POLÍTICA DE SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD

OBJETIVO

Establecer los lineamientos para los controles de seguridad de la información y ciberseguridad necesarios para proteger la confidencialidad, integridad y disponibilidad de la información propiedad de la organización y todas las partes interesadas, apoyados en estándares y buenas prácticas.

DEFINICIÓN DE ABREVIATURAS

Ataque: Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo.

Ataque de diccionario: Intento de averiguar una contraseña o un nombre de usuario probando todas las palabras del diccionario.

Confidencialidad: Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados.

Control: Medida que modifica un riesgo.

Disponibilidad: Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada. En el contexto de los sistemas de información se refiere a la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.

Integridad de la información: Se refiere a la exactitud y consistencia generales de los datos o expresado de otra forma, como la ausencia de alteración cuando se realice cuando se realice cualquier tipo de operación con los datos, lo que significa que los datos permanecen intactos y sin cambios.

Malware: Programa malicioso y/o código maligno, cuyo objetivo es realizar acciones dañinas en un sistema informático permitiendo entre otros el robo o secuestro de información.

Riesgo: Efecto de la incertidumbre sobre la consecución de los objetivos.

SOX (Ley Sarbanes-Oxley): Reglamentación de controles para mejorar la calidad de la información financiera, teniendo en cuenta como base el control interno, gobierno corporativo, independencia de las auditorias y el aumento de las sanciones por delitos financieros.

1 ALCANCE

Aplica para **SIERRACOL ENERGY ARAUCA, LLC., SIERRACOL ANDINA, LLC., & SIERRACOL CONDOR, LLC.** o bien **COLOMBIA ENERGY DEVELOPMENT Co. (CEDCO).** y todas las partes interesadas, en sus servicios en todos los niveles, como parte de su práctica y gestión de todos los procesos de negocio, estratégicos, operacionales y de soporte. Este documento se encuentra en seguimiento y cumplimiento del estándar ISO 27001 – 2013, ISO 27018, Ley 1581 de 2012 y en el Decreto 1377 de 2013.

Todos los lineamientos definidos en esta política y controles establecidos por la organización para la seguridad de la información, ciberseguridad, incluidos los controles normativos y controles SOX, son de obligatorio cumplimiento para todos los colaboradores, contratistas y demás partes interesadas y puede ser objeto de sanciones por su incumplimiento.

2 AMBITO DE APLICACIÓN

Los presentes lineamientos en materia de seguridad de la información y ciberseguridad son de aplicación general y de cumplimiento obligatorio para todo el personal de Sierracol y sus filiales, así como las condiciones técnicas de los equipos de cómputo y/o dispositivos móviles personales que por alguna razón justificada necesiten ser ingresados a las redes de organización.

Los terceros que por motivos de proyectos, prestación o contrato de servicios profesionales hagan uso de los recursos informáticos y de información de Sierracol y sus empresas, deberán atender los presentes lineamientos de manera obligatoria, con la revisión y supervisión de las áreas correspondientes.

3 USO ADECUADO DE LOS RECURSOS Y ACTIVOS DE INFORMACIÓN

Todos los sistemas de información de la Compañía deben usarse únicamente con fines corporativos. Se permite el uso personal incidental siempre que no involucre una cantidad significativa de recursos de la Compañía, como tiempo de trabajo, tiempo de computadora, almacenamiento, ancho de banda o según se especifique en las siguientes secciones. Todos los datos enviados, recibidos, compuestos o almacenados en los Sistemas de Información de la Empresa son propiedad exclusiva de la organización.

3.1 Uso de los sistemas de información

3.1.1 Los sistemas de información de la Compañía no se pueden usar para acceder, descargar, almacenar, transmitir o difundir contenido o materiales ilegales, abusivos, engañosos, obscenos, difamatorios, ofensivos, amenazantes o inapropiados, incluidos, entre otros: material sexualmente explícito o material que contenga insultos étnicos o calificativos raciales; o cualquier cosa que pueda interpretarse como acoso o menosprecio de otros.

3.1.2 Los usuarios no deben restringir, inhibir, interferir, interrumpir o degradar deliberadamente el rendimiento (independientemente de la intención) de ninguno de los sistemas de información de la empresa. Los usuarios no deben impedir la capacidad de otros para usar los sistemas de información de la Compañía.

3.2 Software

3.2.1 Los usuarios no deben exportar software, información técnica, software de encriptación u otra tecnología en violación de las leyes de control de exportación de Colombia o regionales. Las áreas de Supply Chain Management y Legal deben ser consultadas previo a la exportación de cualquier información de la referencia.

3.2.2 Sin importar el tipo de licenciamiento, los usuarios no deben instalar ni copiar software en los Sistemas de información de la Compañía sin la aprobación previa de Tecnología de la información.

3.3 Seguridad de Información

3.3.1 Los usuarios deben completar toda la capacitación de concientización sobre la seguridad de los sistemas de información asignada dentro de los 8 días posteriores a la asignación.

3.3.2 Los usuarios están sujetos a ejercicios periódicos de capacitación en phishing cibernético o ingeniería social cibernética relacionada. En caso de fracaso repetido de tales ejercicios, el Usuario puede estar sujeto a requisitos de capacitación adicionales, acceso reducido al sistema o acción disciplinaria, incluida la terminación de contrato.

3.3.3 Los usuarios no deben reenviar información confidencial de la empresa a ningún sistema de almacenamiento externo, correo electrónico personal o servicio en la nube no aprobado.

3.3.4 Cada Usuario debe proteger la Información Confidencial de la Compañía salvaguardando los activos digitales accesibles o mantenidos por el Usuario.

3.3.5 Los usuarios deben informar a ciberseguridad el robo, pérdida o divulgación no autorizada de los datos de la empresa que se encuentran en los Sistemas de Información.

3.3.6 Los usuarios no deben proporcionar a personal no autorizado acceso a ninguno de los sistemas de información de la Compañía sin aprobación previa.

3.3.7 Los usuarios no deben afectar negativamente o deshabilitar intencionalmente el funcionamiento del software o la configuración de seguridad instalados en los Sistemas de Información de la Compañía.

3.3.8 Los usuarios no deben intentar eludir intencionalmente los controles de filtrado de Internet o los controles establecidos para evitar el acceso a áreas restringidas de la red de SIERRACOL.

3.3.9 La utilización de USB y otros dispositivos de almacenamiento portátiles están restringidos para proteger la información confidencial de la organización y no introducir malware en ninguno de los sistemas de información de la empresa.

3.4 Privacidad

3.4.1 Excepto donde lo prohíba la ley, se recuerda a los Usuarios que no existe clasificación de privado en los datos creados, almacenados, enviados o recibidos mediante los sistemas de información de la compañía.

3.4.2 Excepto donde lo prohíba la ley, la Compañía tiene derecho a monitorear, registrar y archivar todos los aspectos de sus Sistemas de información, incluidos, entre otros, el uso de Internet, las tecnologías de mensajería y cualquier otra comunicación dentro de las redes de la Compañía. Esta información se puede proporcionar a terceros en relación con el descubrimiento legal o reglamentario o las solicitudes de documentos de acuerdo con las leyes aplicables.

3.5 Propiedad Intelectual

Los usuarios deben colaborar con la protección y gestión del software y los derechos de propiedad intelectual. Los usuarios tienen estrictamente prohibido realizar acciones que violen los derechos de propiedad intelectual de cualquier persona o empresa protegida por derechos de autor, secretos comerciales, patentes u otras leyes o reglamentos de propiedad intelectual o similares. Está prohibido instalar, distribuir, descargar o copiar productos piratas u otros productos digitales que no tengan la licencia adecuada para su uso por parte de la Compañía.

3.6 Bring Your own Device (BYOD)

Los usuarios pueden utilizar dispositivos informáticos personales para acceder a los recursos de la Compañía a través del registro en el sistema de Administración de Dispositivos Móviles (MDM) de la Compañía u otros sistemas de acceso remoto aprobados por la Compañía y deben cumplir con la Política de Seguridad de la Información y Ciberseguridad.

3.7 Equipo de Cómputo

3.7.1 Los usuarios que dispongan de equipos de cómputo, móviles y sistemas informáticos asignados por la organización serán responsables de su buen uso, por lo que evitarán:

3.7.1.1 Compartir, copiar, mover, borrar o imprimir información, donde no se hayan otorgado la autorización explícitamente a los dueños de la información.

3.7.1.2 Interceptar, manipular o alterar datos sobre la red, con intenciones de afectar la confidencialidad e integridad de la información.

3.7.1.3 Enviar comandos, ejecutar programas o mensajes de cualquier tipo, con la intención de interferir, deshabilitar los equipos de cómputo o comunicaciones, a través de la red o localmente.

3.7.1.4 Instalar y/o distribuir software que no se encuentre autorizado para ser usado en los equipos de cómputo y sistemas, acorde al inventario de software autorizado.

3.7.1.5 Deshabilitar, desinstalar o modificar la operación del software de protección de dispositivos de usuario final y demás herramientas, lineamientos y controles de ciberseguridad.

3.7.1.6 Descargar y distribuir programas o código maliciosos a través de la red, así como en documento adjunto de correos cloud electrónicos, como son: virus informáticos, spyware, programas troyanos, entre otros.

3.7.1.7 Descargar, almacenar o reproducir en línea archivos de música, video, no relacionados con las actividades de Sierracol.

3.7.1.8 Instalar software que no cuente con licencia y el soporte correspondiente por parte de Sierracol.

3.7.2 Los usuarios deben tomar medidas razonables para proteger el equipo de cómputo proporcionado por la Compañía contra robo o uso indebido.

3.7.3 Devolver el equipo propiedad de la Compañía a Tecnología de la Información o su designado, al terminar el empleo o el período del contrato.

3.7.4 Será responsabilidad de los usuarios respaldar la información que se encuentre bajo su resguardo en los equipos de cómputo asignados en las herramientas tecnológicas dispuestas por parte de tecnología de la información.

3.8 Email

3.8.1 Los usuarios deben tener el debido cuidado al abrir mensajes de correo electrónico de fuentes externas, ya que se puede introducir malware en los sistemas de información de la Compañía al abrir archivos adjuntos maliciosos o al hacer clic en enlaces web contenidos en el mensaje de correo electrónico.

3.8.2 Los usuarios no deben falsificar la información del encabezado del correo electrónico de la Compañía.

3.8.3 Los usuarios deben utilizar los sistemas de correo electrónico de la Empresa u otros Sistemas de información con el entendimiento de que estos recursos se proporcionan en beneficio de los negocios de la Empresa. El correo electrónico o los sistemas de información de la Compañía no deben usarse para solicitar asistencia social, política, ayuda u otras causas benéficas sin la aprobación previa por escrito de Recursos Humanos. (Esta sección no se interpretará en el sentido de restringir el derecho del Personal de SIERRACOL a participar en actividades concertadas para su ayuda o protección mutua, incluida la solicitud de afiliación a una organización laboral).

3.9 Redes Sociales

Los usuarios son responsables de cumplir con las Políticas de la Compañía con respecto al uso adecuado de las redes sociales y abstenerse de entrar en polémicas que puedan degradar la imagen de la organización, así como realizar publicaciones propias en nombre de la empresa.

4 SEGURIDAD EN EL MANEJO DE INFORMACIÓN

4.1 Clasificación de la información

4.1.1 Los dueños de la información son responsables de asignar la clasificación correspondiente de acuerdo con la criticidad y sensibilidad de la información.

4.1.2 El dueño de la información, de acuerdo con su clasificación, debe autorizar la publicación, compartición o divulgación de la información y definir los términos de su manejo y administración.

4.1.3 Los controles de seguridad sobre la información deben corresponder a la clasificación asignada.

4.1.4 La información debe clasificarse de acuerdo con los siguientes parámetros:

Tipo de Información	Descripción
Confidencial	Toda información de la compañía que no sea de conocimiento público e información estratégica cuya divulgación, pérdida o alteración no autorizada, podría resultar en desprestigio, pérdidas económicas o de clientes para la compañía, incluyendo datos personales y sensibles de los clientes y personal interno y externo.
Critica	Información táctica y operativa necesaria para mantener operativos los procesos core de negocio.
Uso Interno	Información táctica u operativa requerida por las partes interesadas para el desarrollo normal de sus actividades o funciones.
Pública	Información cuya distribución, publicación o divulgación ha sido formalmente autorizada y distribuida por los canales de comunicación formalmente establecidos.

4.1.5 La etiqueta de clasificación *Pública* solo puede ser otorgada con el aval correspondiente de las áreas jurídicas de Sierracol o quienes ellos dispongan para este fin.

4.2 Respaldo de la información

4.2.1 Es responsabilidad de los líderes de procesos y gerentes de área garantizar que la información considerada como critica sea almacenada en los servidores de la empresa según la disposición que esta tenga para los mismos.

4.2.2 La información debe ser respaldada y recuperada periódicamente de acuerdo con la clasificación definida por cada dueño de la información; así mismo es necesario garantizar pruebas de restauración periódica de los backups, para verificar la disponibilidad e integridad de la información. La gerencia de tecnología de la información y su designado deben ser los responsables de coordinar estas actividades.

4.2.3 Por ningún motivo se permite alojar en servidores información personal, música, videos, documentos transitorios, backups de equipos de escritorio, backups de correo electrónico y demás que no sea relevante en el cumplimiento de los objetivos de Sierracol.

4.2.4 Para la gestión de archivos compartidos de los usuarios, tecnología de información dispondrá los medios oficiales para cada una de las áreas de la compañía en un servidor de archivos dando cumplimiento al proceso de retención documental definida por cada grupo.

4.3 Acceso de la información

4.3.1 Los usuarios no deben eludir la autenticación de usuario ni la seguridad de ninguno de los sistemas de Información de la Compañía.

4.3.2 Los usuarios no deben divulgar a terceros no autorizados ninguna Información confidencial de la empresa. Las credenciales de los sistemas de información de la empresa (identidad de usuario/combinación de contraseña) se consideran información confidencial de la empresa y son exclusivamente para su uso previsto. La divulgación no autorizada de las credenciales de acceso está estrictamente prohibida.

4.4 Transferencia o transmisión de la información

4.4.1 Los usuarios deben utilizar únicamente los mecanismos y herramientas proporcionadas por la compañía para el envío o recepción de información.

4.4.2 Todo requerimiento de información que no sea de conocimiento público de la compañía, realizado por un tercero, incluyendo entidades estatales, proveedores, clientes, personas jurídicas etc., debe ser previamente validada y autorizada por la VP Jurídica (General Counsel), con el fin de determinar la viabilidad de compartir la información requerida por el tercero.

4.5 Destrucción de información

4.5.1 La información que ya ha cumplido con su ciclo de vida, que no sea valiosa o utilizada por el dueño de la información debe ser eliminada de forma segura y confiable, sin opción de ser recuperada, de acuerdo con la tabla de clasificación de información. Ver ítem 4.1.4 del presente documento.

4.5.2 Registrar por acta de la destrucción de la información.

5 CONTROLES CRIPTOGRAFICOS

Se debe garantizar que los sistemas o aplicaciones que realicen y/o permitan la transmisión de información confidencial o crítica, lo realicen mediante herramientas de cifrado de datos a través de algoritmos criptográficos fuertes, es decir aquellos que a la fecha no han sido vulnerados.

5.1 Herramientas de encripción

5.1.1 El área de Tecnologías de Información proveerá la herramienta de encripción de datos a los usuarios, previa solicitud formal.

5.1.2 La asignación de la clave para el cifrado de la información en la herramienta debe ser establecida por el usuario que administra dicha información, teniendo siempre presente que, en caso de olvidar la clave, la información cifrada no es recuperable.

5.2 Protección de la confidencialidad

Cuando un activo de información es clasificado como confidencial, debe protegerse con la aplicación de un algoritmo criptográfico fuertes, es decir aquellos que a la fecha no han sido vulnerados.

5.3 Protección de la integridad

Los mecanismos de protección de integridad se definen con base en los dos niveles más altos de clasificación del activo de información, resultado de los ejercicios de riesgos aplicados por Tecnología de Información de la siguiente manera:

- **Muy Alto**: para los activos de información que estén clasificados en este nivel y para los cuales se haya identificado riesgo por encima del NRA (Nivel de Riesgo Aceptable) la verificación de integridad se debe realizar con la aplicación de los algoritmos de firma digital o hashing, de acuerdo con la criticidad de la situación.
- **Alto**: para los activos de información que estén clasificados en este nivel y para los cuales se haya identificado riesgo por encima del NRA (Nivel de Riesgo Aceptable) la verificación de integridad se debe realizar mediante los lineamientos establecidos en las políticas de monitoreo y control de accesos.

6 PROTECCIÓN DE REDES

6.1 6.1 Sobre la Red de Negocio

6.1.1 Se debe contar con controles de acceso físicos y lógicos que garanticen que solo las personas y dispositivos autorizados pueden acceder a los elementos de red, la información almacenada, los flujos de información y los servicios.

6.1.2 El personal que administre u opere dispositivos de comunicaciones o seguridad en la red, deben cumplir con el principio de segregación de funciones mediante la asignación de roles y privilegios. Por la importancia de los equipos de comunicaciones y seguridad solo existirá en caso de ser necesario una cuenta administrativa genérica del dispositivo y quedará a resguardo

del responsable informático asignado por el gerente de TI. La operación de estos equipos se realizará mediante cuentas personalizadas con privilegios específicos.

6.1.3 Los administradores de redes de datos de organización atenderán el perfil de seguridad que se autorice para la operación de los dispositivos de comunicaciones o seguridad en la red. Los cuales atenderán las siguientes configuraciones:

6.1.3.1 Configuración de bitácoras de seguridad hacia servidor de correlación de eventos con la persistencia de información de 6 meses, donde se almacene esta información para propósitos estadísticos y de ciberseguridad.

6.1.3.2 Integración al sistema de monitoreo de sistemas e infraestructura.

6.1.3.3 Establecer los mecanismos para la identificación de manera oportuna de la fuente de posibles riesgos o violaciones a los lineamientos de ciberseguridad.

6.1.4 Se debe contar con controles que garanticen la disponibilidad de la red en caso de que la misma presente alguna anomalía ante cualquier tipo de vulnerabilidad o evento de seguridad.

6.1.5 En caso de detectarse actividades sospechosas o ilícitas que atenten contra la confidencialidad, integridad o disponibilidad de la información, se debe bloquear, ocultar, negar, aislar o descontinuar el servicio de red, sin previo aviso, a los sistemas y usuarios involucrados.

6.1.6 No está permitido exponer servicios, portales, repositorios, APIs o equipos internos de la compañía a internet, si no se ha llevado a cabo previamente el análisis de riesgos por parte de ciberseguridad y si no se han implementado las medidas de seguridad definidas al respecto por la compañía.

6.2 Sobre la Conectividad Remota

6.2.1 Los usuarios autorizados realizarán el acceso haciendo uso de una conexión de red privada virtual (Virtual Private Network / VPN) la cual será personal e intransferible y deberá cumplir con el principio de conexión a través de certificado. El acceso será desde un equipo de cómputo que cumpla con el perfil de seguridad requerido para el acceso remoto.

6.2.2 Los equipos que sean detectados en incumplimiento de los presentes lineamientos podrán ser bloqueados sin previo aviso, restringiéndoles el acceso remoto autorizado a la red de Sierracol.

6.3 Sobre las redes inalámbricas

6.3.1 La red inalámbrica de Sierracol y sus empresas, ofrecerán un acceso administrado por lo que su uso es restringido y controlado, este servicio se proporcionará atendiendo los siguientes requerimientos:

6.3.1.1 El servicio de esta red será accesible exclusivamente al interior de las instalaciones de Sierracol y sus empresas.

6.3.1.2 El protocolo mínimo de seguridad aceptable será WPA2-AES.

6.3.1.3 La plataforma de administración de red inalámbrica implementará los mecanismos de seguridad que permitan identificar y notificar intentos de acceso no autorizados, detectar y bloquear dispositivos de acceso falsos.

6.3.1.4 La plataforma de administración de red inalámbrica en Sierracol y sus empresas mantendrán registros de cada acceso por usuario y por dispositivo por al menos 3 meses.

6.3.1.5 Sierracol contará con la validación de la configuración de seguridad de las redes inalámbricas.

6.4 Sobre las redes de invitados

6.4.1 El uso de redes de invitados está autorizado siempre que estas se encuentren aisladas de la red de datos corporativas, y se cumplan con el perfil base de seguridad definido por ciberseguridad para este propósito, debiendo documentarlo para la verificación y autorización correspondiente.

6.4.2 Se debe mantener actualizado el inventario de redes de invitados y cualquier cambio sobre las mismas debe ser notificado y autorizado por ciberseguridad.

6.4.3 Las redes de invitados deben contar con pruebas de seguridad que garanticen la correcta configuración y confiabilidad de estas.

6.4.4 El acceso a la red de invitados será otorgado por los empleados directos de Sierracol bajo el principio de uso adecuado y razonable de los recursos y será su responsabilidad la administración de dichos accesos y recursos.

6.5 Sobre la interconexión entre las redes de automatización y las redes de negocio

La administración, operación y gestión de los dispositivos, red e infraestructura de la red de automatización deberán estar alineados a la normatividad correspondiente en la materia, definida por los entes reguladores de Sierracol y de la Asociación Colombiana de Petróleo y Gas ACP. Las interconexiones entre redes de automatización (red operativa) y la red de negocio deberán considerar:

6.5.1 Las conexiones entre las redes de automatización y la red de negocios, en ninguna circunstancia deberán ser comunicaciones directas; es decir, las redes no serán visibles entre sí. En ninguna circunstancia se autorizará la conexión directa a internet de los segmentos de automatización.

6.5.2 El direccionamiento IP de la red de automatización será distinto al de la red de negocios, preferentemente sobre un segmento de direccionamiento privado y aislado de la red.

6.5.3 Las empresas o áreas que requieran para su operación establecer una conexión entre la red de automatización y la red de negocios:

6.5.3.1 Solicitarán la validación al área correspondiente del esquema de seguridad de conexión entre la red de automatización y la red de negocios.

6.5.3.2 En caso de autorizarse por el área correspondiente, los puntos de conexión entre las redes de automatización y la red de negocios cumplirán con el esquema de conexión segura autorizado por el área de Ciberseguridad.

6.5.3.3 En el punto de conexión entre las redes de automatización y la red de negocios se instalará un dispositivo de seguridad de propósito específico con al menos capacidad de Firewall, IPS, VPN y preferentemente módulos de ATP (Advanced Threat Protection).

7 SEGUIMIENTO Y MONITOREO DE CIBERSEGURIDAD

7.1 Monitore de redes

7.1.1 Ciberseguridad establecerá los mecanismos para las prácticas de monitoreo sobre las redes de datos, equipos y sistemas informáticos a través de los esfuerzos de control de riesgos de Sierracol, realizando una vigilancia permanente de los eventos de seguridad que generan los recursos informáticos, sistemas críticos y de operación de la organización, con la finalidad de identificar brechas de seguridad y evaluar el nivel de seguridad de la infraestructura tecnológica.

Estas actividades las realizará Ciberseguridad con la infraestructura y herramientas de seguridad de la información y con los procesos que se definan y comuniquen al interior de las áreas de la organización según sea el caso.

7.1.2 Ciberseguridad coordinará los esfuerzos de monitoreo de la marca Sierracol y sus empresas en Internet, contra fraudes cibernéticos, incluido el basado en correos electrónicos, contra el uso mal intencionado y fraudulento de la imagen institucional.

7.1.3 Las revisiones de seguridad a los equipos de cómputo, de comunicaciones, seguridad, sistemas informáticos y servidores que indican estos lineamientos, serán realizados y/o supervisados por Ciberseguridad.

7.2 Infraestructura informática de refuerzo para la Ciberseguridad

7.2.1 Se debe contar con una infraestructura informática que permita aplicar los controles de ciberseguridad y seguridad de la información derivados de esta política.

7.2.2 Una infraestructura de directorio activo que atienda el esquema de jerarquías y dominios, que facilite el cumplimiento a los perfiles de configuración base de equipos de cómputo y servidores.

7.2.3 Los equipos de cómputo de escritorio, laptops, servidores, dispositivos móviles conectados a la red de datos tendrán instalado y en ejecución el software de seguridad definidos por Ciberseguridad en conjunto con las áreas interesadas.

7.2.4 Tecnología de la información debe proporcionará la infraestructura necesaria para almacenar la información de accesos a los recursos informáticos con propósitos estadísticos y de correlación de seguridad.

7.2.5 Se debe considerar al menos para la infraestructura crítica de negocio o de tecnología un Plan de Continuidad de Negocio y un Plan de Recuperación de Desastres (BCP/DRP).

7.2.6 Los servidores de archivos, aplicaciones, portales web internos, bases de datos, servicios cloud, entre otros, que se determinen como críticos se deberán localizar en un centro de datos que cumpla con las condiciones de seguridad física como es el monitoreo por CCTV, control de acceso y seguridad, entre otros.

7.2.7 Los sistemas operativos de los servidores deben cumplir con el perfil de seguridad (hardening) que Ciberseguridad defina para cada propósito, en todos los casos se contará con la configuración base de servidores dependiendo del sistema operativo.

8 CONTROL DE ACCESOS A LOS SISTEMAS DE INFORMACIÓN

8.1 Cuentas de usuario y contraseñas

8.1.1 Todo usuario creado en los sistemas de información debe estar asociado a un empleado activo vinculado a través de contrato laboral con Sierracol o contrato comercial en el caso de terceros o contratistas.

8.1.2 En el caso de personal de terceros, se requiere contar con el soporte del estudio de seguridad vigente según las políticas internas definidas para tal fin.

8.1.3 El acceso a los sistemas de información debe concederse bajo el principio de mínimo privilegio posible y por una necesidad de negocio justificada; es responsabilidad de quien aprueba una solicitud garantizar que este principio se cumpla.

8.1.4 Las cuentas de usuario son únicas, personales e intransferibles, por tanto, no serán compartidas ni reveladas a terceros de manera personal o electrónica.

8.1.5 Los usuarios y administradores para la protección de las cuentas de acceso personal generarán contraseñas robustas, las cuales deberán cumplir con las siguientes características mínimas:

- Longitud mínima de 14 caracteres.
- Contener al menos:
  - 1 carácter en MAYÚSCULA.
  - 1 carácter en minúscula.
  - 1 carácter numérico.
  - 1 carácter especial.
- Vigencia de 90 días o menos.
- No permitir reúso de las últimos 24 contraseñas.
- Expirar la sesión por inactividad mayor a 15 minutos.
- Evitar utilizar contraseñas genéricas como Sierracol2022*, Colombia2022*.

- No generar patrones o secuencias en las contraseñas.

8.1.6 Para reducir los riesgos de accesos no autorizados, los usuarios evitarán en sus contraseñas el uso de palabras basadas en información personal, como nombres de familiares, mascotas. Los usuarios evitarán escribir las contraseñas en papel y evitar mantener a la vista las contraseñas.

8.1.7 Tecnología de la información debe habilitar en los sistemas informáticos, infraestructura de directorio y equipos que lo soporten, los mecanismos de validación de la política de contraseña robusta durante la generación de estas.

8.1.8 En los sistemas críticos y aquellos con exposición a Internet, se incorporarán mecanismos de protección a los accesos de usuario contra ataques por diccionario, bloqueando el acceso a la cuenta de manera temporal al tercer intento fallido, y en los casos que la tecnología lo permita se exige habilitar los mecanismos de doble factor de autenticación.

8.1.9 En los sistemas que lo permitan, deberán habilitarse mecanismos de factor de autenticación múltiple (MFA Multiple Factor Authentication).

8.1.10 Se realizará bloqueo del usuario luego de 6 intentos fallidos en la contraseña.

8.2 Gestión de privilegios en Sistemas de Información

8.2.1 Perfil de aplicaciones

8.2.1.1 Cada área de negocio es responsable de definir los roles y privilegios en los sistemas de información que se otorgan acceso a sus empleados de acuerdo con el rol funcional que desempeña en la organización. Estos privilegios deben estar aprobados por el gerente o vicepresidente del área y deben registrarse como soporte de la solicitud en los sistemas de autoatención dispuestos por la organización.

8.2.1.2 Los miembros del Management Team tienen la potestad de definir de forma autónoma los accesos y privilegios que consideren deben tener en los sistemas de información de la compañía, por tanto, no requieren de avales adicionales para solicitar modificaciones en los accesos asociados a su cargo.

8.2.1.3 Para el caso de permisos terceros o aliados el administrador del contrato o Gerente de área debe aprobar los accesos solicitados.

8.3 Gestión de accesos

8.3.1 Es responsabilidad de Recursos Humanos y los administradores de contratos o Gerente de área, que cada vez que se presente el ingreso de un empleado directo, tercero o contratista, realizar el registro del funcionario en la herramienta dispuesta por la compañía para dicho fin según sea el caso.

8.3.2 Todo usuario debe tener asociada una identidad en la herramienta que la compañía defina como gestor de identidades, información que se ingrese en la herramienta de gestión humana de cada empleado directo o tercero debe ser completa y debe identificar de manera individual a cada persona.

8.3.3 La configuración y aprovisionamiento de los accesos en los sistemas de información de la compañía estarán a cargo de la Gerencia de Tecnología de Información o su designado para esta labor.

8.3.4 La gestión de los accesos a cualquier sistema de información debe realizarse, sin excepción, siguiendo los procedimientos y estándares formales establecidos por la compañía. La Gerencia de Tecnología de Información o su designado para esta labor deben garantizar que las solicitudes recibidas para creación, modificación, inactivación o eliminación de cuentas de usuario sean ejecutadas de acuerdo con lo solicitado y a través de los canales oficiales establecidos para dicho fin.

8.3.5 Se definirá una Línea Base de Accesos tanto para empleados directos como aliados que será ejecutada una vez el empleado sea registrado como activo en los sistemas de administración de personal por parte de Recursos Humanos o los Administradores de Contrato o Gerente de área.

8.3.6 Toda solicitud de accesos debe quedar registrada y documentada con los soportes a los que haya lugar en las herramientas de gestión que se dispongan para este fin.

8.4 Registro del acceso

8.4.1 Todos los sistemas de información deben almacenar un registro de accesos que, como mínimo registren la fecha y hora del ingreso, el usuario, actividad ejecutada en el sistema, fecha y hora de logout del sistema.

8.4.2 Es responsabilidad de Recursos Humanos que la información personal y familiar de los empleados sea inequívoca y corresponda a datos reales del usuario. En ese mismo sentido, es responsabilidad de los administradores de contrato o Gerente de área que la información de los terceros sea veraz y se encuentre registrada de forma correcta en los sistemas de la organización.

8.5 Control del acceso

8.5.1 El acceso a los sistemas tenderá al uso de una sola instancia de autenticación basada en el directorio activo, eliminado el uso de múltiples usuarios para la misma persona con el riesgo asociado de múltiples contraseñas.

8.5.2 Es responsabilidad de Recursos Humanos y los Administradores de Contrato informar el retiro de un empleado directo o tercero y su correspondiente registro en los sistemas de información establecidos por la compañía.

8.5.3 Es responsabilidad de Recursos Humanos y los Administradores de Contrato Gerente de área informar las novedades que se presenten con el colaborador directo o tercero tales como: Cambios de cargo, ausencias por licencias (maternidad, remuneradas, no remuneradas, incapacidades, vacaciones) o retiro, estas novedades deben tener su correspondiente registro en los sistemas de información establecidos por la compañía.

8.5.4 responsabilidad de Recursos Humanos y los Administradores de Contrato Gerente de área informar los cambios de cargo de los empleados directos o terceros y su correspondiente registro en los sistemas de información establecidos por la compañía.

8.5.5 Tecnología de información generará los controles de inactivación y desactivación de cuentas sin uso, según las condiciones que considere pertinentes con el fin de optimizar los recursos de licenciamiento de la organización.

9 DESARROLLO Y ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN

9.1 Sobre el desarrollo de sistemas y aplicaciones

9.1.1 Para el desarrollo de aplicaciones y sistemas informáticos, Sierracol y sus empresas a través de los responsables de ciberseguridad y el personal que se defina, deberán incorporar prácticas de desarrollo seguro, así como una fase de pruebas y validación de seguridad previa a su liberación, el cual deberá contar con análisis dinámico y estático de los aplicativos a publicarse, así como pruebas de estrés de los aplicativos, con el propósito de reducir riesgos de seguridad.

9.1.2 Se debe contar con ambientes separados para desarrollo, prueba y producción.

9.1.3 Se debe validar y aprobar por parte de ciberseguridad la arquitectura de seguridad de los sistemas y aplicativos previo a su liberación.

9.1.4 Los sistemas o aplicaciones que requieran ser publicados en internet deben ser sometidos a pruebas de penetración o ethical hacking antes de su puesta en producción.

9.1.5 Se deberá considerar en todas las fases de desarrollo de sistemas y aplicativos la alineación a un marco de referencia de desarrollo seguro.

9.1.6 Los requerimientos de Seguridad de la Información mínimos que se deben observar en la adquisición y desarrollo de software son:

9.1.6.1 Procesos de identificación, autenticación y autorización de usuarios

9.1.6.2 Análisis de roles, perfiles y privilegios de acceso; que den origen a una matriz para su gestión.

9.1.6.3 Los requerimientos de protección para datos personales que puedan manejarse como parte de los desarrollos (Ejemplo, Manejo de datos en

ambientes de desarrollo) y cómo es diseñado el software para la posterior administración de estos datos.

9.1.6.4 El análisis sobre el manejo de logs de acuerdo con tipo de aplicación, su criticidad y funcionalidad.

9.2 Sobre la adquisición de hardware o software

9.2.1 Todo nuevo hardware y software que se vaya a adquirir y conectar a las plataformas de tecnología de Sierracol, por cualquier dependencia o proyecto, deberá ser gestionado por el área de Tecnologías de Información para su correcto funcionamiento.

9.2.2 La instalación del software en los activos informáticos de Sierracol, se realizará únicamente a través del área de Tecnologías de Información.

9.2.3 El área de Tecnologías de Información implementará reglas y herramientas que restrinjan la instalación de software no autorizado en los activos de información de la compañía.

9.2.4 El software que se adquiera a través de proyectos o iniciativas organizacionales debe quedar licenciado a nombre de Sierracol.

10 RELACIÓN CON PARTES INTERESADAS

A partir de la fecha de vigencia de esta política, todos los contratos o acuerdos definidos con la organización deben contar con la firma del anexo de requerimientos de seguridad para terceros y acuerdo de confidencialidad.

Las partes interesadas deben conocer, aceptar y dar cumplimiento a los lineamientos, procedimientos y estándares de ciberseguridad establecidos.

11 INCIDENTES DE CIBERSEGURIDAD

11.1 Los usuarios deben informar de inmediato a ciberseguridad todos los casos de sospecha de mensajes de correo electrónico maliciosos, pérdida de información, uso no autorizado de información, acceso no autorizado, infección por malware o actividad sospechosa observada en las máquinas del Usuario o los Sistemas de Información de la Compañía a través de los medios oficiales dispuestos para este fin.

11.2 Todos los incidentes de seguridad deben ser documentados con el fin de ser fuente de conocimiento, aprendizaje y experiencia.

11.3 Los usuarios deben cooperar en cualquier respuesta o investigación de incidentes de ciberseguridad relacionados con los Sistemas de Información de la Compañía.

11.4 Se debe contar con un equipo de respuesta a incidentes de ciberseguridad encargado de coordinar la respuesta a los incidentes de ciberseguridad o seguridad de información, así como liderar los

flujos de información necesarios para la atención y comunicación de este al interior de la organización y a los entes externos o de la industria y entidades de gobierno.

11.5 El equipo de respuesta a incidentes emitirá los protocolos, procedimientos y guías de atención necesarias para la respuesta a los distintos tipos de incidencias al interior de Sierracol. Para cada uno de los incidentes declarados, se emitirá reporte técnico con carácter de dictamen que proporcionará la evidencia del caso para aplicar las sanciones y las medidas correctivas que correspondan.

11.6 El equipo de respuesta a incidentes recurrirá a los procedimientos de respuesta a incidentes para revisar los recursos informáticos, en caso de identificar o de ser notificado de algún incumplimiento o posible violación de las políticas de ciberseguridad, y determinar las acciones correctivas pertinentes.

12 GESTIÓN DE RIESGOS DE CIBERSEGURIDAD

12.1 Se deberán gestionar los riesgos derivados de amenazas o vulnerabilidades en la ciberseguridad.

12.2 Para realizar un control efectivo de los riesgos de ciberseguridad de la infraestructura informática y la red de negocios, la gerencia de tecnología de información y el responsable de ciberseguridad, así como el personal que se defina, participarán en el proceso consolidado de gestión de riesgos de ciberseguridad, así como en la definición de la metodología de evaluación de riesgos.

12.3 Sierracol a través del responsable de ciberseguridad y el personal que se defina:

12.3.1 Notificarán a las áreas la designación del responsable del seguimiento a los procesos de mitigación de riesgos para que se ejecute la remediación correspondiente según sea el caso.

12.3.2 Actualizarán el inventario de riesgos y su evolución de acuerdo con el ciclo de riesgos de ciberseguridad.

12.3.3 Coordinará las acciones de mitigación a los riesgos identificados en el análisis de riesgos.

12.3.4 Informará a través del CEC – Comité Estratégico de Ciberseguridad las acciones para la mitigación de los riesgos y los riesgos residuales que estén por fuera del NRA – Nivel de Riesgos Aceptable de la organización.

12.4 Se debe realizar ejecución periódica de escaneos de vulnerabilidades y pruebas de penetración sobre todos los sistemas de información, las plataformas e infraestructura que los soportan y adoptar las medidas adecuadas para tratar el riesgo asociado.

12.5 Toda implementación nueva o de mejora sobre cualquier sistema de información debe contar con su respectivo análisis continuo de vulnerabilidades. La mitigación de los hallazgos estará a cargo del responsable de la implementación o mejora durante el tiempo de implementación según sea el caso.

13 TRATAMIENTO DE LA INFORMACIÓN Y DATOS PERSONALES

La compañía cumple con lo establecido en la Ley 1581 de 2012 y en el decreto 1377 de 2013 que regula la protección de datos personales y en especial la atención de consultas y reclamos relacionados, así como con los artículos 15 y 20 de la Constitución Política.

Se deben cumplir con la política de tratamiento de la información y datos personales establecida por la organización, garantizando los derechos para los titulares de los datos de carácter personal, registrados en cualquier base de datos que los haga susceptibles de tratamiento por parte de Sierracol Energy y en los procesos que esta soporta.

La política de tratamiento de la información y datos personales es de carácter obligatorio para la compañía en calidad de responsable del tratamiento de datos, así como para los encargados que realizan el tratamiento de datos personales por cuenta de Sierracol.

Tanto el responsable como los encargados deben salvaguardar la seguridad de las bases de datos que contengan datos personales y guardar la confidencialidad respecto del tratamiento.

Se deben tomar todas las precauciones razonables y medidas de índole técnico, administrativo y organizacional conducentes a garantizar la seguridad de los datos de carácter personal de los titulares, principalmente aquellos destinados a impedir su alteración, pérdida y tratamiento o acceso no autorizado, con el fin de garantizar la conservación, confidencialidad, integridad y disponibilidad de los datos, en la prestación de todos los servicios tecnológicos de la compañía, incluidos, entre otros, los servicios on premises y cloud.

14 EXCEPCIONES

Las excepciones a esta Política deben ser documentadas por escrito y aprobadas por el líder de Ciberseguridad y el Gerente de TI de la Compañía.