1. OBJETIVO

Establecer las políticas de seguridad de la información que deben adoptar todos los colaboradores de ALSERTEC S.A.S., aliados estratégicos y proveedores para fortalecer la seguridad de la información y así garantizar confidencialidad, integridad y disponibilidad de la información

2. ALCANCE

Esta política es aplicable:

- La compañía ALSERTEC S.A.S.;
- Todas las ubicaciones de ALSERTEC SA.S.;
- Todos los colaboradores de ALSERTEC S.A.S., aliados estratégicos, visitantes y proveedores;
- Toda la información, datos, sistemas de información, sistemas de procesamiento, computadores, redes y equipos de almacenamiento que pertenecen o son custodiados por ALSERTEC S.A.S. y los aliados estratégicos.

3. RESPONSABLES

Junta Directiva, presidentes y Gerentes

- Promover la cultura de seguridad de la información
- Apoyar la divulgación de las políticas de seguridad de la información
- Velar por el cumplimiento de la presente política

Jefes y Coordinadores

- Aprobar o implementar los controles de seguridad de la información que se hayan definido para garantizar la confidencialidad, integridad y disponibilidad de la información.

Colaboradores

- Cumplir con las políticas, procedimientos y normatividad vigente relacionada con el Sistema de Gestión de Seguridad de la Información – SGSI
- Reportar situaciones, eventos o incidentes que afecten la seguridad de la información.

4. DESCRIPCIÓN DE POLÍTICA

La información perteneciente a ALSERTEC S.A.S. debe protegerse de acuerdo con su valor e importancia. Deben emplearse medidas de seguridad sin importar cómo se guarda, se procesa o se transmite la información. Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo, entre otras medidas de protección.

Los datos y los equipos tecnológicos son recursos importantes y vitales de la Compañía. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén debidamente protegidos de las amenazas y riesgos.

La finalidad de las políticas de seguridad de la información es proporcionar instrucciones específicas sobre cómo mantener más seguros los computadores y la información.

La violación de dichas políticas puede acarrear medidas disciplinarias establecidas.

A continuación, se establecen los lineamientos principales de seguridad informatica a tener en cuenta por todos los usuarios de ALSERTEC S.A.S., al finalizar la lectura de la presente política o un resumen de esta, los usuarios deberán registrar su firma física o digital como evidencia de conocimiento y cumplimiento

4.1. DISPOSITIVOS MÓVILES Y TELETRABAJO

4.1.1. DISPOSITIVOS MÓVILES

- No se encuentra permitido el almacenamiento información personal en los dispositivos móviles corporativos de ALSERTEC S.A.S.

- En caso de pérdida o hurto de un dispositivo móvil corporativo, se debe notificar de manera inmediata a Gestión Administrativa Alsertec para que a su vez este gestione ante TI la des habilitación las cuentas de usuario respectivas y evitar accesos no autorizados a la información.

- Todos los dispositivos móviles que contengan información de la compañía deberán cumplir políticas de seguridad tales contraseña, antivirus y actualizaciones de software.

4.1.2. TELETRABAJO

- Los usuarios que por razones propias del negocio se encuentren autorizadas para realizar teletrabajo, serán responsables por la protección física del equipo asignado, uso no autorizado, hurto, pérdida o daño.

- Las conexiones que se realicen desde y hacia los equipos destinados para teletrabajo, se deben hacer a través de VPN con el fin de asegurar los activos de información de la compañía.

4.2. SEGURIDAD DE LA INFORMACIÓN EN RECURSOS HUMANOS

4.2.1. ANTES DE EMPLEARLOS

- Todas las contrataciones de personal requerirán una verificación de antecedentes de todos los aspirantes finales. Si el aspirante es aceptado para ser contratado, entonces la administración sigue el proceso de contratación establecido por Talento Humano.

- La información personal de los candidatos, incluyendo la de su proceso de selección y contratación, se clasificará como CONFIDENCIAL y se protegerá en concordancia.

- Durante el proceso de contratación los colaboradores deben ser informados de las políticas de la compañía, entre ellas la presente política de seguridad de la información.

4.2.2. DURANTE EL EMPLEO

- Todos los colaboradores deben cumplir con las políticas de seguridad de la información mientras se encuentren laborando para ALSERTEC S.A.S.

- Todos los colaboradores deben recibir a su ingreso a la Compañía y durante su permanencia, (inducciones y reinducciones) temas de seguridad de la información, así como dejar constancia del conocimiento respecto a las políticas y procedimientos de seguridad de la información que sean de su inherencia.

- La compañía impone sanciones disciplinarias o terminación del contrato de aquellos colaboradores que no cumplan con las políticas de seguridad de la información, que violen los términos de un acuerdo de confidencialidad o que participen en un acto de mala conducta.

4.2.3. TERMINACION O CAMBIO DE TRABAJO

- Ante una terminación de contrato laboral, el colaborador debe hacer entrega formal de los activos de información que le fueron asignados por la Compañía para sus actividades laborales, tales como información física impresa y lógica que se encuentre en medios de almacenamiento externos como pendrive, discos duros, equipos de cómputo, servidores, bases de datos, entre otros.

- El acceso de los colaboradores a la información, sistemas de cómputo e instalaciones deberá ser revocado oportunamente al momento de su retiro o si los colaboradores son transferidos o cambian de posición. Esto incluye derechos de acceso lógico y físico, incluyendo, pero sin limitarse a, la revocación inmediata del acceso a la red, aplicaciones, correo y tarjeta de acceso a las instalaciones.

4.3. GESTIÓN DE ACTIVOS - RESPONSABILIDADES Y LINEAMIENTOS DEL MANEJO DE LA INFORMACIÓN SENSIBLE Y CONFIDENCIAL

4.3.1. RESPONSABILIDAD POR LOS ACTIVOS

- Los líderes de los procesos de ALSERTEC S.A.S. son los propietarios de los activos de información de su respectivo proceso.

- Los propietarios de los activos de información son responsables de mantener actualizado periódicamente el inventario de activos de información con su respectiva valoración y clasificación.

4.3.2. CLASIFICACIÓN DE LA INFORMACIÓN

- Todos los activos de información de ALSERTEC S.A.S. deben estar identificados, clasificados y valorados acorde a la documentación de activos definida por la compañía.

- El tratamiento, uso y utilización de los activos de información de ALSERTEC S.A.S., debe ser acorde a su nivel de clasificación.

- Ningún colaborador, tercero o proveedor puede divulgar a personas no autorizadas información de la compañía que contenga datos privados, semiprivados o sensibles.

- Todos los colaboradores, terceros o proveedores son responsables del correcto uso, conservación y transferencia de los activos de información.

- Todos los activos de información de ALSERTEC S.A.S. deben cumplir con el periodo de almacenamiento de acuerdo con los requerimientos legales o misionales y una vez se cumpla este periodo, se tendrá en cuenta la disposición final del activo cumpliendo con los tiempos de retención establecidos.

- Los activos de información que pertenecen a ALSERTEC S.A.S. y el uso de estos debe emplearse exclusivamente para la realización de las actividades y obligaciones contratadas y no para otro fin.

- Cualquier usuario de los recursos tecnológicos de ALSERTEC S.A.S. que sea identificado haciendo uso inadecuado de los activos de información que ocasionen fuga, daño o divulgación de la información institucional, será notificado oficialmente acerca de la gravedad del hecho, recibiendo un llamado de atención o amonestación proporcional al mismo. Dependiendo de la gravedad de la falta o incidente de seguridad, ALSERTEC S.A.S. adelantará las acciones disciplinarias o legales correspondientes.

- Todo activo de información debe contar con los controles asociados al valor que este posea para la Compañía.

- Ningún colaborador o tercero puede divulgar información confidencial de la Compañía a personas no autorizadas.

- La información física y los dispositivos de almacenamiento que contienen información reservada, deben destruirse físicamente o sobrescribir cuando ya no sean requeridos por el negocio, de tal forma que los datos no se puedan recuperar.

- Los controles para la custodia de información reservada y confidencial deben estar acordes al nivel de su importancia para el negocio y el cumplimiento de dichos controles será una responsabilidad compartida entre el custodio y dueño de la información.

La siguiente clasificación aplica para los activos de información de la compañía:

Tabla 1. Clasificación de la Información

VALOR	CONFIDENCIALIDAD		INTEGRIDAD	DISPONIBILDAD
ALTO	**INFORMACIÓN RESERVADA**	La pérdida de confidencialidad de la información puede conllevar un impacto negativo alto de índole legal, operativa, de pérdida de imagen o económica. Solo puede ser conocida por procesos autorizados. **Por regla general** la información pública reservada corresponde a la determinada en el **art. 19 de la ley 1712 de 2014:** • Defensa y seguridad nacional • Seguridad pública • Relaciones internacionales, • Prevención, investigación y persecución de los delitos y las faltas disciplinarias • El debido proceso y la igualdad de las partes en proceso judiciales • La administración efectiva de la justicia	La pérdida de exactitud y completitud de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a Terceros. (Ej.: Procuraduría, Defensoría del Pueblo, Contraloría, Ministerios, Fiscalía, entre otros)	La no disponibilidad del activo y/o de los sistemas de información puede conllevar un impacto negativo a Terceros. (Ej.: Procuraduría, Defensoría del Pueblo, Contraloría, Ministerios, Fiscalía, entre otros) Impacto alto en el tiempo de ejecución del proceso mayor a 2 días

VALOR	CONFIDENCIALIDAD		INTEGRIDAD	DISPONIBILDAD
		• La estabilidad macroeconómica y financiera del país • Los derechos de la infancia y la adolescencia • La salud pública • Se exceptúan también los documentos que contengan opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos. Así mismo, frente a activos que **excepcionalmente** requieran un tratamiento especial por no caber en ninguna de las causales descritas o requerir una confidencialidad mayor, se deberá recurrir a criterios de interpretación de acuerdo con su impacto negativo de índole legal o económico por pérdida de confidencialidad, por retrasar sus funciones, o generar pérdidas de imagen severas ante Terceros (Ej.: Procuraduría, Defensoría del Pueblo, Contraloría, Ministerios, Fiscalía, entre otros)		

VALOR	CONFIDENCIALIDAD		INTEGRIDAD	DISPONIBILDAD
MEDIO	**INFORMACIÓN CONFIDENCIAL**	La pérdida de confidencialidad de la información puede conllevar un impacto negativo medio de índole legal, operativa, de pérdida de imagen o económica. Puede ser conocida por todos los procesos de la compañía, pero exclusivamente para realizar labores propias de la compañía **Por regla general** la información pública clasificada corresponde a la determinada en el **art. 18 de la ley 1712 de 2014**: • Derecho a la intimidad bajo las limitaciones propias que impone la condición de servidor público (datos personales, datos financieros, datos Sensibles) • El derecho a la vida, la salud y la seguridad (historia clínica) • Los secretos comerciales, industriales y profesionales Así mismo, frente a activos que **excepcionalmente** requieran un tratamiento especial por no caber en ninguna de las causales descritas o requerir una	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a los procesos internos de la Compañía. (Alta Dirección, Oficina Control Interno, Oficina Jurídica, Talento Humano, Operaciones, Financiera)	La no disponibilidad de la información, del activo y/o de los sistemas de información puede conllevar un impacto negativo a los procesos internos de la Compañía. (Alta Dirección, Oficina Control Interno, Oficina Jurídica, Talento Humano, Operaciones, Financiera) Impacto medio en el tiempo de ejecución del proceso entre 1 y 2 días seguidos

VALOR	CONFIDENCIALIDAD		INTEGRIDAD	DISPONIBILDAD
		confidencialidad mayor, se deberá recurrir a criterios de interpretación de acuerdo con su impacto negativo de índole legal o económico por pérdida de confidencialidad, por retrasar sus funciones, o generar pérdidas de imagen severas al interior de los **procesos de la compañía.** (Alta Dirección, Oficina Control Interno, Oficina Jurídica, Talento Humano, Operaciones, Financiera)		
BAJA	**INFORMACIÓN PÚBLICA**	La pérdida de confidencialidad de la información puede conllevar un impacto negativo bajo. Información pública es toda información en posesión, custodia o bajo el control de las entidades obligadas, siempre y cuando su contenido no se incluya en alguna de las excepciones mencionadas en los artículos 18 y 19 de la Ley 1712 de 2014.	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo. A nivel interno del proceso. (jefe de la Dependencia, equipo de trabajo, supervisor)	La no disponibilidad de la información, del activo y/o de los sistemas de información puede conllevar un impacto negativo: A nivel interno del proceso (jefe de la Dependencia, equipo de trabajo, supervisor) Impacto bajo en el tiempo de ejecución de proceso entre 1 y 8 horas seguidas.

4.3.3. MANEJO DE MEDIOS – MANEJO ADECUADO DE DISPOSITIVOS EXTRAÍBLES USB

- Se encuentra prohibido el uso de dispositivos extraíbles para ingreso y salida de la información, las unidades removibles se habilitarán únicamente cuando exista una necesidad justificada para hacerlo. Los medios removibles deben ser cifrados cuando contengan información reservada o confidencial.

- Toda excepción de uso de USB los usuarios deberán gestionarlas a través de la herramienta de soporte de mesa de ayuda y deberán estar autorizadas por el Analista Administrativo.

- Los medios de almacenamiento (Discos duros, cintas magnéticas, etc.) de datos se deben proteger adecuadamente contra daños, pérdida o robo.

- Cuando ya no se necesiten, los medios de almacenamiento (Discos duros, USB, cintas magnéticas, medios ópticos de almacenamiento) se deben eliminar de forma segura.

- Los medios de almacenamiento (Discos duros, cintas magnéticas, etc.) que contengan información reservada o confidencial de la Compañía, que se vaya a reusar, se deben borrar de forma segura antes de volverlos a utilizar.

4.4. CONTROL DE ACCESO INFORMACIÓN DEL NEGOCIO

- Los dueños de los activos de información (líderes de proceso) deben definir los requerimientos del negocio para controlar el acceso a los activos teniendo en cuenta:
    - Los requerimientos de seguridad de la información (distinguiendo requerimientos obligatorios, requerimientos recomendados, opciones o condicionales)
    - Las obligaciones legales y contractuales relevantes en relación con la protección de la información
    - La segregación de las obligaciones, cuando sea aplicable.

- Los dueños de los activos de información (líderes de proceso) deben definir revisar rutinariamente al menos una vez al año los accesos a los activos de información de su proceso.

4.4.1. GESTION DE ACCESO DE USUARIOS

- El acceso a las redes, los sistemas y las aplicaciones debe ser otorgado con base en las necesidades del negocio, los requerimientos de seguridad y el menor privilegio.

- No deben existir usuarios privilegiados genéricos o por defecto (de fábrica). La clave será administrada por al menos dos colaboradores autorizados y custodiada en un entorno seguro, cada vez que sea usada deberá ser cambiada.

- Los usuarios privilegiados únicamente se asignarán, y será utilizados por individuos autorizados para propósitos legítimos de negocio. Los usuarios privilegiados no se utilizarán para actividades de rutina.

- Las contraseñas asociadas a las cuentas de servicios son las únicas permitidas para que nunca expiren, dichas cuentas deberán ser identificadas, inventariadas y describir la función que están realizando.

- Las cuentas de usuario privilegiado sólo deben ser otorgadas al personal de nivel técnico / funcional apropiado y únicamente para el cumplimiento de sus funciones, para ello se deberá segregar las funciones, estableciendo qué permisos concretos tendrán los usuarios autorizados en el sistema, asegurándose de que

éstos sean los mínimos estrictamente necesarios (garantizando así los principios de mínimo privilegio y necesidad de saber).

- Los colaboradores, proveedores y terceros que posean acceso a la plataforma tecnológica de ALSERTEC S.A.S. deben acogerse a los lineamientos emitidos por TI para la configuración de contraseñas implantadas.

- Se establece el uso de contraseñas individuales para determinar la responsabilidad de su administración.

- Los colaboradores, terceros y proveedores antes de contar con acceso lógico por primera vez a la red de ALSERTEC S.A.S., deben realizar la solicitud por el medio de la herramienta de soporte para la creación de las respectivas cuentas de usuario, detallando claramente el objetivo del acceso y permisos de uso solicitados.

- Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario requeridos y realizar el proceso de autorización a dichos recursos con quien corresponda de acuerdo con los perfiles establecidos.

- Los propietarios de los activos de información deben verificar y actualizar periódicamente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

- Por ningún motivo las credenciales de acceso de personal retirado deben ser utilizadas, teniendo en cuenta que todo acceso es personal e intransferible.

- Está prohibido almacenar en texto plano las credenciales de acceso, estas deben ser almacenadas en bóvedas seguras provistas por la compañía.

- Para la creación y asignación de carpetas que permite almacenar información de ALSERTEC S.A.S., se debe tener en cuenta lo siguiente:
  - Por defecto, **NO** otorgar permisos de control total
  - Se deben limitar los permisos de crear, eliminar, ejecutar, leer y modificar de acuerdo con el rol desempeñado y a los accesos solicitados.

4.4.2. USO DE CONTRASEÑAS

- Las cuentas de usuario, contraseñas o cualquier otro mecanismo de autenticación usado y/o asignado para acceder a los servicios de red, dominio, correo, equipos y sistemas de información, deben ser tratados como información confidencial de ALSERTEC S.A.S., por lo cual no se deben divulgar, publicar ni compartir con ninguna persona.

- Se deben cambiar las contraseñas de acceso que se encuentran predeterminadas y establecidas por el fabricante y/o proveedores de servicios una vez instalado, configurado y recibido por ALSERTEC S.A.S. el software y hardware.

- Está prohibido almacenar en texto plano las credenciales de acceso, estas deben ser almacenadas en bóvedas seguras provistas por la compañía.

- Es responsabilidad única y exclusiva del usuario el manejo, uso adecuado y resguardo de las cuentas de usuario y contraseñas asignadas.

- Las contraseñas asociadas a las cuentas de servicios son las únicas permitidas para que nunca expiren, dichas cuentas deberán ser identificadas, inventariadas y describir la función que están realizando.

- Se debe utilizar diferentes contraseñas en los diferentes sistemas de información.

- Las contraseñas de acceso al dominio:
    - Son información confidencial
    - Fáciles de memorizar, pero difíciles de adivinar
    - Se cambiarán inmediatamente si existe una posibilidad significativa de que haya comprometido un sistema o la contraseña.
    - Longitud mínima de contraseña es de 10 caracteres
    - Expiraran máximo cada 60 días
    - Deben contener números, letras, mayúsculas y caracteres especiales (caracteres no alfanuméricos)
    - Las ultimas 7 contraseñas de un usuario no se podrán utilizar.
    - Después de 4 intentos incorrectos de la contraseña sobre la una cuenta, el acceso será bloqueado.
    - No deben contener palabras relacionadas con la información personal como nombre, apellido, cedula, nombre de la empresa, teléfono, etc.

4.5. SEGURIDAD FISICA DE LA INFORMACION Y DEL ENTORNO

4.5.1. AREAS SEGURAS - CONTROL DE ACCESO EQUIPOS DE CÓMPUTO

- Todas las puertas de acceso a las instalaciones de ALSERTEC S.A.S. que utilizan sistemas de control de acceso deben permanecer cerradas y es responsabilidad de todos los colaboradores, terceros y proveedores autorizados evitar que las puertas se dejen abiertas.

- Todos los funcionarios, colaboradores, terceros y visitantes deben portar el carné en un lugar visible mientras permanezcan dentro de las instalaciones, en caso de pérdida del carné y/o credencial de acceso se debe reportar a la mayor brevedad posible a Seguridad Física.

- Los ingresos y retiros del personal interno y externo a las instalaciones de ALSERTEC S.A.S. deben ser registrados.

- Todo espacio físico donde resida la infraestructura tecnológica necesaria para la operación de ALSERTEC S.A.S., debe contar con mecanismos de acceso para la restricción de personal no autorizado como son los centros de cómputo, centros de cableado, entre otros.

- Deben existir controles ambientales operando eficientemente en las áreas seguras en donde se encuentre la infraestructura tecnológica necesaria para la operación de ALSERTEC S.A.S. como centros de cómputo, centros de cableado, entre otro.

- Todo ingreso de personas a los centros de computo de la Compañía, debe quedar registrado en la bitácora de ingreso de visitantes incluyendo objetivo del ingreso hora de entrada y salida; los visitantes siempre deberán estar acompañados por un colaborador de TI durante su visita en el centro de cómputo o centro de cableado.

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por TI de acuerdo con las actividades a ejecutar.

- Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por un colaborador de T. El personal de limpieza se debe capacitar acerca de las precauciones mínimas a seguir en dichas instalaciones.

4.5.2. EQUIPOS

4.5.3. EQUIPOS – MANEJO ADECUADO DEL HARDWARE

- Los componentes, equipos de procesamiento de información, comunicaciones y archivos importantes para ALSERTEC S.A.S., deben estar ubicados en áreas de acceso restringido a personal no autorizado, empleando mecanismos de control como tarjetas de proximidad, esquemas biométricos, cerraduras, entre otros. Asimismo, deben contar con cámaras de video que permitan grabar el flujo de personas que entran y sales de dichos espacios.

- En caso de pérdida de un equipo tecnológico de propiedad de ALSERTEC S.A.S. se debe informar inmediatamente a la Gerencia de TI por medio de notificación a la mesa de servicio, el usuario responsable del bien debe poner la denuncia ante las autoridades competentes y debe hacer llega copia de esta a la Gerencia de TI de ALSERTEC S.A.S.

- Cuando los equipos portátiles se encuentren desatendidos deben estar asegurados con una guaya, dentro o fuera de las instalaciones de ALSERTEC S.A.S.

- Los funcionarios de ALSERTEC S.A.S. y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.

- Al imprimir información clasificada o confidencial esta debe ser retirada de las impresoras inmediatamente. Así mismo, no se debe reutilizar papel que contenga información clasificada o confidencial.

- En horario no hábil o cuando los lugares de trabajo se encuentren desatendidos, los usuarios deben dejar la información clasificada o confidencial protegida bajo llave.

4.6. SEGURIDAD EN LAS OPERACIONES

4.6.1. PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

- Toda solicitud de cambios en los equipos de cómputo y de procesamiento de ALSERTEC S.A.S., se debe realizar siguiendo el procedimiento de gestión de cambios, con el fin de asegurar la planeación del cambio y evitar una afectación a la disponibilidad, integridad o confidencialidad de la información.

- Se debe llevar una trazabilidad de los controles de cambios solicitados en la infraestructura tecnológica (Firewall, servidores, etc.).

- Los cambios sobre sistemas de información deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa.

- Antes de la implementación de un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información, estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.

- Se debe disponer de un plan roll-back en la implementación de un cambio, que incluya las actividades a seguir para abortar los cambios y volver al estado anterior.

- TI debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

4.6.2. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

- Todos los equipos de cómputo en los que se almacene o procese información de ALSERTEC S.A.S. deben tener instalado y actualizado el software antivirus corporativo.

4.6.3. COPIAS DE RESPALDO

- Los dueños de los activos de información son los responsables de definir qué información requiere ser respaldada y de definir el periodo de retención de los respaldos, en función de los requerimientos de los procesos.

- Toda la información de la compañía debe ser almacenada en OneDrive o SharePoint de acuerdo a la necesidad y estas serán las herramientas corporativas de Backup de usuarios.

- Los usuarios deben realizar el respaldo de su información laboral utilizando OneDrive o SharePoint.

- No se debe almacenar información personal en los equipos y las herramientas provistas por la compañía.

- Se debe realizar copias de respaldo de los eventos de auditoria y en caso de que ocurra un incidente de seguridad de la información deben estar disponibles.

4.6.4. MANEJO ADECUADO DE SOFTWARE

- Los usuarios no pueden realizar instalación de software en los computadores, salvo con autorización expresa de TI.

- La instalación de software se encuentra bajo la responsabilidad de TI.

- La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considerada como una violación grave a las Políticas de Seguridad de la Información.

- Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados a través de la mesa de ayuda de TI con su correspondiente justificación.

- Los usuarios no podrán efectuar ninguna de las siguientes labores:
    - Instalar software en cual1quier equipo de ALSERTEC S.A.S.; esto incluye el Software Open Source también denominado Software libre, los Freeware y Shareware con licenciamiento de uso comercial.
    - Descargar software de Internet u otro servicio en línea en cualquier equipo de ALSERTEC S.A.S.
    - Modificar, revisar, transformar o adaptar cualquier software propiedad de ALSERTEC S.A.S.
    - Descompilar o realizar ingeniería inversa en cualquier software de propiedad de ALSERTEC S.A.S.
    - Copiar o distribuir cualquier software de propiedad de ALSERTEC S.A.S.
    - Utilizar servicios freeware del estilo WeTransfer o aquellos que no hayan sido previamente autorizados

- Todas las adquisiciones e implementaciones de software deben estar revisadas y aprobadas por TI y por el líder de proceso.

- Todo el software de ALSERTEC S.A.S. debe estar protegido por derechos de autor.

4.7. SEGURIDAD EN LAS COMUNICACIONES

4.7.1. GESTIÓN DE LA SEGURIDAD DE LAS REDES

- Todo equipo de cómputo que esté o sea conectado a la Red de ALSERTEC S.A.S. debe sujetarse a los procedimientos de acceso establecidos por TI.

- Para propósitos de seguridad y mantenimiento de la red, personal autorizado de TI puede monitorear los equipos, sistemas y tráfico de red en cualquier momento.

- Se prohíbe la suplantación y modificación de la identidad de los paquetes de datos y mensajes: modificación de la cabecera de los paquetes TCP/IP, mensajes de correo electrónico entre otros.

4.7.2. USO ADECUADO DEL INTERNET

- El acceso a Internet estará reservado para todos aquellos funcionarios que lo requieran según sus funciones de trabajo, de acuerdo con las necesidades del negocio y para uso laboral exclusivamente.

- La compañía restringirá el acceso a sitios de internet que por alguna circunstancia vayan en contra de sus políticas institucionales y del negocio, políticas de seguridad y buenas prácticas adoptadas tales como consultar material ilegal, de acoso, difamatorio, abusivo, amenazador, nocivo, vulgar, obsceno o de cualquier otra manera censurable.

- No está permitido hacer uso de los recursos de ALSERTEC S.A.S. tales como redes para acceder a redes sociales, servicios interactivos de almacenamiento masivo, streaming de videos, páginas de mensajería instantánea y servicios de correo electrónico personal.

- Se prohíbe toda publicación o intercambio de información reservada y clasificada de ALSERTEC S.A.S. a través de cualquier medio físico, magnético o electrónico sin el consentimiento y la respectiva autorización del responsable de la información y en cumplimiento de los controles establecidos para la protección de la información.

- Se prohíbe la publicación de información reservada y clasificada mediante las redes sociales.

- La información consultada en cualquier horario de trabajo a través de Internet debe apoyar directamente las funciones relacionadas con el campo de responsabilidad laboral del usuario y/o servir como herramienta para desempeñar sus funciones.

4.7.3. MANEJO ADECUADO DEL CORREO ELECTRONICO

- El uso de cada cuenta de correo es de carácter personal e intransferible.

- El servicio de correo electrónico se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales a desarrollar en ALSERTEC S.A.S. y no se debe utilizar para otros fines.

- El correo electrónico se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos a la operación, la red, los sistemas de información e imagen de la compañía.

- Toda la información contenida en los buzones de correo es de propiedad de la compañía y puede ser examinada en cualquier momento por el personal autorizado para dicha actividad.

- Cada usuario debe asegurar que el reenvió de correos electrónicos a la dirección de destino es correcta, de tal manera que garantice que la información está siendo enviada a los destinarios correctos. En el caso de tener listas de distribución, estas deben ser depuradas de manera permanente.

- Ningún colaborador o tercero debe suscribirse en boletines, publicidad u otros que no tengan relación con las actividades y obligaciones laborales.

- Los colaboradores y terceros no deben responder correos electrónicos donde soliciten información de datos personales, financieros con fines de sorteos, ofertas labores y comerciales, ayudas humanitarias, entre otros.

- Se debe garantizar el cumplimiento de los controles de seguridad para él envío y tratamiento de información confidencial por correo electrónico.

- No se debe enviar o intercambiar mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, actividades ilegales, información terrorista, información de datos personales sensibles, cadenas de cualquier tipo, racista, entre otros.

- Se encuentra prohibido adulterar los correos electrónicos.

- El mal uso de los medios electrónicos estará sujeto a investigaciones de carácter disciplinario o legal.

- Es responsabilidad de los usuarios reportar a TI los incidentes de seguridad relacionados con los medios electrónicos.

- No se permite crear reglas de reenvío a correos externos.

- La autenticación al correo electrónico de usuarios con licencia E3 o superior deberá realizarse **SIEMPRE** mediante autenticación de doble factor.

- Se prohíbe el uso no autorizado o adulteración de encabezados de correo electrónico.

- Se prohíbe cualquier forma de acoso vía correo, teléfono, u otro mecanismo de comunicaciones de la compañía.

- Se prohíbe a los colaboradores utilizar sistemas de correo electrónico de terceros o cuentas personales (Yahoo!, Gmail, Hotmail, etc.) para realizar comunicaciones en nombre de ALSERTEC S.A.S., crear o ejecutar cualquier transacción, almacenar o retener correos electrónicos de ALSERTEC S.A.S. entre otros.

4.7.4. MANEJO ADECUADO DE LAS INTERCONEXIONES EXTERNAS

- Toda conexión remota a la red de ALSERTEC S.A.S. debe ser a través de canales seguros como VPNs, canales dedicados o servicios web. Éstos deben solicitar autenticación para establecer la conexión remota a la red con el fin de prevenir accesos no autorizados.

- Se permite el uso de VPN para usuarios que por actividades propias de la Compañía requieran acceso a los sistemas de información de forma remota.

- Un colaborador, contratista o tercero vinculado a ALSERTEC S.A.S. con autorización de acceso a los sistemas de información a través de VPNs, deberá hacer uso correcto de los activos de información.

- Toda autorización para conexiones remotas por parte de proveedores debe tener una vigencia, una contraseña de acceso y una cuenta de usuario que deberá ser bloqueada una vez finalizada las labores para las cuales se crea.

- Toda conexión remota sea de colaboradores o proveedores, será monitoreada y podrá ser bloqueada en caso de identificar situaciones inusuales respecto al uso de la cuenta y el acceso a los activos de información.

- Los puertos utilizados para conexiones externas deben estar controlados de forma segura.

- Todas las conexiones que se originan desde redes o equipos externo a la red de ALSERTEC S.A.S., deben limitarse únicamente a los servicios, servidores o aplicaciones necesarias. Si es posible, estos servidores destino deben estar física o lógicamente separados de la red interna de ALSERTEC S.A.S.

- No se encuentra permitidas conexiones externas directas a los servidores.

4.8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- Se deben implementar controles adecuados en las aplicaciones para garantizar que los datos sean completos, precisos e íntegros, satisfaciendo los requerimientos de seguridad de la información.

- Se deben identificar los riesgos asociados para nuevos desarrollos o proyectos, con el fin de establecer los controles para el aseguramiento de la información.

- Todas las aplicaciones deben pasar por un proceso de pruebas y aceptación en un ambiente dedicado para tal fin antes de ser liberados a producción.

- No está permitido el acceso a personal no autorizado a editores, compiladores o cualquier otro tipo de utilitarios que estén asociados al ambiente productivo, cuando no sean indispensables para el funcionamiento de este.

- Todo el software adquirido, instalado/implementado en la infraestructura de ALSERTEC S.A.S. debe estar previamente validado y aprobado por TI.

4.9. PROVEEDORES

- En todos los Contratos o Acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de ALSERTEC S.A.S. se deben establecer Acuerdos de Confidencialidad sobre el manejo de la información.

- Los Acuerdos de Confidencialidad de la información deben hacer parte integral de los contratos o documentos que legalicen la relación con los proveedores.

- Los Proveedores, contratistas o terceros vinculados a ALSERTEC S.A.S. deben garantizar que el intercambio de información desde y hacia ALSERTEC S.A.S. cumple con las exigencias que éste defina con base en las leyes y regulaciones vigentes, así como también las políticas de seguridad de la información.

- El acceso de los proveedores a la información de ALSERTEC S.A.S. estará sujeto a la evaluación de riesgos realizada por el responsable del contrato.

- ALSERTEC S.A.S. se reserva el derecho de monitorear, registrar el uso, restringir, suspender o revocar los derechos de acceso a la red y la información de ALSERTEC S.A.S.

4.10. INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- Todos los empleados y contratistas vinculados a ALSERTEC S.A.S. deben estar conscientes de los procedimientos y su importancia para reportar incidentes de seguridad.

- Los colaboradores que utilicen servicios de información de ALSERTEC S.A.S., deben reportar cualquier sospecha de amenazas o debilidades en los sistemas o servicios tecnológicos. Dichos reportes deben ser comunicados al área de Seguridad de la Información.

- Se debe reportar al área de Seguridad de la información, cualquier incidente de seguridad que pueda comprometer la confidencialidad, integridad y/o disponibilidad de los activos de información de ALSERTEC S.A.S., siguiendo el procedimiento de notificación de incidentes establecido.

4.11. CONTINUIDAD DEL NEGOCIO

- Los Líderes de cada proceso de ALSERTEC S.A.S. deben identificar y generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información.

- Los planes de continuidad del negocio deben ser documentados, probados y evaluados por lo menos una vez al año para verificar su funcionamiento adecuado.

- Los planes de continuidad deberán estar ubicados en un lugar seguro dentro de Alsertec S.A.S. De igual forma debe ser de conocimiento de todos los colaboradores y distribuido según su inherencia a toda la estructura de Alsertec S.A.S.

- Los terceros contratados deben contar con planes de continuidad debidamente documentados y probados, con el fin de dar continuidad a las operaciones críticas del negocio.

4.12. CUMPLIMIENTO

- Todos los Colaboradores y Terceros están obligados a ceder a ALSERTEC S.A.S. los derechos exclusivos de propiedad literaria, licencias, invenciones, u otra propiedad intelectual que ellos creen o desarrollen durante su periodo laboral con las compañías. En el caso de aplicaciones de terceros, este aspecto se regirá por las condiciones y cláusulas establecidas en el contrato de adquisición de productos y/o servicios, con la finalidad de prevenir cualquier disputa respecto a la propiedad del software, licencias, entre otros, una vez que el proyecto sea completado.

- ALSERTEC S.A.S. tiene propiedad legal de la información Corporativa almacenada, enviada y compartida en todos sus computadores, sistemas de información y comunicación que hayan sido transmitidos por medio de estos recursos, por lo cual se reserva el derecho de acceder a esta información sin autorización del autor o usuario del recurso, así como también se reserva el derecho de disponer de toda la información que cualquier empleado haya colocado en los medios de comunicación existentes de ALSERTEC S.A.S..

- Los contratistas y terceras partes deben cumplir con las disposiciones establecidas por la Legislación Colombiana vigente asociados a la de protección de datos personales, propiedad intelectual y seguridad de la información.

4.13. SANCIONES – MEDIDAS DISCIPLINARIAS

- La política de la Compañía impone sanciones disciplinarias o terminación del contrato de aquellos colaboradores que no cumplan con las políticas establecidas, que violen los términos de un acuerdo de confidencialidad o que participen en cualquier otro acto de mala conducta que sea inconsciente con el comportamiento esperado de todo el personal que trabaja en ALSERTEC S.A.S.

- El incumplimiento de las políticas, lineamientos y procedimientos establecidos de Seguridad de la Información podrá ocasionar a los colaboradores, proveedores o clientes, amonestaciones, suspensiones, sanciones disciplinarias o terminación definitiva del contrato entre otras, de acuerdo con el reglamento interno o el clausulado establecido contractualmente.

5. DOCUMENTOS REFERENCIADOS

Ley 1273 de 2009 “de la protección de la información y de los datos”
Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”
Norma Internacional **ISO / IEC 27001** - seguridad de la información
Resolución 67 DE 2016 - Capitulo 8. Seguridad en tecnología de la información.

6. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio	Cargo responsable del Cambio