Procedimiento de Cifrado de Seguridad Informática

Versión	Fecha	Control de Cambios
02	10/12/2025	• Se agregaron definiciones y disposiciones para aplicar el enmascaramiento de datos en la empresa, alineado a la norma ISO 27001 de seguridad de la información.

Áreas Responsables	Nombres y Cargos
Elaborado: **Departamento de Tecnología de la Información y Comunicaciones**	Henry Tornero Especialista en Sistemas de Información Erik Prado Especialista en Redes y Comunicaciones
Revisado: **Departamento de Tecnología de la Información y Comunicaciones**	Moisés Palomino Jefe del Departamento de Tecnología de la Información y Comunicaciones
Homologado: **Oficina de Planeamiento y Mejora Continua**	Deymer Barturén Especialista en Calidad y Mejora de Procesos Miguel Tito Jefe de la Oficina de Planeamiento y Mejora Continua
Aprobado: **Gerencia de Administración y Finanzas**	Julio Temple Gerente de Administración y Finanzas

INDICE

I. OBJETIVO

Establecer las actividades que se deben realizar para el uso de cifrado de seguridad informática y el enmascaramiento de datos, con el fin de proteger la información de Activos Mineros S.A.C. (en adelante AMSAC), que es manejada y transmitida interna o externamente.

II. ALCANCE

El procedimiento aplica a la información de AMSAC que, por su criticidad, debe ser cifrada para evitar que sus datos sean revelados a terceros no autorizados.

III. DOCUMENTOS DE REFERENCIA

- Ley N° 27309, Ley que incorpora los delitos informáticos al código penal.
- Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM) y su reglamento aprobado mediante Decreto Supremo N° 031-2005-MTC.
- Ley N° 29733, Ley de Protección de Datos Personales y su reglamento aprobado mediante Decreto Supremo N° 016-2024-JUS.
- Lineamiento Corporativo: “Lineamiento del Sistema de Gestión de la Seguridad de la Información” de FONAFE.
- Manual Corporativo: “Manual Metodológico para la Implementación del Sistema de Gestión de Seguridad de la Información” de FONAFE.
- NTP ISO/IEC 27001:2022 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información, ciberseguridad y protección de la privacidad. Requisitos. 3a. Edición.
- NTP ISO/IEC 27002:2022 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información, ciberseguridad y protección de la privacidad. 2a. Edición.
- Política de Seguridad de la Información de AMSAC.
- Directiva S3.1.DR1 Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones.
- Directiva S3.1.DR2 Administración de Software.

IV. VIGENCIA

Este documento entrará en vigencia a partir del primer día hábil después de la fecha de aprobación, derogándose su precedente Versión 01 de fecha 12.dic.2023.

V. CONTENIDO

1. DEFINICIONES / CONSIDERACIONES

1.1. Definiciones y Abreviaturas

- **Activo de Información:** Es todo aquello que es o contiene información de valor para la Empresa (que incluye información de tipo datos personales) y por tanto requiere protección. Los activos están sujetos a muchos tipos de amenazas que pueden explotar sus vulnerabilidades. Se debe tener en cuenta que parte de los activos de información serán aquellos que por regulación corresponde incorporarlos como información o contenedores de información de valor para le empresa, como por ejemplo los datos personales, las tecnologías digitales, los servicios digitales y los contenidos.
- **Autenticidad:** Propiedad que una entidad es lo que dice ser.

- **Controles de Cifrado:** Se basa en la confidencialidad, autenticación, integridad y no repudio:
  - Confidencialidad: Codifica el contenido del mensaje.

- Autenticación: Verifica el origen de un mensaje.
- Integridad: Garantiza que el contenido de un mensaje no ha cambiado desde su envío.
- No repudio: Evita que los remitentes nieguen haber enviado el mensaje cifrado.

- **Cifrado de información**: Se aplican mecanismos criptográficos para volver incomprensible información que es catalogada como confidencial y evitar que sea accedida por personas no autorizadas.
- **Certificado SSL**: Es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Secure Sockets Layer (Capa de sockets seguros), un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.
- **Confidencialidad**: Principio de la seguridad de la información que busca asegurar que solo quienes estén autorizados puedan acceder a la información.
- **Enmascaramiento de datos:** Técnica de seguridad que oculta o altera los datos sensibles para protegerlos del acceso no autorizado.
- **Encriptación:** Proceso criptográfico que convierte los datos en un formato ilegible utilizando un algoritmo y una clave de cifrado.
- **Firma Electrónica**: Método criptográfico para preservar la integridad o autenticidad de la información crítica que se almacena o se transmite.
- **No repudio:** Capacidad para demostrar la ocurrencia de un evento o acción reclamada y sus entidades de origen.
- **Integridad:** Principio de la seguridad de la información que busca asegurar que la información y sus métodos sean exactos y completos.
- **Trabajadores:** Se refiere a todo el personal interno que guarde relación directa con las actividades laborales realizadas en AMSAC
- **Terceros:** Personas o grupos de personas externas a AMSAC que interactúan de alguna manera con activos e información de la empresa como lo son proveedores, contratistas, auditores, entes de control, pasantes, entre otros.

2. DESCRIPCIÓN

2.1. Disposiciones Generales

2.1.1. El Jefe del Departamento de Tecnología de la Información y Comunicaciones, como dueño del proceso, es responsable que el proceso de Cifrado de Seguridad Informática se efectúe cumpliendo los plazos y las disposiciones previstas en la normativa legal y el presente procedimiento.

2.1.2. El Especialista en Redes y Comunicaciones es el responsable de gestionar, administrar y monitorear el cifrado de seguridad en los servicios del Departamento de Tecnología de la Información que lo requieran.

2.1.3. Los parámetros que deben cumplir las claves de cifrado son:
- Mayor o igual a 8 caracteres
- No utilizar palabras reconocibles
- No utilizar caracteres cortos
- Utilizar minúsculas, mayúsculas, números y caracteres especiales.
- No utilizar datos públicos, por ejemplo, nombres, direcciones, fechas de aniversario.

2.1.4. En caso de que el remitente de la información sea un tercero, el usuario es responsable de garantizar el correcto intercambio de llaves públicas, utilizando canales o medios de comunicación alternos.

2.1.5. El enmascaramiento de datos se aplica a aquella información que contenga datos personales para dar cumplimiento a la normativa de protección de datos personales y las disposiciones internas sobre el tratamiento de los datos personales en AMSAC.

2.1.6. Para el enmascaramiento de datos, el Departamento de TIC debe considerar las siguientes recomendaciones:

a) Hacer una priorización de la información relevante, usando los criterios de confidencialidad, integridad y disponibilidad del inventario de activos, para identificar la información que debe ser enmascarada y evitar su exposición; considerar información contenida en los activos relevantes dentro del alcance del SGSI para esta priorización.

b) Diseñar consultas o máscaras para mostrar datos mínimos con el objetivo de no otorgar a todos los usuarios acceso a todos los datos.

c) Considerar que la solución o mecanismo de enmascaramiento contenga encriptación (acceder a través de una clave para visualizar los datos), números y fechas variables, anular o eliminar caracteres (evitar que los usuarios no autorizados no vean los mensajes completos), sustitución (cambiar un valor por otro para ocultar información confidencial).

2.2. Cifrado Web

Ejecutor	Actividad
2.2.1. Generación del Certificado	
ERC	1. Define las características del certificado SSL.
	2. Gestiona la contratación para la adquisición, instalación y mantenimiento de los certificados SSL en los servidores, que deben ser emitidos por una entidad certificadora.
	3. Ejecuta la instalación de los certificados SSL en los servidores.
2.2.2. Almacenamiento del certificado	
ERC	1. Almacena y custodia el certificado SSL en un repositorio compartido y restringido.
2.2.3. Renovación del certificado	
ERC	1. Monitorea permanentemente el estado de vigencia de los certificados web en los servidores.
	2. Solicita la renovación de los certificados SSL un mes antes de su caducidad.
JTIC	3. Aprueba la solicitud de la renovación u adquisición del certificado SSL.
ERC	4. Gestiona la contratación de la renovación del certificado SSL.

2.3. Firma Electrónica

Ejecutor	Actividad
2.3.1. Generación del certificado digital	
ESI	1. Una vez recibido el formato de Solicitud de Alta/Baja de Usuario o Cambio con de Perfil aprobado, considerando la generación de certificado digital, solicita a RENIEC la generación del certificado electrónico y su instalación en un token.
RENIEC	2. Valida la información personal del usuario y remite la autorización de uso.
Usuario	3. Dispone del token para su uso. La asignación de clave privada se realiza directamente en el token.
DTIC	4. Brinda el soporte al usuario para la activación de su certificado digital.
2.3.2. Conservación del certificado digital	
Usuario	1. Asegura el cuidado y conservación física del token, almacenándolo en gabinetes, cajones o armarios que cuenten con seguridad física para evitar acceso no autorizado. En caso de robo o pérdida del token, comunica el evento al DTIC para el inicio del proceso de renovación. Las claves pública y privada permanecerán almacenadas en el token.
2.3.3. Renovación del certificado digital	
Oficina de Gestión Humana	1. En caso se identifica la proximidad del vencimiento de la vigencia de los certificados digital de los usuarios de la empresa, envía al usuario el formato de declaración jurada de identificación para solicitar certificado digital de

Ejecutor	Actividad
	RENIEC, con copia al Departamento de Tecnología de la Información y Comunicaciones, vía correo electrónico, con un mes de anticipación a su caducidad.
Usuario	2. Remite el formato de declaración jurada de identificación para solicitar certificado digital de RENIEC, debidamente llenado, a la Oficina de Gestión Humana, con copia al Departamento de Tecnología de la Información y Comunicaciones, vía correo electrónico.
DTIC	3. Realiza la gestión de la solicitud de certificado digital para su aprobación por la Gerencia General y su envío a RENIEC.
	4. Brinda el soporte al usuario para la activación de su certificado digital.
2.3.4. Eliminación del certificado digital	
DTIC	1. Una vez recibido el formato de Solicitud de Alta/Baja de Usuario o Cambio con de Perfil aprobado, considerando la baja del usuario, elimina el certificado digital.
	2. Requiere al usuario la entrega del token, lo formatea y verifica que no tenga el certificado digital.

2.4. Cifrado de Comunicaciones, mediante VPN

Ejecutor	Activi
2.4.1. Instalación de VPN	
ERC	1. Define el tipo de VPN a utilizar para la comunicación y el protocolo de encriptación que requerirá el canal establecido. Nota: La autenticación multifactor o MFA es un tipo de VPN que puede ser usado.
	2. Establece el rango de red y protocolos de seguridad dentro del canal.
	3. En coordinación con el JTIC, gestiona la contratación para la adquisición del licenciamiento de la solución VPN integrada la Firewall, según lo establecido en el Procedimiento de Contrataciones correspondiente.
	4. Una vez efectuada la contratación, documenta y almacena las licencias de la solución VPN en el repositorio.
2.4.2. Configuración de VPN cliente	
ERC	1. Una vez recibido el formato de Solicitud de Alta/Baja de Usuario o Cambio con de Perfil aprobado, considerando la habilitación del acceso VPN, crea el acceso VPN en la solución integrada.
	2. Realiza la instalación del cliente VPN en el equipo del usuario y verifica que el usuario tenga el acceso VPN.
2.4.3. Desactivación de VPN	
ERC	1. Una vez recibido el formato de Solicitud de Alta/Baja de Usuario o Cambio con de Perfil aprobado, considerando la desactivación del acceso a la VPN o la eliminación de un servicio, elimina las reglas de conexión, políticas y túneles configurados.
2.4.4. Monitoreo de VPN	
ERC	1. Realiza el monitoreo permanente de las conexiones VPN, revisando el estado y tiempo de conexión.
	2. Genera un reporte periódico del acceso VPN e informa a la JDTIC.

3. ALCANCES FUNCIONALES

3.1. Gerente de Administración y Finanzas

- Aprobar el presente documento.

3.2. Jefe del Departamento de Tecnología de la Información y Comunicaciones

- Conducir el proceso de Cifrado de seguridad informática en la empresa, cumpliendo los plazos y las disposiciones previstas en los lineamientos de FONAFE.

- Velar por el cumplimiento del presente procedimiento.
- Velar porque el procedimiento se mantenga vigente, siendo responsable de realizar revisiones y actualizaciones periódicas, así como de la difusión y conocimiento del mismo por parte del equipo de trabajo y áreas vinculadas.

3.3. Especialista en Redes y Comunicaciones

- Ejecutar el proceso de Cifrado de seguridad informática, cumpliendo los plazos y las disposiciones establecidas en el presente procedimiento.
- Identificar oportunidades de mejora al presente procedimiento.

3.4. Oficina de Gestión Humana

- Remitir a los usuarios el formato de declaración jurada de identificación para solicitar certificado digital de RENIEC, en caso identifique la proximidad de su vencimiento.

4. REGISTROS / ANEXOS

- Solicitud de Alta/Baja de Usuario o Cambio de Perfil.