completa responsabilidad del servidor público o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas.
- Sobre el uso del correo electrónico.
- El único servicio de correo electrónico autorizado para el manejo o transmisión de la información en la Sociedad es el asignado por el área de Tecnología, con el dominio de la Sociedad, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando cualquier tipo de ataque cibernético. Así mismo deberán contener una sentencia de confidencialidad, que será diseñada por el área de Tecnología e Información, con el apoyo de el área de Comunicaciones y el área Jurídica, o similares en la Sociedad.
- El servicio de correo electrónico de la Sociedad debe ser empleado únicamente para enviar y recibir mensajes de carácter y debe contener cuando aplique la firma digital de la Sociedad; en consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro fin ajeno a los propósitos de la Sociedad.
- En cumplimiento de la iniciativa de reducción de papel, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la Ley lo permita.
- Se permite el envío masivo de correos desde las cuentas corporativas, los cuales deben cumplir con las características de comunicación e imagen corporativa y ser asignadas a un responsable para garantizar el correcto uso de estas.
- Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado a el área de Tecnología a través de la respectiva Mesa de ayuda, como incidente de seguridad, y deberán acatarse las indicaciones recibidas para su tratamiento.
- La cuenta de correo no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, o cualquier otra ajena a los fines de la Sociedad.
- Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y que atenten contra la integridad moral y/o buena imagen de las personas o instituciones.

- Está expresamente prohibido distribuir información catalogada como clasificada o reservada a otras Sociedades o ciudadanos sin la debida autorización de la Gerencia General, Secretaria General o las que hagan sus veces, en los casos que aplique.
- El cifrado de los mensajes será necesario siempre que la información transmitida desde un correo electrónico esté catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la Ley Colombiana vigente.
- Está expresamente prohibido distribuir, copiar, reenviar información propiedad de la Sociedad a través de correos personales o sitios web diferentes a los autorizados en el marco de sus funciones u obligaciones contractuales.
- El área de Tecnología debe coordinar internamente la identificación de los buzones de correo que se considere su contenido como información relevante para la Sociedad y por ello se hace necesario salvaguardar la información de acuerdo con las regulaciones vigentes en cuanto a preservación y conservación documental establecidas por el Archivo General de la Nación y Ministerio de Tecnologías de la Información y Comunicaciones.
- La Sociedad Tequendama se reservan el derecho de monitorear los accesos y el uso de los buzones de correo de todos sus integrantes o contratistas. Además, podrá realizar copias de seguridad del correo electrónico en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información propios o de terceros operados en la Sociedad Tequendama.

2.4. Dispositivos y software

- el área de Tecnología e Información deberá establecer y aplicar controles respecto al uso adecuado de los activos de información, así como la verificación de cumplimiento del software base y de aplicaciones, para prevenir la descarga, instalación y uso de software no licenciado y/o no autorizado, definiendo, manteniendo y controlando la lista de software y aplicaciones autorizadas para ser instaladas en las estaciones de trabajo de los usuarios, cumpliendo los criterios de autenticidad, vigencia, términos y condiciones legales para la utilización de la licencia.
- En caso de que el servidor público, contratista y/o terceros deba hacer uso de equipos ajenos a la Sociedad Tequendama, éstos deberán cumplir con la legalidad del Software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red , si es autorizado por el área de Tecnologías o quien haga sus veces.
- Es responsabilidad de los integrantes, contratistas y terceros mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas al finalizar la vinculación con la Sociedad para su custodia.
- Está expresamente prohibido el almacenamiento en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, de archivos de video, música y fotos que no sean de carácter o que atenten contra los derechos de autor o propiedad intelectual de los mismos.
- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos autorizados expresamente por la dependencia responsable.
- Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar,

revisar y/o reparar sus componentes, son las designadas para tal labor por el área de Tecnología e Información.

- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la que tenga bajo su responsabilidad dicha función previa coordinación del área de Tecnología e Información, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias del área de Activos fijos
- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes deberá ser informada de inmediato a el área de Tecnología e Información por el servidor público, contratista o tercero a quien se le hubiere asignado; así mismo, deberá reponerse a la Sociedad o aplicar los procedimientos establecidos para este tipo de siniestros que estime la Sociedad.
- La pérdida de información deberá ser informada con detalle a el área de Tecnología e Información, a través de la Mesa de ayuda, como incidente de seguridad.
- Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información física o digital deberá ser reportado a la mayor brevedad al área de Tecnología, a través de la mesa de ayuda.
- El área de Tecnología es la dependencia autorizada para administrar el software, la cual no deberá ser copiada, suministrada a terceros ni utilizada para fines personales.
- Todo acceso a la red deberá ser informado, autorizado y controlado por el área de Tecnología.
- el área de Tecnologías será responsable de que sus usuarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas Web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.
- Los teléfonos móviles y/o teléfonos inteligentes asignados por la Sociedad, debe permanecer encendidos y cargados como mínimo durante las horas laborales.
- El uso del dispositivo móvil suministrado debe ser para realizar actividades propias de su cargo o funciones asignadas en la Sociedad.
- No están autorizados a cambiar la configuración, ni a la desinstalación de software de los equipos móviles asignados posterior a su recibo; únicamente se deben aceptar y aplicar las actualizaciones.
- Evitar hacer uso de los dispositivos móviles asignados en lugares con algún riesgo de seguridad, con el fin de evitar el extravío o hurto del equipo.
- No se debe hacer uso de los dispositivos móviles asignados en redes inalámbricas públicas.

2.5. Conexión Wifi

- La conexión a la red Wifi para integrantes y contratistas deberá ser administrada desde el área de Tecnología, mediante un SSID (Service Set Identifier) único; la autenticación deberá ser con usuario y contraseña de directorio activo u otro tipo de autenticación cuando aplique para la Sociedad.
- La conexión a la red Wifi para visitantes deberá tener un SSID y las contraseñas serán administradas por el área de Tecnología y las contraseñas deberán cambiar cada

semana, solo estarán disponibles en el horario laboral definido y la conexión solo será para el servicio de internet y estará restringida para la conexión a servicios .

- Los equipos deben quedar apagados cada vez que el integrante, contratista o tercero no se encuentre en el área o durante la noche; esto, con el fin de proteger la seguridad y distribuir bien los recursos; se exceptúa aquellos casos en que se esté realizando trabajo remoto.
- Cuando se utilicen aplicaciones de mensajería instantánea para actividades , deberán adoptarse políticas de seguridad y términos de uso de las aplicaciones, evaluando previamente los riesgos de vulnerabilidades de afectación a la confidencialidad, integridad y disponibilidad de la información.

2.6. Uso de Internet, Redes sociales

Sobre el uso de Internet: el área de Tecnología, a través del Jefe de Seguridad de la Información, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones y será responsabilidad de los colaboradores las siguientes, entre otras:

- No está permitido enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o de las instituciones.
- No está permitido acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por la política de navegación de la Sociedad Tequendama.
- No está permitido enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.
- No está permitido propagar intencionalmente virus o cualquier tipo de código malicioso.
- El área de Tecnología debe implementar protocolos y políticas de acceso remoto que impidan a los usuarios escalar privilegios y que mitigue el riesgo de acceso no autorizado a recursos o información.
- El área de Tecnología se reserva el derecho de monitorear los accesos y el uso del servicio de Internet, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines de la Sociedad.
- Del uso de las redes sociales: Todos los integrantes son responsables de la información que generan, acceden y procesan, así como de evitar su uso indebido, para lo cual se dictan los siguientes lineamientos:
  - Las redes sociales de carácter no deben ser abiertas a nombre propio de funcionarios o contratistas sino de la Sociedad.
  - El funcionario responsable del manejo de las redes sociales debe garantizar el uso adecuado de las mismas.
  - El uso de las redes sociales debe ser controlada por el área de comunicación de la Sociedad, con el fin de contar con niveles de protección adecuados para un uso correcto y seguro de estas plataformas en apoyo con el área de Tecnología.
  - Se deben utilizar soluciones de seguridad, configurar correctamente los usuarios en las redes sociales, utilizar cuando sea posible un segundo factor de autenticación y el protocolo HTTPS para la navegación, entre otros.

- Se requiere no utilizar un usuario con permisos de administrador al momento de navegar en las redes sociales, y que cada funcionario permitido cuente con sus propios perfiles. Esta es una forma de minimizar el impacto en caso de que ocurra un incidente.
- No utilizar la contraseña de una red social en otros sitios de internet y nunca compartirla, aplicar reglas de contraseña segura, evitar utilizar computadoras públicas para ingresar en las redes sociales.

2.7. Uso del escritorio, pantalla limpia y periféricos

Todos los integrantes, contratistas o terceros que laboran en la Sociedad Tequendama y que hagan uso de estaciones de trabajo, deberán acatar las siguientes disposiciones:

- En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, dejar los medios que contengan información crítica protegida bajo llave.
- Bloquear su estación cada vez que se retiren de su puesto de trabajo y solo se podrá desbloquear con la contraseña del mismo usuario que lo bloqueó.
- Tomar las medidas de seguridad necesarias en el uso de sus contraseñas, para evitar que estas sean conocidas por personal interno o externo a la Sociedad.
- Cuando se imprima o digitalice documentos con información pública clasificada o pública reservada, éstos deben retirarse inmediatamente de dichos dispositivos.
- Los dispositivos de impresión y digitalización deben permanecer limpios de documentos.
- Los documentos que contengan información sensible no deben ser reutilizados y destruirse de acuerdo con los parámetros y normatividad vigente establecida en la ley de Archivo General vigente.
- Sobre el uso de los sistemas o herramientas de Información: Todos los integrantes, contratistas o terceros que laboran en la Sociedad Tequendama son responsables de la protección de la información que acceden y procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:

  - Las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible.
  - Es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos asignados de acuerdo con las políticas de administración de usuarios establecidas en la Sociedad.
  - Es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.
  - Cuando se ausenta por vacaciones, permiso, comisiones, excusas médicas, entre otros, deberá solicitar a través de la mesa de ayuda, el bloqueo de acceso a la estación de trabajo y la cuenta de correo electrónico al área de Tecnología o quien haga sus veces, así mismo si tiene asignado accesos a sistemas de información, deberá reportar al área de Tecnología para que inactiven las respectivas licencias, con el fin de evitar la fuga de la información, el acceso a terceros, lo cual pueda generar daño, alteración o uso indebido a la información, así como la suplantación de id . La dependencia de Gestión del

Talento Humano, y supervisores de los contratos, deberán reportar inmediatamente cualquier tipo de novedad que presenten los integrantes, contratistas o terceros a el área de Tecnología.

- Cuando cesa sus funciones o culmina la ejecución de contrato con la respectiva Sociedad, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información del integrante o contratista será almacenada en los repositorios.
- Cuando cesa sus funciones o culmina la ejecución de contrato con la respectiva Sociedad, el jefe inmediato o supervisor es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual, de acuerdo con la normativa vigente.
- Dar estricto cumplimiento a la reglamentación vigente sobre derechos de autor.

2.8. Control de acceso

La Sociedad determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos; las políticas relacionadas con el control de acceso deben contemplar como mínimo:

- Control de acceso con usuario y contraseña: Se debe elaborar una política sobre control de acceso a redes, aplicaciones, y/o sistemas de información de la Sociedad, mediante la cual se determinen los responsables y los procedimientos formales de autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas. La política debe enunciar las responsabilidades que los integrantes, contratistas o terceros tienen al contar con un usuario o contraseña de la Sociedad, se debe estipular que los usuarios (ID) y contraseñas son personales e intransferibles y no deben prestarse, ni compartirse. La Sociedad debe establecer que por cada integrante, contratista o tercero debe tenerse un usuario y una contraseña para el acceso.
- Suministro del control de acceso: Se asignará acceso a los usuarios mediante el diligenciamiento del formato SOLICITUD DE SERVICIOS INFORMATIVO.
- Gestión de Contraseñas: Lineamientos mínimos que deben tener las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la Sociedad. Esta política debe indicar a los integrantes, contratistas y/o terceros los parámetros mínimos para que una contraseña sea considera como fuerte, gestión de cambio de contraseña, debe determinar que los accesos a la red, las aplicaciones y sistemas de información deben requerir un usuario (ID) y una contraseña fuerte para que realice la correspondiente autenticación y acceso a la información de forma segura.
- Perímetros de Seguridad: La política debe definir los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información a los cuales los integrantes, contratistas o terceros, tienen acceso y a cuales no, la política debe definir los responsables de autorizar o no ingresos a las áreas delimitadas como de acceso restringido.

2.9. No Repudio

La política de seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción. La política deberá incluir mínimo los siguientes aspectos:

- Trazabilidad: La política hará que por medio de la trazabilidad de las acciones se haga seguimiento a la creación, origen, recepción, entrega de información y otros.
- Retención: La política debe incluir el periodo de retención o almacenamiento de las acciones realizadas por los usuarios, el cual deberá ser informado a los integantes, contratistas y/o terceros de la Sociedad.
- Auditoría: La política incluirá la realización de auditorías continuas, como procedimiento para asegurarse que las partes implicadas nieguen haber realizado una acción.
- Intercambio electrónico de información: La política incluirá en los casos que aplique, que los servicios de intercambio electrónico de información son garantía de no repudio.

2.10. Privacidad y Confidencialidad

Esta política debe contener una descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente. La política de privacidad debe contener como mínimo lo siguiente:

- Ámbito de aplicación
- Excepción al ámbito de aplicación de las políticas de tratamiento de datos personales
- Principios del tratamiento de datos personales:
  - Principio de la Legalidad: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
  - Principio de finalidad: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
  - Principio de libertad: El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.
  - Principio de veracidad o calidad: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
  - Principio de transparencia: Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.
  - Principio de acceso y circulación restringida: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.
  - Principio de seguridad: La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento
  - Principio de confidencialidad: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.
- Derechos de los titulares: La política debe indicar los derechos de los titulares de los datos, tales como:

- Conocer, actualizar y rectificar sus datos personales.
- Solicitar la prueba de su autorización para el tratamiento de sus datos personales.
- Ser informado respecto del uso que se le da a sus datos personales.
- Revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere, siempre y cuando no se encuentren vigentes con el Banco los servicios o productos que dieron origen a dicha autorización.
- Presentar quejas utilizando el medio entregado para tal fin para la protección de los datos personales.

- Autorización del titular: La política debe indicar cómo obtener autorización del titular para el tratamiento de sus datos personales, así como los casos en los cuales no se requiere autorización del titular.
- Deberes de los responsables del Tratamiento: La política debe indicar cuales son los deberes de los responsables y/o encargados del tratamiento de los datos personales.
- Política de controles criptográficos: Esta política deberá especificar como se asegura la confidencialidad y autenticidad de la información que circula o se genera a través de los diferentes sistemas de información.
- La política de confidencialidad, debe contener un compromiso o acuerdo de confidencialidad, por medio del cual todo funcionario, contratista y/o tercero vinculado a la Sociedad, deberá firmar un compromiso de no divulgar la información interna y externa que conozca de la Sociedad, así como la relacionada con las funciones que desempeña en la misma. La firma del acuerdo implica que la información conocida por todo funcionario, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.
- La política deberá indicar desde cuando se firma el acuerdo de confidencialidad, así como la vigencia del mismo.

2.11. Gestión de incidentes de Seguridad de la Información

La Sociedad deberá documentar una política general de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Debe ir dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.

La política debe contemplar para su elaboración los siguientes parámetros:

- Debe estar aprobada por la alta dirección, certificando así el compromiso con el proceso.
- Visión General: ¿Qué se debe reportar? ¿A quién debe reportarse?, ¿Qué medios pueden emplearse para hacer el reporte?
- Definir Responsables: Se deben mencionar de manera muy general quienes serán los responsables de gestionar los eventos.
- Actividades: Explicar de manera general en que consiste el proceso de gestión de incidentes desde el reporte hasta la resolución.
- Documentación: Se debe hacer referencia sobre la documentación del esquema de gestión y los procedimientos.

- Descripción Del Equipo Que Manejará Los Incidentes: Se debe indicar como está compuesta la estructura general para la gestión de incidentes y vulnerabilidades de seguridad.

2.12. Capacitación y Sensibilización de la Seguridad de la Información

Esta política se centra en la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

Dicha política debe contener los siguientes parámetros.

- El compromiso de la alta dirección en destinar los recursos suficientes para desarrollar los programas.
- ¿Quiénes deberán ser entrenados? ¿Quiénes deberán ser sensibilizados?
- La obligación de los usuarios a asistir a los eventos o cursos de capacitación.
- Revisión periódica de resultados de capacitaciones para mejoramiento de los procesos.
- Documentación sobre planes de estudio y desarrollo de los programas.
- Compromisos y obligaciones por parte del personal capacitado.
- Contener políticas adicionales relacionadas directamente con el debido comportamiento de los usuarios como las siguientes:
  - Política De Escritorio Limpio
  - Política De Uso Aceptable
  - Ética Empresarial.