ANDINA DE ENERGÍA S.A.S.
ANDIENERGÍA

POLÍTICA DE SEGURIDAD INFORMATICA

Contenido

1. Introducción

La seguridad Informática, es un proceso donde se deben evaluar y administrar los riesgos, apoyados en políticas y estándares que cubran las necesidades de GESTION Y DISEÑOS ELECTRICOS S.A.S., (en adelante la compañía) en materia de seguridad de la información.

Las normas y políticas expuestas en este documento sirven de referencia, en ningún momento pretenden ser normas absolutas, las cuales están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad de la información y los servicios prestados por la red a los usuarios finales.

El documento pretende, ser el medio de comunicación en el cual se establecen las reglas, normas, controles y procedimientos que regulen la forma en que la Compañía, prevenga, proteja y maneje los riesgos de seguridad en diversas circunstancias

2. Objetivo de la política de seguridad

La política de seguridad Informatica proporciona la base para la aplicación de controles de seguridad que minimizan los riesgos y las vulnerabilidades que puedan atentar contra la infraestructura tecnológica de la compañia y su entorno. Se aclarará la responsabilidad de los usuarios y las medidas que se deben adoptar en la compañía, para proteger la información y la tecnología de la Compañía para evitar pérdidas y/o la divulgación no autorizada de esta.

3. Alcance

La Política de Seguridad Informatica está orientada a establecer medidas para proteger las tecnologías informáticas (Equipos de cómputo, sistemas de información, redes, servidores etc.) y las demás necesarias para asegurar la confidencialidad, integridad, confidencialidad y disponibilidad de la información. Lo dispuesto en este documento debe ser cumplido por todos los funcionarios de la compañía, sin excepción.

3.1 Marco de la gestión de seguridad de la información

La política y procedimientos incluidos en este documento deben ser cumplidos por todo el personal de la compañía, incluidos los contratistas.

La política de seguridad Informatica es muy importante para la compañía, y es de vital importancia que su información esté protegida de acuerdo con el valor crítico y el carácter delicado de la misma y la tecnología que soporta la operación diaria, se tomarán las medidas de seguridad descritas a continuación para su cumplimiento.

4. Ámbito de aplicación

4.1 Los empleados y/o Colaboradores vinculados mediante contrato de prestación de servicios profesionales

Seguridad de la información es un esfuerzo de equipo. Requiere la participación y el apoyo de todos los miembros de la Compañía que trabajan con sistemas de información y/o tienen a su cargo herramientas tecnológicas. El no cumplimiento generará incumplimiento al Reglamento Interno de Trabajo.

4.2 Infraestructura

Esta política se aplica a todos los equipos, redes, aplicaciones, software ofimático, base de datos y sistemas operativos de propiedad y/o operados por las personas de la compañía, así como los archivos y datos producto del trabajo realizado por sus empleados cuya propiedad es de la compañía.

5. Roles y responsabilidades

Las divisiones para administrar seguridad de la información

La Coordinación Informática es responsable de:

- Establecer y mantener la política de seguridad Informatica, las normas, directrices y procedimientos de la compañía, referentes a tecnología.
- Monitorear la infraestructura para asegurar la seguridad de la información.
- Investigar sobre las vulnerabilidades de los sistemas y otros incidentes de seguridad de la información.
- La Coordinación Informática debe garantizar el cumplimiento de la política de sistemas, procedimientos y cualquier legislación aplicable referente a tecnología y seguridad de la información, con el apoyo directo del Departamento Jurídico.
- Los Coordinadores de las diferentes áreas o Directores de Proyecto, la Dirección Jurídica junto con la Gerencia General y la Coordinación Informática son responsables de enviar los casos disciplinarios en respuesta a violaciones de normas de seguridad de la información de conformidad con lo establecido en el artículo 45 del Reglamento Interno de Trabajo.

6. Categorías de responsabilidad

Con el fin de coordinar los esfuerzos en seguridad, la compañía, ha dividido las responsabilidades de sus miembros en tres categorías.

6.1 Responsabilidades del usuario

- Los usuarios deben familiarizarse con el contenido de la política, conocerla y aplicarla en todas las actividades que realice para la compañía.
- Los responsables de los activos informáticos de propiedad de la compañía son los gerentes, directores, coordinadores, analistas, empleados y colaboradores, que, de acuerdo con sus funciones, deban generar cualquier tipo de información o adquirir herramientas para la generación de la información.
- La Coordinación Informática asistirá a todos los usuarios en la adquisición de hardware, software, sistemas de información, sitios de almacenamiento externo que apoyan la toma de decisiones y otras actividades organizativas.
- Cada aplicación operativa debe tener un responsable designado y cada usuario tendrá la responsabilidad de custodiar y administrar adecuadamente los recursos y la información que maneja.
- El usuario no podrá modificar, desinstalar o evitar la ejecución de los programas instalados por la Coordinación de Informática.

6.2 Responsabilidades del propietario

- Los responsables de los activos informáticos de propiedad de la compañía son generalmente los gerentes, directores, coordinadores, analistas y empleados que de acuerdo con sus funciones deban generar cualquier tipo de información o adquirir herramientas para la generación de la información. La Coordinación Informática asistirá a todos los usuarios en la adquisición de hardware, software, sistemas de información, sitios de almacenamiento externo que apoyan la toma de decisiones y otras actividades organizativas.

- Cada aplicación operativa debe tener un responsable designado y cada usuario tendrá la responsabilidad de custodiar y administrar adecuadamente los recursos y la información que maneja.

6.3 Responsabilidades de los administradores de la información

- El personal de la Coordinación Informática y los usuarios que manejan información en sus computadoras o cualquier equipo tecnológico que almacene datos, son los responsables de esta y de la información contenida en él.
- Todo funcionario interno o externo que labora para la Compañía como responsable de la información propia de su labor, debe asegurar que el software para la realización de las copias de respaldo o Backups se estén ejecutando de manera periódica.

- La coordinación de Informatica será la responsable de almacenar la información final entregada el departamento.
- Definir usuarios de la información y administradores de esta.

7. Marco de actuación

7.1 Seguridad de la compañía

7.1.1 Divulgación a terceros

- El acceso de terceros a la información de la compañía puede estar permitido siempre y cuando se demuestre que esta información es necesaria para el desarrollo de la labor del tercero. Para entregar esta información es indispensable que el coordinador o administrador de la información avalen dicha solicitud.
- Cualquier pérdida o divulgación sospechosa o no autorizada de información confidencial debe notificarse inmediatamente al propietario de la información, a la Coordinación Informática, al Departamento Jurídico y a la Gerencia General.

7.1.2 Solicitudes de terceros de la información

- Para entregar información de la compañía, debe ser solicitada mediante comunicación escrita o correo electrónico.
- Una vez autorizada la entrega de información, se debe determinar el tiempo que el usuario tendrá acceso a la misma.

7.1.3 información no autorizada

- Está prohibido que los usuarios copien, transmitan o publiquen información confidencial a terceros sin una justificación válida y sin la autorización correspondiente.
- Está prohibido la publicación de información de la empresa en portales o páginas de internet. sin tener la previa autorización de la Gerencia General o quien haga sus veces.
- Los responsables de reenvío no autorizado de la información confidencial copiada a terceros estarán sujetos a medidas disciplinarias incluidas dentro del Reglamento Interno de Trabajo.

8. Controles de seguridad administrativa

8.1 Uso de los recursos tecnológicos de la compañía

Todos los empleados que deseen utilizar los sistemas o herramientas de la compañía deben:

- Tener la aprobación del Coordinador de área o Director de Proyecto.
- Para los nuevos usuarios, la coordinación de Informatica deberá recibir en el formato de ingreso, la solicitud para el acceso a los Sistemas, entrega de herramientas ofimáticas y se comprometen a cumplir la política de Informatica.

A Todos los empleados que la compañía le asigne una herramienta o hardware debe:

- Firmar el formato de recibido y aceptar las políticas y procedimientos de la compañía en cuanto a lo que se refiere a la utilización de equipos y redes, incluyendo las instrucciones contenidas en la presente Política.
- El funcionario tiene la responsabilidad de cuidar y responder por los elementos que le han sido asignados para sus labores.

9. Propiedad exclusiva de los materiales desarrollados

La compañía tiene los derechos exclusivos de todo el material desarrollado por sus empleados para la realización de sus labores.

Todos los programas y documentos producidos o provistos por los empleados en beneficio de la compañía son propiedad de la compañía y los derechos de autor y el uso de esta información cuando lo amerite.

10. Acceso a Internet

Todos los empleados y/o personal que maneje equipos de la compañía que tienen acceso a Internet, deben tener en cuenta los siguiente:

- El acceso a Internet está controlado para asegurar el uso apropiado y el cumplimiento de las políticas de seguridad.
- Está prohibido incluir a la empresa en grupos de noticias o en otros foros públicos a menos que haya sido previamente autorizado o sea propio de su cargo. Esta autorización la debe tramitar el Gerente General.
- Está prohibido el ingreso a sitios inapropiados relacionados con pornografía, apuestas, videojuegos o sitios que puedan contender malware, estos accesos serán sancionados por crear brechas en la seguridad informática de la compañía.
- Está prohibido colocar material o información que comprometa a la Compañía en sitios públicos.

- La información confidencial, como contraseñas y números de tarjeta de crédito de la compañía solo deben utilizarse en páginas de Internet que sean seguras provistas con un protocolo HTTPS.

11. Correo electrónico

La compañía asigna a los empleados y/o colaboradores externos, que hayan recibido la aprobación de su jefe inmediato en el formato de ingreso, una dirección de correo electrónico y los servicios relacionados, con el fin de facilitar el desempeño de sus tareas. La dirección de correo electrónico y la información que aquí reposa es de propiedad exclusiva de la compañía y no puede ser utilizada para asuntos diferentes a los propios de su cargo y/o responsabilidades.

- Todas las comunicaciones de relacionadas con el cargo deben ser enviadas y recibidas mediante la dirección de correo electrónico asignado. En caso de alguna falla con el dominio o con la cuenta de correo, y se requiera el envío de la información por otro medio no oficial este debe ser avalado por el jefe inmediato con su aprobación necesaria.
- Todo el personal debe utilizar la firma suministrada por la coordinación de informática, de acuerdo con sus propios procedimientos.
- El correo electrónico de la empresa no debe ser utilizado para nada diferente a las responsabilidades propias del cargo que desempeña.
- Está totalmente prohibido la inscripción de la cuenta de correo corporativo en los portales web, tiendas online, noticias, etc., que no correspondan al objeto de sus labores
- Es responsabilidad del usuario de la cuenta de correo, que todos los mensajes que salgan del buzón y la información que esté en ella no sean borrados, por lo tanto, se debe:
    - NO proporcionar la contraseña a ninguna persona.
    - Tener bloqueado el equipo cuando no se está frente a él.
    - Cambiar la contraseña periódicamente.
    - La compañía, proporciona una contraseña que puede ser modificada o bloqueada a criterio de esta, teniendo en cuenta que la información y la cuenta son propiedad de esta.

12. Copia de seguridad de datos, restauración de archivos y Backup

- La empresa al iniciar su vinculación laboral le asignará una licencia de Microsoft 365 para el desarrollo de sus funciones, la cual será usada exclusivamente para todo lo concerniente al desarrollo de sus funciones dentro a la compañía.
- Usando la herramienta OneDrive se realizan copias automáticas de respaldo a la carpeta de “Mis Documentos”, “Imágenes”, “Escritorio” de aquellos equipos que pertenecen a la empresa. (Es necesario una conexión a internet para que este proceso sea exitoso).
- Se debe tener en cuenta que todo archivo que se encuentre en una carpeta diferente a “Mis Documentos”, “Imágenes”, “Escritorio”, no se le realizará copia, y si se pierde algún dato por robo o daño del disco el usuario será el directamente responsable.

- En caso de que el equipo sea propiedad del usuario, este deberá crear un usuario en su equipo con el primer nombre y apellido en mayúscula, adicional contar con un antivirus y realizar la copia de seguridad en OneDrive con la licencia asignada por la empresa. En este caso el usuario será el responsable de la información y del respaldo de esta.
- En caso de perdida o robo de equipo donde tiene su información debe comunicarse de inmediato con la Coordinación de Informatica para el respectivo Backup y la protección de su información.

Estas copias deben mantenerse únicamente con el fin de:

- Restaurar el sistema después de una infección de virus informáticos.
- Defectos de la unidad de disco duro u otros problemas de equipo.
- Cuando los datos son de un exfuncionario, estos pueden ser asignados al funcionario que lo está reemplazando u otro funcionario siempre y cuando tenga la autorización del jefe inmediato o del Gerente si el funcionario pertenece a otra Área.
- Todo Gerente, Director, Coordinador o Director de Proyecto debe validar que la Coordinación Informática realice el Backup de un subordinado cuando este se retire. Por ello está totalmente prohibido reasignar el equipo sin antes realizar la copia de seguridad.
- Está totalmente prohibido almacenar música, fotos o información personal en los equipos de la Compañía.

13. Gestión de cambios

- Toda implementación nueva, actualizaciones o modificaciones a los sistemas de información, servidores, bases de datos, hardware de seguridad y comunicaciones deben entrar al proceso de Gestión del Cambio el cual será liderado por la Coordinación Informática.
- Los cambios a servidores y comunicaciones de la compañía deben ser realizados bajo el proceso de gestión de cambio documentado para garantizar los cambios.
- Todo proceso de cambio debe ser realizado únicamente por personal de la Coordinación Informática o por la empresa proveedora del servicio a actualizar. Para ello la Coordinación Informática informará sobre el cambio con anterioridad y enviará la notificación de quienes serán los responsables.
- Está totalmente prohibido realizar cambio de equipos o sus partes como teclado o mouse, celulares etc., sin la aprobación de la Coordinación Informática.

14. Adquisición o renta de sistemas de información o herramientas de productividad

- Todo desarrollo, compra o arrendamiento de sistemas de información o herramientas de productividad deben ser avalados por la Coordinación Informática. Por ningún motivo las áreas pueden contratar / instalar sistemas de información sin la aprobación de la Coordinación Informática.

- Una vez aprobada la compra de un activo de software, la licencia deberá ser entregada a la Coordinación Informática para su custodia y la administración del licenciamiento.
- Para realizar un desarrollo o compra de sistemas de información, el Coordinador de Informática debe dar su visto bueno con el fin de asegurar el cumplimiento de la infraestructura existente y poder dar soporte cuando se encuentre en operación.

15. Hosting y almacenamiento externo

- Se prohíbe que cualquier funcionario de la Compañía contrate un hosting o almacenamiento externo a excepción de la Coordinación Informática.
- Cuando se requiera contratar un servicio de almacenamiento externo, se debe contactar a la Coordinación Informática quien evaluara el caso y de su aprobación o solución alternativa.
- La Coordinación Informática será el contacto y responsable de todo almacenamiento externo o hosting que se contrate.

16. Administración de licencias

Está totalmente prohibido instalar software en los equipos de la compañía. Si se requiere algún aplicativo o software para la realización de las labores debe pasar primero a la Coordinación Informática quien validara la disponibilidad presupuestal para la adquisición. Si la compañía cuanta con la licencia disponible se procede a la instalación. Si no se tiene se solicitará por medio del proceso de compras.

17. Medio ambiente y controles físicos

17.1 Control de acceso a la información y servicios

- Está restringido el acceso al cuarto de servidores. El acceso a los empleados a estos sitios debe ser autorizado previamente por el Coordinación Informática y consignado en la bitácora de accesos.

17.2 Protección contra robo

- Todos los servidores y equipos de red deben ser protegidos físicamente.
- Los equipos de red y servidores, así como los dispositivos de almacenamiento, deben colocarse en sitios seguros con llave y bajo los controles ambientales correspondientes.
- Todos los equipos portátiles y de escritorio deben ser bloqueados con clave cuando el usuario no se encuentre frente a él.

18. controles de seguridad técnica

18.1 Identificación de usuario y la autenticación

18.1.1 ID de usuario y contraseña

- Todo usuario con acceso a los Sistemas de información de la Compañía debe tener un ID de usuario y una contraseña que es suministrada por la Coordinación Informática.
- El ID de usuario debe utilizarse con el fin de restringir los privilegios de acceso a los Sistemas de acuerdo con las funciones, responsabilidades y actividades de cada usuario.
- Todos los empleados son responsables de proteger su ID de usuario y contraseñas.
- La contraseña es responsabilidad del usuario y por ende es obligatorio cambiarla periódicamente según las políticas de seguridad y de no entregársela a nadie, ni compartirla. Si llegase a existir un evento de seguridad en un sistema de información o un equipo, el usuario propietario de la contraseña será el responsable.

18.1.2 Opciones de contraseña

Los usuarios del sistema de información deben elegir contraseñas que sean complejas y que no contengan ninguna información relacionada con su trabajo o su vida personal.

Estos son algunos consejos para la creación de contraseñas:

- Combinar varias palabras juntas.
- Combinar números con una palabra (letras mayúsculas o minúsculas) o signos de puntuación
- Transformar una palabra común mediante un método específico
- Crear acrónimos (iniciales que forman una palabra)

18.1.3 Similitud de contraseña

Los usuarios no deben crear repetidamente contraseñas que sean idénticas o esencialmente similares a contraseñas anteriores.

18.1.4 Restricciones de contraseña

Las contraseñas deben contener los siguientes aspectos de acuerdo con la política establecida.

- La contraseña se debe cambiar cada determinado tiempo. El sistema obliga el cambio, por lo cual el usuario debe realizarlo en su momento.
- La contraseña se bloquea después de un número de intentos fallidos.

- El sistema no acepta repetición de contraseñas hasta por un número determinado de ciclos.
- El sistema de gestión de contraseña obliga a los usuarios combinar letras y números y no permite el uso repetido de una contraseña en un tiempo determinado.

18.1.5 Almacenamiento de información de contraseña

- Las contraseñas no deben almacenarse de forma legible en archivos o papeles donde puedan ser encontrados por otros usuarios o terceras personas.

18.1.6 Uso compartido de información

- Cuando la información deba ser compartida, los empleados deben hacerlo mediante mensajes de correo electrónico, OneDrive, bases de datos, directorios públicos situados en servidores de red de área local u otros medios de intercambio de la compañía.
- Las contraseñas nunca deben ser compartidas o divulgadas.
- Cuando la persona de tecnología reinicie la contraseña, el usuario debe cambiarla inmediatamente.
- Si los usuarios sospechan que alguien está usando su ID de usuario y contraseñas que está bajo su responsabilidad, debe asesorarse con un funcionario de la Coordinación Informática.

19. Software malintencionado

19.1 Software de detección de virus

- Es obligatorio que los usuarios dejen terminar el proceso de actualización del software antivirus.
- Todos los archivos almacenados en el equipo deben analizarse por el software de detección de virus.
- Al ingresar un CD, USB, tarjeta, etc. Debe realizarse un análisis con el software antivirus antes de acceder al mismo.
- La Coordinación Informática, cuenta con un proceso de revisión de los equipos donde más se encuentran y controlan los virus. Si un equipo es persistente, será notificado. Si persiste se tomarán las medidas disciplinarias del caso debido a que esto atenta contra la seguridad informática.

19.2 Eliminación de virus

- A la primera señal de un posible virus, el usuario debe dejar de utilizar el equipo inmediatamente y solicitar apoyo a la Coordinación de Informática.

- El medio de almacenamiento magnético utilizado en el equipo infectado no debe utilizarse en ningún otro equipo hasta que sea verificada la eliminación del virus.
- El equipo infectado debe ser retirado de la red (apagado el wifi, desconectado el cable) mientras se revisa que el equipo está libre de virus.
- Los usuarios no deben intentar eliminar los virus, deben apoyarse en el área de Tecnología.
- Si el personal de Coordinación Informática no puede eliminar el virus, debe contactarse con el proveedor del antivirus y retener el equipo y el medio infectado hasta que se pueda eliminar el virus para así asegurar que la red corporativa no se infecte del virus encontrado.

20. Seguridad de red

20.1 Conexión de red interna

- Todos los equipos que almacenan información confidencial y están permanente o intermitentemente conectados a redes de informática interna de la compañía deben tener un sistema de control de acceso aprobado por el área de Informática de la Compañía.
- Todos los demás tipos de sistemas de procesamiento de información deben estar equipados con una contraseña de protector de sesión que bloquea el equipo tras un determinado período de inactividad. La pantalla se reactivará cuando se introduzca la contraseña correcta.
- Todo equipo que no pertenezca a la compañía y deba conectarse a la red, debe contar con un antivirus y ser registrado al ingreso.
- Ningún funcionario debe conectarse a internet utilizando módems USB o compartiendo el servicio de internet del celular dentro de las sedes de la compañía. Solamente se permite acceder a internet por el servicio contratado por la empresa.
- Todas las conexiones externas a los sistemas de información de la Compañía deben estar protegidas por un sistema de control de acceso de contraseñas aprobadas.

20.2 Cambios en la red

- Excepto en situaciones de emergencia, todos los cambios en las redes de la compañía deben registrarse por medio de una solicitud de mantenimiento/cambio y debe ser aprobada por la Coordinación Informática.
- Todos los cambios en las redes internas deben llevarse a cabo por personal autorizado por la Coordinación de Informática.
- Está completamente prohibido instalar equipos de telecomunicaciones y software (Sniffer, detección de claves, etc.) dentro de la Compañía que atenten contra la seguridad informática. Solo la Coordinación de Informática podrá realizar dichas instalaciones bajo la aprobación de la Gerencia General.

21. Equipos asignados

21.1 Equipos de Cómputo, impresoras, periféricos, Teléfonos celulares

- Todo equipo asignado debe entregarse mediante un acta diligenciada por la Coordinación de Informática.
- Todo funcionario es responsable por la seguridad de los equipos asignados a él por lo tanto cualquier robo o pérdida debe ser comunicado a la Coordinación de Informática y seguirá el proceso de acuerdo con la política de uso de equipos especificada en el Acta de Entrega.
- Si el equipo presenta fallas, este debe ser revisado por la Coordinación Informática. Queda totalmente prohibido llevar los equipos a sitios de reparación por seguridad de la información de la Compañía.
- Todo funcionario al retirarse de la compañía debe cerciorarse en entregar todos los equipos asignados en buen estado de lo contrario se seguirá el proceso de acuerdo con la política de uso de equipos especificada en el Acta de Entrega.

CARLOS MAURICIO QUINTERO CHAVES
C.C. No. 80.422.135 de Bogotá D.C.
Representante Legal