LINEAMIENTOS DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

LA REFORESTADORA INTEGRAL DE ANTIOQUIA S.A.

REFORESTADORA
INTEGRAL DE ANTIOQUIA S.A.
NIT: 811.038.424-6

Contenido

1. OBJETIVO 3
2. ALCANCE 3
3. GLOSARIO 3
4. LINEAMIENTOS 7

PUNTO 1: LA SEGURIDAD DE LA INFORMACIÓN: 7
PUNTO 2: CLASIFICACIÓN Y CONTROL DE ACTIVOS DE LA INFORMACIÓN: 7
PUNTO 3: CLASIFICACIÓN DE LA INFORMACIÓN: 8
PUNTO 4: INTERCAMBIO DE INFORMACIÓN: 8
PUNTO 5: DE LA PRESTACIÓN DE SERVICIOS DE TERCEROS: 9
PUNTO 6: PROTECCIÓN CONTRA VIRUS – MALWARE – ADWARE – BONET – RANSOMWARE - ETC: 9
PUNTO 7: SERVICIOS INFORMÁTICOS EN LA RED: 10
PUNTO 8: USO DE CUENTAS DE USUARIO: 12
PUNTO 9: MONITOREO DEL USO DE LOS ACTIVOS: 13
PUNTO 10: USO DE INTERNET: 13
PUNTO 11: USO DE CORREO ELECTRÓNICO Y MENSAJERÍA: 15
PUNTO 12: USO DEL SOFTWARE: 18
PUNTO 13: REDES SOCIALES: 18
PUNTO 14: RECURSOS COMPARTIDOS: 19
PUNTO 15: USO DE PORTÁTILES Y DISPOSITIVOS MÓVILES: 20
PUNTO 16: ACCESO A EQUIPOS DISTINTOS A LOS DESIGNADOS: 21
PUNTO 17: TRATAMIENTO Y GESTIÓN DE EL RIESGO: 21
PUNTO 18: SEGURIDAD DE LA INFORMACIÓN EN TALENTO HUMANO: 22
PUNTO 19: SEGURIDAD FISICA Y DEL ENTORNO: 22
PUNTO 20: CONTROL DE ACCESO A LA INFORMACIÓN: 23
PUNTO 21: GESTIÓN DE CONTRASEÑAS Y USUARIOS: 25
PUNTO 22: GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: 26
PUNTO 23: GESTIÓN DE INCIDENTES DE TELECOMUNICCIONES E INFRAESTRUCTURA TIC: 27
PUNTO 23: GESTIÓN DEL CAMBIO: 27
PUNTO 24: COPIAS DE SEGURIDAD: 28
PUNTO 25: GESTIÓN DE LA SEGURIDAD EN LAS REDES: 28
PUNTO 26: SERVICIOS DE COMERCIO ELECTRONICO: 29
PUNTO 27: MONITOREO DEL USO DEL SISTEMA. 29
PUNTO 28: TRATAMIENTO DE MEDIOS DE INFORMACIÓN: 29
PUNTO 29: CUMPLIMIENTO Y NORMATIVA LEGAL: 29

5. EXCEPCIONES.....31

1. OBJETIVO

Definir detalladamente cómo se debe implementar la Política de Seguridad de la información de La Reforestadora Integral de Antioquia S.A., que se alcanzan con la aplicación de estos controles de Seguridad de la Información, para gestionar un nivel de riesgo aceptable.

Los lineamientos de la política de seguridad de la información deben ser revisados como mínimo una vez al año o cuando sea necesario.

2. ALCANCE

Los lineamientos enumerados en el presente documento aplican a todos los empleados, directivas, agentes externos, colaboradores, proveedores, vendedores, contratistas, terceras partes, que ingresen física o remotamente al perímetro de seguridad de la empresa y accedan a los activos de información propiedad de La Reforestadora Integral de Antioquia S.A..

3. GLOSARIO

Activo crítico: *Instalaciones, sistemas o equipo eléctrico que, si es destruido, degradado o puesto indisponible, afecta la confiablidad u operatividad del sistema eléctrico. Acorde con las recomendaciones del Comité Tecnológico del CNO para la definición de activos críticos que comprometan la seguridad de operación del SIN.*

Activo: *cualquier cosa que tenga valor para la empresa.*

Amenaza: *causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema o a la empresa.*

Confidencialidad: *propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.*

Comité de Riesgos de Tecnología: *el Comité de Riesgos de Tecnología debe establecer los criterios de dirección y control, que permitan implantar los mecanismos más apropiados de protección de la información de CELSIA, aplicando los principios de confidencialidad, integridad y disponibilidad de la misma y de los recursos informáticos o de otra índole que la soportan, acorde con la planeación estratégica de la empresa.*

Derecho de autor: *Protección legal que cubre las actividades y trabajos de creación de productos de cualquier tipo que sean plasmados de forma tangible o material de conformidad con el marco aplicable en la materia. Las leyes de derecho de autor garantizan al creador el derecho exclusivo de reproducir, creación de derivados o hacer público su trabajo.*

Desastre o contingencia: *interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras u otros medios necesarios para la operación normal de un negocio.*

Disponibilidad: *propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.*

Lineamientos de seguridad: *son productos, procedimientos y métricas aprobadas, que definen en detalle como las políticas de seguridad serán implementadas para un ambiente en particular, teniendo en cuenta las fortalezas y debilidades de las características de seguridad disponibles. Deben estar reflejadas en un documento que describe la implantación de una guía para un componente específico de hardware, software o infraestructura.*

Equipo móvil: *Es todo activo informático físico que tiene la facilidad de movilidad, como laptops, tabletas, teléfonos inteligentes, entre otros.*

Evaluación del riesgo: *proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.*

Evento de seguridad de la información: *presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.*

Integridad: *propiedad de salvaguardar la exactitud y el estado completo de los activos.*

Impacto: *la consecuencia que al interior de la empresa se produce al materializarse una amenaza.*

Organización de seguridad: *es una función que busca definir y establecer un balance entre las responsabilidades y los requerimientos de los roles asociados con la administración de seguridad de la información.*

Medio de almacenamiento removible: *Medio externo al equipo de cómputo en el que se almacena información, como disquetes, CD, DVD, memorias (USB, SD, otras), cartuchos de respaldo, discos externos y otros.*

Políticas: *toda intención y directriz expresada formalmente por la dirección.*

Procesos: *se define un proceso de negocio como cada conjunto de actividades que reciben una o más entradas para crear un producto de valor para el cliente o para la propia empresa (concepto de cliente interno de calidad). Típicamente una actividad empresarial cuenta con múltiples procesos de negocio que sirven para el desarrollo de la actividad en sí misma.*

Procedimientos: *los procedimientos son los pasos operacionales que los funcionarios deben realizar para alcanzar ciertos objetivos.*

Riesgo: *combinación de la probabilidad de un evento y sus consecuencias.*

Servicio informático: *Bien intangible que se proporciona para satisfacer los requerimientos de los usuarios, relacionado con el uso de activo informático.*

Seguridad de la información: *preservación de la confidencialidad, integridad y disponibilidad de la información, además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (accountability), no repudio y fiabilidad.*

Software institucional: *Software con licenciamiento de uso y/o propietario que puede ser instalado y utilizado por los usuarios para el desempeño de sus actividades o funciones, o para la gestión de un servicio informático otorgado por la institución.*

Software libre: *También conocido como freeware, shareware, software demo. Software gratuito proveniente de internet o cualquier otro medio que no requiere la compra de una licencia para su uso.*

TI*: se refiere a tecnologías de la información*

TIC: *se refiere a tecnologías de la información y comunicaciones*

Usuario: *Todo empleado o prestatario de servicios autorizado por ITSON, alumnos y terceros que haga uso de los activos o servicios informáticos de la institución, para el desempeño de sus funciones, consulta o atención al servicio.*

Vulnerabilidad: *debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.*

Virus: *Programa informático creado para producir daño en el equipo informático.*

4. LINEAMIENTOS

PUNTO 1: LA SEGURIDAD DE LA INFORMACIÓN:

Lineamiento 1: Responsabilidad para la seguridad de la información. La Reforestadora Integral de Antioquia S.A. es el directo propietario de la información. Su tenencia y manejo es delegada a los líderes quienes son responsables de la custodia de la información de su respectivo proceso, considerando su propósito y uso. Por ello los lideres deben ser conscientes de los riesgos a la que está expuesta la información a su cargo, de forma que ejerzan frente a sus colaboradores el liderazgo apropiado para disminuirlos.

Lineamiento 2: Actualización de normativas. La Reforestadora Integral de Antioquia S.A. debe procurar estar al día en todos los cambios de normativa del gobierno electrónico en Colombia e identificar las tendencias en Seguridad de la Información, mediante el contacto continuo con entes y áreas afines y en la página de MINTIC.

Lineamiento 3: Revisión frecuente de la seguridad de la información. Se debe implementar y ejecutar un plan interno de auditoría de seguridad de la información. Este plan debe estar enfocado hacia la revisión de todos los requerimientos (políticas y procedimientos) de seguridad. Los resultados deben generar un programa de seguridad, que incluya como mínimo: acciones a realizar, tablas de tiempo y responsables. El programa debe ser presentado al Comité de Riesgos de la empresa.

Lineamiento 4: Acceso de terceros. El área de sistemas debe realizar una evaluación de riesgos para identificar el riesgo de acceso por terceros a la información de La Reforestadora Integral de Antioquia S.A.. Cada líder del proceso debe verificar la implementación de acuerdos, monitorear el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros.

PUNTO 2: CLASIFICACIÓN Y CONTROL DE ACTIVOS DE LA INFORMACIÓN:

Lineamiento 5: Responsabilidad sobre los activos. La Reforestadora Integral de Antioquia S.A. pone al servicio de los colaboradores el uso de los medios necesarios para el normal desarrollo de las labores

propias de sus respectivos roles, para lo cual adopta y comunica las políticas de uso aceptable, controles y medidas dirigidas a garantizar la seguridad y continuidad del servicio que presta.

Lineamiento 6: Clasificación de los activos. Para asegurar que los activos de información reciben el nivel de protección adecuado, se debe crear un comité responsable de definir la metodología de clasificación de activos de información y la forma de guardarlos, estos se deben clasificar según la necesidad, las prioridades y el grado de protección esperado en el manejo de estos.

PUNTO 3: CLASIFICACIÓN DE LA INFORMACIÓN:

Lineamiento 7: Responsabilidad sobre la información. El dueño de un servicio ofrecido por la empresa es responsable de la información que este servicio genera y procesa.

Lineamiento 8: Clasificación de la información. Los líderes de cada dependencia deben informar a sus colaboradores de la clasificación de la información a su cargo para su adecuado tratamiento y además definir la forma de guardar la información en sus respectivos equipos.

Lineamiento 9: Responsabilidad sobre la información que maneja cada empleado. Todo empleado responsable de resguardo de información debe asegurar que la información esté protegida para asegurar su integridad y confidencialidad, acorde a su clasificación y forma de guardarla, ya que no se deben utilizar nombres largos en las rutas de las carpetas y no deben sobrepasar en los equipos antiguos los 130 caracteres incluyendo espacios y en los nuevos los 260 caracteres, porque si no hay perdida de información y no se garantiza la copia de seguridad. La información puede estar disponible de manera electrónica, impresa en papel, magnética, óptica y otro medio.

Lineamiento 10: Uso de la información. Todo usuario deberá hacer uso de la información a la que tenga acceso únicamente para propósitos relacionados con el cumplimiento de sus funciones, debiendo resguardar principalmente la relativa a datos personales, absteniéndose de comunicarlos a terceros sin el consentimiento expreso de la persona a la que se refieren.

Lineamiento 11: Cuidado de la información. Todos los usuarios que hacen uso de información clasificada como restringida o confidencial, evitarán que sea accedida por personas no autorizadas.

PUNTO 4: INTERCAMBIO DE INFORMACIÓN:

Lineamiento 12: Seguridad en la entrega de información. Toda persona que intercambie información reservada y/o confidencial con personal de La Reforestadora Integral de Antioquia S.A. o terceras personas, debe asegurar la identidad de la persona a la que le es entregada la información, ya sea por medio físico o electrónico, dejando constancia que es procedente la entrega de información.

Lineamiento 13: Información a terceras personas. Todo convenio de La Reforestadora Integral de Antioquia S.A. con terceras personas para compartir información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales.

PUNTO 5: DE LA PRESTACIÓN DE SERVICIOS DE TERCEROS:

Lineamiento 14: Proveedor de servicios informáticos. Todo proveedor que proporcione servicios informáticos a La Reforestadora Integral de Antioquia S.A. y que tenga acceso a información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales y contar con acuerdos de no divulgación ni uso que perjudique a La Reforestadora Integral de Antioquia S.A..

Lineamiento 15: Monitoreo de servicios informáticos. Todo servicio informático otorgado por terceros debe ser monitoreado y revisado por la persona responsable de su contratación, para asegurar que se cumplan con los términos estipulados en los acuerdos o contratos de La Reforestadora Integral de Antioquia S.A..

PUNTO 6: PROTECCIÓN CONTRA VIRUS – MALWARE – ADWARE – BONET – RANSOMWARE - ETC:

Lineamiento 16: Protección antivirus instalada. Todo equipo de cómputo institucional y equipo de computo propiedad de contratista que se conecte a la red local, a la intranet y a las impresoras debe contar con solución antivirus definida por el área de sistemas. Si la solución no cubre a la plataforma utilizada, el personal notificará al área de sistemas para buscar una alternativa de solución o para negar el acceso a dicho equipo.

Lineamiento 17: Reporte de incidentes. Todo Usuario que identifique una anomalía en su equipo de cómputo deberá reportarla al área de sistemas mediante sistema de mesa de servicio del área de sistemas a través del correo soporte@riaforestal.org,. Incidentes que serán atendidos en orden de

solicitud y de prioridad, priman los servicios pedidos por este medio sobre los servicios pedidos verbalmente, por WhatsApp o al correo de sistemas@riaforestal.org.

PUNTO 7: SERVICIOS INFORMÁTICOS EN LA RED:

Lineamiento 18: Buen uso de la información. Todos los empleados y terceros son responsables del buen uso de los servicios informáticos institucionales alojados en la empresa y en la nube, asignados para realizar sus funciones administrativas y laborales.

Lineamiento 19: Acceso del área de sistemas a activos informáticos. Personal de seguridad informática del área de sistemas queda facultado para acceder a los equipos de cómputo institucionales para:

- la realización de revisiones en base a cumplimiento de medidas de seguridad informática como antivirus y actualizaciones.
- el inventario de software y hardware.
- por ausencia del personal en base a petición del jefe inmediato y que se requiera acceder a información y servicios en base a sus funciones.
- y a petición del área administrativa o gerencial para realizar una revisión de seguridad informática y descartar uso no debido (daños intencionales a información, equipo, a personas) del equipo de cómputo, bajo previa notificación al usuario, como se especifica en lineamiento 32 y lineamiento 33 del presente documento. En caso de ausencia e imposibilidad de localizar al usuario, la notificación se realizará a el jefe inmediato.

Lineamiento 20: Niveles de acceso a los usuarios. el área de sistemas es responsable de autorizar el nivel de acceso con privilegios mínimos necesarios para que todo el personal de la empresa.

Lineamiento 21: Borrado de la información. Ninguna persona debe ver, copiar, alterar o destruir la información que reside en los equipos de cómputo y servidores sin el consentimiento explícito del responsable del equipo o del dueño de la información, excepto en casos que se especifican en el lineamiento 19 del presente documento.

Lineamiento 22: Cuentas de usuario y contraseñas. Todas las cuentas de usuario y su respectiva contraseña de acceso a los sistemas y servicios de información en la red de La Reforestadora Integral

de Antioquia S.A., así como a los de telefonía, son personales, permitiéndose el uso bajo su responsabilidad, única y exclusivamente durante la vigencia de los derechos del usuario. La vigencia de las cuentas de usuarios es facultad del área de sistemas y del área dueña del servicio, éstas son habilitadas, suspendidas o canceladas por el área en consideración a las solicitudes, necesidades y conductas de los usuarios.

Lineamiento 23: Herramientas de análisis de red. Toda utilización de herramientas tales como analizadores, escaneo y monitoreo de red, son permitidas únicamente para las funciones de administración de las tecnologías de información y de actividades como pruebas de continuidad del negocio, evaluación de riesgos, etc.

Lineamiento 24: Habilitación de dispositivos en la red. Todo hardware de telecomunicaciones (switches, enrutadores, puntos de acceso inalámbrico, entre otros) y servidores (web, FTP, correo y otros) que se requiera habilitar en la red de telecomunicaciones institucional debe ser previamente autorizado por el área de sistemas.

Lineamiento 25: Acceso del área de sistemas a activos informáticos. A todo equipo de cómputo institucional conectado a la red de La Reforestadora Integral de Antioquia S.A. (computadoras de escritorio y portátiles), personal autorizado por el área de sistemas deberá de configurarlo en la red y en el servidor, y además otorgar cuenta de usuario para acceder a los servicios de la red La Reforestadora Integral de Antioquia S.A..

Lineamiento 26: Redes VPN y acceso externo. Todo servicio de Red Privada Virtual (VPN) para ser utilizado en laptops fuera de la empresa, será otorgado a todo el personal que lo requiera para sus funciones laborales, siendo autorizado por el área de sistemas, considerándose para ello la capacidad de la infraestructura de tecnologías de información de que dispone la institución.

Lineamiento 27: Finalización de relación laboral. A toda persona que deje de laborar o tener relación con La Reforestadora Integral de Antioquia S.A., le será cancelado su acceso de manera definitiva a los recursos informáticos institucionales. Talento humano comunicará al área de sistemas y a las demás áreas responsables de brindar servicios informáticos, toda alta, baja o cambio del personal para que se tomen las medidas correspondientes de privilegios de acceso a los servicios de red.

Lineamiento 28: Hardware y Software que sea riesgoso. A todo hardware y software de uso laboral que sean considerados de riesgo para la seguridad de los servicios informáticos de la empresa, deberán ser utilizados en ambiente aislado. Ejemplos de hardware y software con analizadores de tráfico de red, herramientas de análisis y diagnóstico de equipos de cómputo y telecomunicaciones, inventario de red, equipos de laboratorio de redes, entre otros.

PUNTO 8: USO DE CUENTAS DE USUARIO:

Lineamiento 29: Acceso A Servicios Informáticos. Toda persona que requiera acceder a servicios informáticos de la empresa requerirá de una cuenta de usuario y contraseña u otro medio de autenticación. La cuenta de usuario y contraseña deberá ser asignada por el responsable del servicio.

Lineamiento 30: Cambio en privilegios de cuentas de usuario. Toda solicitud de alta, baja o cambio de privilegios de cuentas de usuario para acceder a los servicios informáticos adicionales a su perfil de puesto debe ser solicitada a través del sistema de mesa de servicios del área de sistemas por el jefe inmediato o jefe de área demandante, debidamente justificado.

Lineamiento 31: Actualización de contraseñas. Todo usuario debe actualizar la contraseña de su cuenta de acceso a los servicios informáticos de manera periódica (al menos cada 90 días) o cuando sospeche de su divulgación. La contraseña debe ser de al menos 8 caracteres alfanuméricos, con mayúscula, minúscula, números y símbolos y que sea fácil de recordar.

Lineamiento 32: Acceso A Servicios Informáticos. Cuando se requiera acceder a información de un equipo de cómputo y/o cuenta de correo institucional de una persona ausente ya sea por cuestiones de salud, por estar comisionado a actividades fuera de su área de trabajo u otro motivo no especificado, el responsable del área correspondiente deberá solicitar al área de sistemas que se brinde el acceso al equipo y/o servicio o sistema informático para poder dar continuidad a algún proceso de la empresa.

Personal del área de sistemas únicamente proporcionará acceso al responsable del área correspondiente que lo haya solicitado a efecto de que sustraiga la información necesaria, dejando constancia de ello en un acta circunstanciada que se levante con asistencia del área jurídica, bajo previa notificación a la persona ausente.

Si una persona deja de laborar en la Institución o cambia de puesto, el jefe inmediato podrá solicitar al área de sistemas el acceso al equipo que ésta tenía asignado, el cual es concedido para que sustraiga la información pertinente, y sin necesidad de la intervención del área jurídica.

PUNTO 9: MONITOREO DEL USO DE LOS ACTIVOS:

Lineamiento 33: Revisión de los activos informáticos. Personal del área de sistemas realiza periódicamente inventarios de hardware y software del activo informático de la empresa, para dar atención a problemas de obsolescencia y revisiones de licenciamiento. Además, se monitorean los servicios informáticos de red para administrar el uso del recurso informático de internet y solución de problemas, además que el equipo cuenta con restricciones, puntualmente que cada equipo institucional posee una cuenta administrador con una clave para evitar que se instalen programas o se realicen cambios en la configuración del equipo, esta clave solo será revelada a través de un correo a soporte@riaforestal.org con copia a direccionadministrativa@riaforestal.org y con la autorización respectiva a través de correo desde la dirección administrativa.

PUNTO 10: USO DE INTERNET:

Lineamiento 34: Internet solo para uso laboral. El servicio de Internet a través de las redes de La Reforestadora Integral de Antioquia S.A. se considera como herramienta de trabajo, por lo que todo usuario deberá utilizarlo exclusivamente para apoyo a sus actividades académicas y/o administrativas en la empresa.

Lineamiento 35: Restricción parcial o total de internet. Todo responsable de área puede solicitar la restricción total o parcial de acceso a Internet del personal a su cargo, considerando para ello las funciones laborales que éstos realizan.

Lineamiento 36: Protocolos de internet. Para la integración de toda solución informática basada en protocolos de internet, el área requirente debe solicitar a personal del área de sistemas evaluar y recomendar los recursos de infraestructura de cómputo y telecomunicaciones, con el fin de que el área requirente gestione los recursos necesarios para la puesta en producción de la solución.

Lineamiento 37: Descarga de información. Todo usuario que descargue información y archivos de Internet mediante el navegador web u otro medio como FTP y mensajería instantánea, debe de omitir descargar archivos de dudosa procedencia. Los archivos descargados de Internet pueden contener virus o software malicioso que pongan en riesgo la información del equipo de cómputo de la persona, e incluso de la empresa.

Lineamiento 38: Descarga de programas sospechosos. El usuario debe abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía web o medios magnéticos.

Lineamiento 39: Descarga de multimedia. La descarga de música y videos no es una práctica permitida.

Lineamiento 40: Servicios de descarga. Evitar el uso de servicios descarga de archivos no autorizados por la La Reforestadora Integral de Antioquia S.A..

Lineamiento 41: Salas de videoconferencia. Las salas de videoconferencia de la organización deben ser de uso exclusivo para asuntos relacionados con la empresa.

Lineamiento 42: Sitios seguros solamente. Abstenerse de usar sitios que salten la seguridad del servidor de acceso a Internet y evitar conectarse a sitios que no cuenten con protocolo seguro (https).

Lineamiento 43: El uso de internet con fines preestablecidos. El uso con fines comerciales, políticos, particulares o cualquier otro que no sea el laboral y que dio origen a la habilitación del servicio, no está permitido.

Lineamiento 44: Uso responsable de los sitios. Evitar coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar en cualquier forma actos ilegales, inmorales, engañosos y/o fraudulentos es una responsabilidad de los empleados de la empresa; así como también amenazas, abusos, difamaciones, injurias, calumnias, escándalos, actos obscenos, pornográficos, profanos, racistas, discriminatorios, actos que invadan la privacidad de los demás u otro tipo de materias, informaciones, mensajes o comunicaciones de carácter ofensivo.

Lineamiento 45: Confidencialidad y legalidad de la información. Los usuarios no deberán coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que pueda infringir o violar cualquier patente, derechos de autor, marcas, secretos empresariales o cualquier otro derecho intelectual de otra persona.

Lineamiento 46: Privacidad de la identidad de terceros. No está permitido personificar o intentar personificar a otra persona a través de la utilización de encabezados falsificados u otra información personal.

Lineamiento 47: Sobre cadenas y ofertas fraudulentas. Hacer ofertas fraudulentas de compra o venta, así como también, conducir cualquier tipo de fraude financiero, tales como "cartas en cadena" o "las pirámides", son faltas que se constituyen como violaciones a esta Política.

Lineamiento 48: Sabotear el servicio de otro usuario. Hacer o intentar hacer, cualquier cosa que afecte desfavorablemente la habilidad de utilizar el servicio de internet por otros usuarios, incluyendo sin limitación alguna, "negación de servicios", ataques contra otros sistemas o contra el anfitrión de redes u otros usuarios, se constituye como una violación a esta Política.

PUNTO 11: USO DE CORREO ELECTRÓNICO Y MENSAJERÍA:

Lineamiento 49: Uso del correo electrónico institucional. El correo electrónico institucional es para uso exclusivo del empleado activo administrativo, ventas, activaciones y todas las áreas de la empresa y personas externas a las que se les reconoce la relación con La Reforestadora Integral de Antioquia S.A.. Éste deberá ser utilizado sólo para realizar actividades relacionadas con sus funciones.

Lineamiento 50: Solicitud de cuenta de correo. Los responsables de área deberán solicitar por los medios establecidos por el área de sistemas, a través del sistema de mesa de servicio, una nueva cuenta de correo electrónico para personal a su cargo.

Lineamiento 51: Descarga de información. La Reforestadora Integral de Antioquia S.A. no es garante de los contenidos expresados en texto, sonido o video, redactados y enviados mediante el correo electrónico institucional.

Lineamiento 52: Finalización de relación laboral, correo e información del correo. A toda persona que termine la relación laboral con el La Reforestadora Integral de Antioquia S.A., una vez recibida la notificación de baja por parte Talento humano, se inhabilitará el servicio de correo electrónico. Transcurridos 30 días hábiles, el contenido de la cuenta de correo inhabilitada será respaldado como histórico de las funciones del empleado.

Lineamiento 53: Envío de elementos puntuales. Evitar el envío desde su buzón de elementos (textos, software, música, imágenes o cualquier otro) que contravengan lo dispuesto en la legislación vigente y

en los reglamentos internos, sobre propiedad intelectual y derechos de autor. En especial, es necesario evitar la distribución de software que requiera licencia, claves ilegales de software, programas para romper licencias (crackers), y en general, cualquier elemento u objeto de datos sin permiso específico del autor cuando este sea requerido. La violación de esta obligación origina automáticamente la suspensión del servicio y puede ser causa de sanciones al colaborador, con perjuicio de las responsabilidades que eventualmente puedan surgir ante la ley.

Lineamiento 54: Creación de perfiles sociales: No está permitida la práctica de utilizar el correo corporativo para la creación de perfiles en redes sociales.

Lineamiento 55: Envío de correos no solicitados o no deseados. Los colaboradores de la compañía se abstendrán de utilizar la cuenta para el envío o reenvío de mensajes spam (no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades), hoax (es un intento de hacer creer que algo falso es real), con contenido que pueda resultar ofensivo o dañino para otros colaboradores (como virus o pornografía), o que sea contrario a las políticas y normas institucionales.

Lineamiento 56: No usar credenciales de acceso corporativo. Evitar usar el correo y credenciales de acceso corporativo en sitios para uso personal como cuentas bancarias, almacenes de cadena, entre otros.

Lineamiento 57: Reenvío de mensajes recibidos. Evitar el envío de respuestas con copia a todos los destinatarios de un mensaje recibido, y en particular cuando se trata de mensajes que originalmente hayan sido dirigidos a un grupo grande de colaboradores; salvo cuando se trate de una respuesta que por su naturaleza o contenido necesariamente requiera ser conocida por todos ellos.

Lineamiento 58: Recepción de correos sospechosos. Evitar abrir mensajes no esperados que contengan archivos adjuntos, aunque provengan de personas conocidas. Podría tratarse de un virus. En particular, no abrir mensajes cuyo asunto contenga palabras en inglés a menos que lo esté esperando

Lineamiento 59: Uso adecuado de la redacción de un correo. En lo posible, es necesario evitar usar letras mayúsculas, especialmente en el campo de “Asunto:”, al igual que el uso excesivo de signos de exclamación (&, %, $, #, ?, ¡, !, ¿), esto puede hacer que los sistemas de correo lo identifiquen como correo no deseado o spam, y el mensaje posiblemente no llegue al destinatario, o llegue con identificación de correo no solicitado.

Lineamiento 60: Capacidad del buzón de correo. Si utiliza el servicio de correo a través del sitio web de la empresa, se recomienda que no deje mensajes almacenados por mucho tiempo en el servidor de correo. Tenga presente descargarlos con frecuencia, preferiblemente a diario. Tenga en cuenta que el tamaño de su buzón de correo es limitado; una vez superado este tope, el sistema no le procesará más correos. Elimine mensajes si lo necesita y vacíe la papelera siempre que sea posible.

Lineamiento 61: Solicitud de alta o baja de grupos de correo. Toda solicitud de alta, baja o cambio de un grupo de correo institucional debe ser solicitado por el responsable del área solicitante.

Lineamiento 62: Prohibiciones en envío y recepción de correo. Queda prohibido utilizar el correo electrónico para envíos de correo basura, cadenas, mercadotecnia, religiosos, propaganda política, actos agresivos e ilegales y cualquier otro contenido no apropiado para el destinatario. No podrá recibir o enviar mensajes de sus colaboradores con contenido impropio, difamatorio, ilícito, obsceno, indecente o que contengan difusión de noticias sin identificar plenamente su autor; adicionalmente, los colaboradores no podrán enviar anónimos, propagandas o literatura de cualquier índole, encuestas, concursos, esquemas piramidales, cartas en cadena, mensajes no deseados, o cualesquiera que contenga mensajes duplicativos o no solicitados, u otra información ajena a las labores que desempeñan en su rol.

Lineamiento 63: Uso no autorizado de su cuenta de correo. Es responsabilidad de todo usuario del correo electrónico institucional notificar al personal del área de sistemas la sospecha del uso no autorizado de su cuenta.

Lineamiento 64: Pérdida en el servicio de correo. Todo usuario del correo electrónico institucional, acepta que comprende y acuerda expresamente que La Reforestadora Integral de Antioquia S.A., no es responsable directo e indirecto y sin limitación alguna, por pérdida de datos o de cualquier otra pérdida intangible en el servicio de correo electrónico.

Lineamiento 65: Envío masivo de correo. Todo usuario que desde una cuenta de correo electrónico institucional o externo, requiera enviar un correo masivo, entendiéndose como aquel que se envía a más de 20 destinatarios, ya sea en un mismo envío o en varios envíos con contenido similar, deberá previamente solicitar la autorización del Director de su área y posteriormente realizar la solicitud correspondiente en Sistema de Mesa de Servicio del área de sistemas.

Lineamiento 66: Utilización de mensajería instantánea. Todo servicio de mensajería instantánea debe ser utilizado para el desarrollo de actividades concernientes al puesto del personal; donde cada persona es responsable del buen uso de este servicio.

Lineamiento 67: Mensajería instantánea interna. Todo empleado La Reforestadora Integral de Antioquia S.A. puede acceder a la mensajería instantánea interna solicitando al área de sistemas su usuario y contraseña e instalación de la aplicación.

PUNTO 12: USO DEL SOFTWARE:

Lineamiento 68: Instalación de Software. En todos los equipos de cómputo de La Reforestadora Integral de Antioquia S.A., solo se permite la instalación de software con licenciamiento vigente, ya sea de uso libre o comercial. Las áreas de Soporte Técnico Informático están facultadas para asesorar la instalación del software.

Lineamiento 69: Adquisición de Software. Toda persona que necesite adquirir software podrá solicitar apoyo al área de sistemas, quien verificará los requerimientos técnicos y el completo licenciamiento, y recabar una copia de esta licencia para su resguardo.

Lineamiento 70: Software sin licenciamiento. Todo empleado, personal de la empresa y terceros que instale software sin licenciamiento vigente o malicioso en equipos de cómputo de la institución, se hace único responsable de las consecuencias que esto conlleve.

Lineamiento 71: Software propiedad de la empresa. Las licencias de uso de software propiedad La Reforestadora Integral de Antioquia S.A., otorgan a éste el derecho de emplearlas exclusivamente en los equipos asignados al personal de la institución.

PUNTO 13: REDES SOCIALES:

Lineamiento 72: El uso de la imagen empresarial. No utilizar el nombre, imagen, marca, logo o instalaciones de la organización para fines personales o divulgación de contenidos en nuestras redes sociales salvo que haya sido promovido o autorizado por la organización y siempre que no vayan en detrimento de su imagen.

Lineamiento 73: Compartir información empresarial. Evitar compartir información confidencial sobre la organización o información en redes sociales y/o foros externos.

Lineamiento 74: Relación comercial con clientes. Evitar entrar en debates y/o discusiones con clientes o potenciales clientes a través de las redes sociales.

Lineamiento 75: Sobre perfiles o enlaces sospechosos. No hacer clic en contenidos sobre los que no se tenga claro su origen o propósito y estar atentos a los mensajes de identidades desconocidas.

Lineamiento 76: Compartir información sensible. No compartir contenidos sensibles sobre la vida personal o la de otros en redes sociales, por ejemplo: documentos de identificación, números de teléfono, direcciones, localizaciones exactas, identificadores de vehículos, entre otros.

Lineamiento 77: Difusión de información privada de terceros. No difundir información privada sobre otras personas sin su consentimiento y no etiquetar por su nombre a otras personas que no tienen perfil en redes sociales sin solicitar previamente su permiso para hacerlo.

Lineamiento 78: Privacidad de perfil y contenido. Comprobar la configuración de privacidad tanto en el perfil como en los contenidos que se comparten.

Lineamiento 79: Acceso a perfiles. Proteger el acceso a los perfiles en redes sociales con contraseñas fuertes utilizando dos factores de autenticación donde sea viable.

Lineamiento 80: Sobre los contactos. Mantener en privado la lista de contactos y analizar con detenimiento las solicitudes de amistad de desconocidos.

Lineamiento 81: Geolocalización. Controlar la geolocalización de perfiles y contenidos en redes sociales. Desactivar la geolocalización por defecto en el menú de configuración de los perfiles.

PUNTO 14: RECURSOS COMPARTIDOS:

El uso de carpetas compartidas en los equipos de cómputo de los usuarios es una práctica que, aunque puede ser una herramienta útil de trabajo, tiene implícitos algunos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información, por lo tanto, su uso y aplicación debe ser controlado. Con este propósito la organización define los siguientes lineamientos para su uso seguro:

Lineamiento 82: Uso de carpetas compartidas. Se debe evitar el uso de carpetas compartidas en equipos de escritorio, para esto se utiliza el servidor NAS.

Lineamiento 83: Habilitación de carpetas compartidas. Los administradores de la red establecen e implementan, en los casos aprobados, la configuración de acceso a la carpeta, previo requerimiento formal de la misma a través de la Mesa de Ayuda .

Lineamiento 84: Responsabilidad sobre compartir recursos. El usuario que autoriza y dispone el recurso compartido es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.

Lineamiento 85: Roles del acceso. Se debe definir el tipo de acceso y los roles estrictamente necesarios sobre la carpeta (lectura, escritura, modificación y borrado).

Lineamiento 86: Límite de tiempo en el recurso compartido. Debe tenerse claramente especificado el límite de tiempo durante el cual estará publicada la información y compartido el recurso en el equipo.

Lineamiento 87: Información compartida en el servidor. Si se trata de información secreta o restringida, deben utilizarse las carpetas destinadas para al fin en el servidor de archivos de usuarios, para que sean incluidos en las copias diarias de respaldo de información o implementar herramientas para el respaldo continuo de información sobre dichos equipos.

Lineamiento 88: Limite de usuarios con acceso al recurso. El acceso a carpetas compartidas debe delimitarse a los usuarios que las necesitan y deben ser protegidas con contraseñas.

Lineamiento 89: Protección en el acceso al recurso. No se debe permitir el acceso a dichas carpetas a usuarios que no cuenten con antivirus corporativo actualizado.

PUNTO 15: USO DE PORTÁTILES Y DISPOSITIVOS MÓVILES:

Los usuarios, contratistas y terceros se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la empresa, tales como escritorios y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros, atendiendo los siguientes lineamientos:

Lineamiento 90: Uso en sitios públicos. En sitios públicos, adopte precauciones con los dispositivos móviles que no esté usando, asegurándose que se encuentre en el bolsillo, maletín o lugar no visible.

Lineamiento 91: Seguridad de acceso al dispositivo. El dispositivo móvil debe estar configurado para bloqueo automático por un tiempo de inactividad a través de medios disponibles de configuración tales como contraseña, patrón huella dactilar, reconocimiento de voz, guaya, pregunta entre otras.

Lineamiento 92: Protección del dispositivo. Uso de aplicación de antivirus.

Lineamiento 93: Seguridad de uso del dispositivo. Uso de múltiple factor de autenticación, para mitigar el riesgo de suplantación de identidades, uso de canales seguros y cifrados cuando se conecte a redes compartidas de acceso libre, no seguras, accesos privilegiados, entre otras.

PUNTO 16: ACCESO A EQUIPOS DISTINTOS A LOS DESIGNADOS:

Lineamiento 94: Autoguardado de contraseñas. Desactivar la opción de autoguardado de contraseñas en los diferentes navegadores web.

Lineamiento 95: Sobre el uso de las claves. No dejar claves en ningún sistema de almacenamiento de información web.

Lineamiento 96: Contraseñas seguras. Creación de contraseñas seguras, no incluir información personal como nombres, fechas de nacimiento, otros.

Lineamiento 97: Cerrar sesiones. Cerrado de sesión de escritorio virtual cuando no esté en uso.

Lineamiento 98: Autenticación y canales seguros. Uso de múltiple factor de autenticación (algo que sé con algo que tengo), para mitigar el riesgo de suplantación de identidades, uso de canales seguros y cifrados cuando se conecte a redes compartidas de acceso libre, no seguras, entre otras.

PUNTO 17: TRATAMIENTO Y GESTIÓN DE EL RIESGO:

Lineamiento 99: Revisión constante de riesgos. Periódicamente se debe realizar una valoración del riesgo para contemplar los cambios en los requisitos de seguridad y la situación de riesgo, tales como cambio en los activos, las amenazas, las vulnerabilidades y los impactos. Se debe decidir cuándo un riesgo es aceptable, ya sea por motivos de objetivos de negocio o por costes no rentables.

Los posibles tratamientos a los riesgos identificados incluyen:

- Evitar el riesgo.
- Mitigar el riesgo.
- Transferir los riesgos.

- Retener los riesgos.

PUNTO 18: SEGURIDAD DE LA INFORMACIÓN EN TALENTO HUMANO:

Lineamiento 100: Seguridad previa a la contratación. Para toda persona que ingrese a la compañía, Talento Humano debe asegurar las responsabilidades sobre seguridad de la información de manera previa a la contratación. Esta tarea debe reflejarse en una adecuada descripción del rol y en los términos y condiciones de la contratación, si la persona es contratista y posee un equipo de computo que va a ser utilizado en las instalaciones físicas de la Reforestadora, la persona debe firmar un documento en el cual indica que el equipo de marca tal con serial tal es de su propiedad y asume toda responsabilidad del software instalado en dicho equipo.

Lineamiento 101: Seguridad durante el contrato. El área de sistemas debe desarrollar un programa efectivo y continuo de concientización de protección de la información para todo el personal. También se requiere de capacitación específica en administración de riesgos tecnológicos para aquellos individuos que están a cargo de responsabilidades especiales de protección y los conceptos básicos con que debe cumplir todo colaborador.
Es responsabilidad y deber de cada colaborador de La Reforestadora Integral de Antioquia S.A. asistir a los cursos de concientización en seguridad de la información que la empresa programe y aplicar la seguridad según las políticas y los procedimientos establecidos por la empresa.

Lineamiento 102: Finalización o cambio de puesto. Talento Humano debe asegurar que todos los colaboradores que salgan de la empresa o cambien de puesto de trabajo, hayan firmado un acuerdo de confidencialidad, cuyo cumplimiento será vigente hasta que La Reforestadora Integral de Antioquia S.A. lo considere conveniente, incluso después de la finalización del puesto de trabajo o del contrato.
Talento Humano se asegurará que la salida o movilidad de los usuarios sea gestionada hasta la completa devolución de todos los activos y la entrega de toda la información del contrato al cual el contratista estaba adscrito y retirada de los derechos de acceso.

PUNTO 19: SEGURIDAD FISICA Y DEL ENTORNO:

Lineamiento 103: Controles de acceso físico. El acceso a áreas TIC restringidas sólo se debe permitir para:

- Desarrollo de operaciones tecnológicas.

- Tareas de aseo (monitoreado por personal del equipo de Tecnología).
- Pruebas de equipos.
- Almacenamiento de equipos.
- Implementación o mantenimiento de los controles ambientales.

Lineamiento 104: Escritorio limpio. La implementación de una directriz de escritorio limpio permitirá reducir el riesgo de acceso no autorizado o daño a medios y documentos.
Los computadores deben bloquearse después de diez (5) minutos de inactividad, el usuario tendrá que autenticarse antes de reanudar su actividad. Todos los usuarios, consultores, contratistas, terceras partes deben bloquear la sesión al alejarse de su computador.

Lineamiento 105: Seguridad de los equipos. Para prevenir la pérdida de información daño, robo o el compromiso de los activos de información y la interrupción de las actividades de La Reforestadora Integral de Antioquia S.A. los equipos deben estar conectados a la toma regulada destinada para tal fin y debidamente asegurados mediante el uso guayas para los equipos portátiles.

Lineamiento 106: Retiro de equipos. Se deben tener en cuenta los procesos de instalación y retirada del equipo, de tal manera que estos se hagan de forma controlada y segura. La protección de los equipos, incluso cuando se utilizan fuera de la oficina, es necesaria para reducir el riesgo no autorizado de acceso a la información y para protegerlo contra pérdida o robo.

PUNTO 20: CONTROL DE ACCESO A LA INFORMACIÓN:

Lineamiento 107: Gestión de acceso a usuarios. El área de sistemas establecerá procedimientos formales para controlar la definición de perfiles y la asignación de derechos de acceso a los colaboradores, previamente definidos por el líder responsable del proceso. Dichos procedimientos deben cubrir todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta la eliminación o desactivación del registro a quienes no necesiten el acceso. Se debe brindar atención y seguimiento especial, donde sea apropiado, a la necesidad del control de asignaciones de accesos privilegiados.

Lineamiento 108: Registro de usuarios. Todos los usuarios deben tener una identificación única personal o jurídica, que se utilizará para el seguimiento de las actividades de responsabilidad individual o jurídica. Las actividades habituales de colaborador no deben ser desempeñadas a través de cuentas privilegiadas.
En circunstancias excepcionales, por beneficio de la compañía, se podrá usar un identificador compartido, para un grupo de colaboradores con trabajo específico; este debe ser autorizado y debidamente aprobado por el líder del proceso, previo visto bueno del área de sistemas.
El usuario debe tener autorización el líder del proceso para el uso del sistema o servicio de información. Se debe verificar que el nivel de acceso otorgado sea adecuado para los propósitos de la

empresa y conserven una adecuada segregación de funciones. Adicionalmente, deben tomar y certificar la formación y así garantizar el uso adecuado del sistema o servicio de información.

Lineamiento 109: Responsabilidades del usuario. Una seguridad efectiva requiere la cooperación de los usuarios autorizados, quienes deben saber sus responsabilidades para el mantenimiento de controles efectivos al acceso, en particular, aquellos con referencia al uso de contraseñas, el área de sistemas implementará los procedimientos necesarios que permitan controlar la creación, modificación, desactivación y eliminación de colaboradores, administración de contraseñas y permisos de acceso a los recursos tecnológicos y a la información. Adicionalmente, es necesario implementar un procedimiento de revisión periódica de los permisos de acceso de los colaboradores.
Los usuarios, contratistas y terceros entienden las condiciones de acceso y deben mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de este. Esta declaración puede ser incluida en los términos y condiciones laborales. Igualmente deben cumplir las buenas prácticas en la selección y uso de la contraseña.

Lineamiento 110: Control de acceso a la red. Únicamente se debe proporcionar a los usuarios el acceso a los servicios para los que específicamente se les haya autorizado su uso. Se deben utilizar métodos apropiados de autenticación para el control de acceso a los colaboradores remotos. Se deben implantar controles adicionales para el acceso por redes inalámbricas. Se debe establecer una adecuada segregación de redes, separando los entornos de red de usuarios y los servicios. Además todo equipo que tenga acceso a la Intranet debe contar con antivirus licenciado.

Lineamiento 111: Control de acceso a las aplicaciones. El uso de programas que puedan ser capaces de invalidar los controles del sistema y de la aplicación, deben estar restringidos y estrictamente controlados.

Lineamiento 112: Restricción de tiempo en conexión. Las sesiones inactivas deben cerrarse después de un período de inactividad definido y se deben usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo.

Lineamiento 113: Inhabilitación de usuario. Los usuarios que no ingresen a los aplicativos por más de 60 días se le inhabilitará el usuario, estos no se deben eliminar para no perder la trazabilidad de la gestión.

Lineamiento 114: Depuración de usuarios. El funcional de cada aplicativo debe depurar los usuarios de empleados que lleven más de 60 días sin actividad. Esta gestión se debe realizar con una periodicidad de dos (2) meses.

Lineamiento 115: Cuenta individual de ingreso. Los usuarios deben contar con una cuenta individual para ingresar a las aplicaciones y se debe restringir el uso de usuarios genéricos.

Lineamiento 116: Requerimiento para creación de usuarios. Los requerimientos para la creación de usuarios genéricos en los aplicativos deben ser denegados por el administrador.

Lineamiento 117: Depuración de usuarios de soporte. Los administradores de los sistemas deben depurar los usuarios que tengan perfiles de soporte y cuentas de servicio. Esta actividad se debe realizar con una periodicidad de dos (2) meses.

Lineamiento 118: Des habilitación en procesos esporádicos. Las cuentas del usuario, de herramientas o productos que vengan por omisión se deben deshabilitar inmediatamente después de la instalación de los sistemas o software.

Lineamiento 119: Contraseñas por defecto desde el proveedor. Las contraseñas predeterminadas por el proveedor se deben cambiar inmediatamente después de la instalación de los sistemas o software.

PUNTO 21: GESTIÓN DE CONTRASEÑAS Y USUARIOS:

Lineamiento 120: Cambio de contraseñas. Todos los usuarios deben cambiar la contraseña cada 60 días y en la construcción se debe tener en cuenta las siguientes recomendaciones:

- La longitud de la contraseña no debe ser inferior a ocho (8) caracteres.
- Las contraseñas deben contar con una mezcla de caracteres alfabéticos (donde se combinen las mayúsculas y las minúsculas), dígitos e incluso caracteres especiales (@, ¡, +, &).
- No almacenar las contraseñas en un lugar público y al alcance de los demás.
- La contraseña no debe contener el nombre de usuario de red, o cualquier otra información personal fácil de averiguar. Tampoco una serie de letras dispuestas adyacentemente en el teclado (qwerty) o siguiendo un orden alfabético o numérico (123456, abcde, etc.)
- No compartir las contraseñas, son personales e intransferibles.

PUNTO 22: GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:

Lineamiento 121: Monitoreo, detección, análisis y mitigación. El área de sistemas debe implementar un centro de operaciones de seguridad (SOC), que permita monitorear, detectar, analizar, mitigar y responder a las amenazas cibernéticas y actividades adversas.

Lineamiento 122: **Comunicación de los eventos.** El área de sistemas debe asegurarse de que los eventos y los puntos débiles de seguridad de la información asociados con los sistemas de información, se comunican de forma que sea posible emprender acciones correctivas.

Lineamiento 123: Procedimiento para la comunicación de los eventos. Se debe establecer un procedimiento formal de comunicación de eventos de seguridad de la información, junto con un procedimiento de respuesta y escalado de incidentes, que determine la respuesta que debe darse cuando se recibe un informe de un evento de seguridad de la información.

Lineamiento 124: Gestión de incidentes de seguridad de la información. Se deben establecer responsabilidades y procedimientos para tratar los eventos y los puntos débiles de seguridad de la información de forma efectiva. Una vez que se hayan comunicado a través de un proceso de mejora continua, el grupo de resolución de problemas se encargará de analizar la causa y evaluar conforme al proceso de gestión de problemas.

Lineamiento 125: Eventos que implican acciones legales. Cuando se detecta por primera vez un evento de seguridad de la información, puede que no resulte evidente si dicho evento tendrá como consecuencia una acción legal. Por este motivo, existe el peligro que se destruyan de forma intencional o accidental de las pruebas necesarias antes de tomar conciencia de la gravedad del incidente. Se debe hacer uso de los servicios jurídicos de La Reforestadora Integral de Antioquia S.A. y/o de la Policía en las primeras fases de cualquier acción legal que se esté considerando, así como asesorarse de las pruebas necesarias.

Lineamiento 126: Recolección de pruebas para procesos legales del evento. Cuando una acción contra una persona u organización, después de un incidente de seguridad de la información, implique medidas legales (tanto civiles como penales), deberían recopilarse pruebas, que deberían conservarse y presentarse de manera que se ajusten a las normas legales vigentes.
A la hora de la recopilación de las pruebas, se preservará la cadena de custodia y se utilizarán herramientas y procedimientos aceptados de análisis forenses.

PUNTO 23: GESTIÓN DE INCIDENTES DE TELECOMUNICCIONES E INFRAESTRUCTURA TIC:

Lineamiento 127: Procedimientos y responsabilidades de operación. Tecnología debe definir y documentar claramente las responsabilidades para el manejo y operación de instalaciones de computadores y redes, apoyadas por instrucciones operacionales apropiadas incluyendo procedimientos de respuesta en caso de incidentes.

Lineamiento 128: Controles de operación tecnológica. Tecnología debe definir controles que garanticen la apropiada operación tecnológica. Estos controles deben incluir como mínimo los siguientes procedimientos:

- Copias de seguridad.
- Verificación de dispositivos para copias.
- Recuperación de datos y reversión de cambios.
- Administración de sistemas de antivirus.
- Administración de colaboradores y contraseñas.
- Administración de acceso a los recursos.
- Administración de acceso remoto.
- Medición de desempeño.
- Capacidad y disponibilidad de los recursos de TI.
- Gestión de pistas de auditoría y sistemas de registro de información.
- Aseguramiento de plataformas.

PUNTO 23: GESTIÓN DEL CAMBIO:

Lineamiento 129: Implementación de controles. El área de sistemas debe implementar los controles necesarios que permitan garantizar la segregación de funciones y un adecuado seguimiento a los cambios efectuados a los activos críticos de TI. La documentación debe incluir, entre otros:

- Persona que solicita el cambio.
- Responsable de autorización.
- Descripción del cambio.
- Justificación del cambio para el negocio.
- Lista de chequeo para evaluación de riesgos, sistemas y/o dispositivos comprometidos.
- Nivel de impacto.

- Pruebas, aprobación revisiones de post-implementación.
- Capacitación, cuando sea necesario.

PUNTO 24: COPIAS DE SEGURIDAD:

Lineamiento 130: Integridad y disponibilidad de las copias de seguridad. Se deben hacer copias de respaldo de la información y del software. Para garantizar la integridad y disponibilidad, se debe hacer su comprobación regular de los mecanismos y la información en conformidad con la política de respaldo acordada, conservando los niveles de confidencialidad requeridos. El área de sistemas debe almacenar las copias de seguridad por fuera de las instalaciones de La Reforestadora Integral de Antioquia S.A. con el fin de garantizar su recuperación en caso de un evento mayor en la sede principal. La copia será realizada de una carpeta ubicada en la unidad C o D con nombre RIA o que comience con RIA, para las siguientes locaciones, la copia de seguridad y el resguardo de la información serán absoluta responsabilidad del usuario: todo lo que esté fuera de esa carpeta no será guardado en el servidor, todo lo que se encuentre en memorias usb o disco externo no será guardado en el servidor, todo lo que se tenga en una nube personal no será guardado en el servidor, y se exime de toda responsabilidad al área de sistemas, cada usuario es responsable de depurar su información y no tener información repetida ya que el servidor cuenta con una rutina de borrar la información repetida.

PUNTO 25: GESTIÓN DE LA SEGURIDAD EN LAS REDES:

Lineamiento 131: Seguridad de red. Se le debe dar atención especial al manejo de la seguridad en redes, la cual puede extenderse más allá de los límites físicos de La Reforestadora Integral de Antioquia S.A.. Procedimientos y medidas especiales se requieren para proteger el paso de información sensible a redes de dominio público. El área de sistemas debe garantizar que los proveedores de servicios de red implementan medidas en cumplimiento con las características de seguridad, acuerdos de niveles de servicio y requisitos de gestión.

Lineamiento 132: Controles y disponibilidad de red. Se deben establecer controles especiales para salvaguardar la integridad y confidencialidad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectadas, igualmente se debe garantizar la disponibilidad de los servicios de red y computadores conectados.

PUNTO 26: SERVICIOS DE COMERCIO ELECTRONICO:

Lineamiento 133: Evaluación de riesgos. Se debe realizar una evaluación para identificar el riesgo asociado con el uso de servicios de comercio electrónico, incluyendo las transacciones en línea y los requisitos para los controles. Se debe considerar la integridad y la disponibilidad de la información publicada electrónicamente a través de sistemas disponibles al público.

PUNTO 27: MONITOREO DEL USO DEL SISTEMA.

Lineamiento 134: Monitoreo y registro. El nivel de monitoreo necesario para los servicios se determinará mediante una evaluación de riesgos. La Reforestadora Integral de Antioquia S.A. cumplirá los requisitos legales que se apliquen en sus actividades de monitoreo. Se deben registrar las actividades tanto del operador como del administrador del sistema. Las actividades por monitorear incluyen: operaciones privilegiadas, acceso no autorizado y alertas o fallas del sistema, entre otras.

Lineamiento 135: Registros de auditoría. Se deben elaborar y mantener durante un período acordado, los registros de auditoría de las actividades de colaborador, de operación y administración del sistema.

PUNTO 28: TRATAMIENTO DE MEDIOS DE INFORMACIÓN:

Lineamiento 136: Control de medios. Se deben controlar los medios y proteger para prevenir la revelación, modificación, eliminación o destrucción no autorizada de los activos y la interrupción de las actividades del negocio.

Lineamiento 137: Borrado seguro. El área de sistemas debe implementar los controles que permitan garantizar que la eliminación de cualquier dispositivo o componente tecnológico que contenga información secreta, sean destruidos físicamente, o bien que la información sea destruida, borrada o sobrescrita, mediante técnicas que no hagan posible la recuperación de la información original, en lugar de utilizar un borrado normal o formateado.

PUNTO 29: CUMPLIMIENTO Y NORMATIVA LEGAL:

Lineamiento 138: Cumplimiento legal. Todos los requerimientos contractuales y legales que puedan afectar los sistemas de información de La Reforestadora Integral de Antioquia S.A. deben definirse

previamente y documentarse de acuerdo con la metodología empleada por la empresa. Los controles específicos, medidas de protección y responsabilidades individuales que cumplan con los requerimientos, deben así mismo definirse y documentarse. El área jurídica de La Reforestadora Integral de Antioquia S.A. asesorará al Comité de Riesgos en dichos aspectos legales específicos.

Lineamiento 139: Propiedad intelectual. Se protegerá adecuadamente la propiedad intelectual de La Reforestadora Integral de Antioquia S.A., tanto propia como la de terceros (derechos de autor de software o documentos, derechos de diseño, marcas registradas, patentes, licencias, código fuente, entre otros). El material registrado con derechos de autor no se debe copiar sin la autorización del propietario.

Lineamiento 140: Protección de datos. Los lineamientos de seguridad son de obligatorio cumplimiento para los usuarios con acceso a los datos de carácter personal y a los sistemas de información. Deberán considerar, los siguientes aspectos:

- Ámbito de aplicación del procedimiento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido por la ley.
- Funciones y obligaciones del personal con acceso a las bases de datos.
- Estructura de las bases de datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante los incidentes.
- Procedimientos de realización de copias de respaldo y de recuperación de los datos.
- Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el procedimiento de seguridad que se implemente. Medidas a adoptar cuando un soporte o
- documento vaya a ser transportado, desechado o reutilizado.
- El procedimiento se mantendrá actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

Lineamiento 141: Cumplimiento de políticas y normas de seguridad. Los líderes de la compañía se deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas. Los resultados de estas revisiones serán mantenidos para su revisión con auditoria.

Lineamiento 142: Cumplimiento técnico. Se debe comprobar periódicamente que los sistemas de información cumplen con las normas de implementación de seguridad. Se deben realizar auditorías

periódicas con ayuda de herramientas automatizadas y se deben generar informes técnicos que reflejen la evaluación de riesgos de seguridad de la información, las vulnerabilidades y su grado de exposición al riesgo.

5. EXCEPCIONES

Las excepciones a cualquiera de los lineamientos de la Política de Seguridad de la Información deben ser aprobados por Líder de Tecnología, la cual puede requerir autorización de la gerencia de La Reforestadora Integral de Antioquia S.A. y del Líder de Talento Humano y Soluciones Organizacionales. Todas las excepciones a la política deben ser formalmente documentadas, registradas y revisadas.

Elaboró
Iván Darío Gutiérrez De La Hoz
Soporte TI

Aprobó

Carolina Vélez Guerra
Dirección Administrativa