1. RESUMEN

El presente documento define las políticas y normas que regulan el uso y acceso a los sistemas de información y activos de información de la organización, con la finalidad de garantizar su uso adecuado y seguro.

2. OBJETIVO

El presente documento tiene como objetivo establecer las pautas y procedimientos para el uso seguro y adecuado de los Sistemas de Información, con el fin de prevenir accesos no autorizados y garantizar la seguridad de la información a través de técnicas de autenticación y autorización.

Además, busca concienciar a los usuarios sobre su responsabilidad en el uso de contraseñas y equipos, y promover una cultura de seguridad de la información en todos los ámbitos de la organización

3. ALCANCE

Esta política rige el acceso a los Sistemas de Información y repositorios de información confidencial y sensible de la organización. Todos los empleados, contratistas, consultores, temporales y demás personal de la organización y sus subsidiarias tienen la responsabilidad de utilizar estos recursos de manera apropiada y responsable, de acuerdo con las políticas y normas internas, así como con las leyes y regulaciones aplicables.

4. POLÍTICA

La política de control de acceso tiene como objetivo establecer medidas de seguridad para regular el acceso a la red, sistemas operativos, sistemas de información y servicios de la organización. Es fundamental que todos los empleados conozcan y comprendan estos

controles de acceso, que deben ser limitados y asignados de acuerdo con el perfil de cargo y las necesidades específicas de cada empleado.

Además, se deben implementar procedimientos claros y documentados para la asignación de privilegios de acceso a sistemas de información, bases de datos y servicios, garantizando que se comuniquen y controlen adecuadamente para asegurar el cumplimiento de la política.

4.1 NORMAS GENERALES APLICABLES PARA EL CONTROL DE ACCESO

4.1.1 NORMA N°1: REQUERIMIENTOS PARA EL CONTROL DE ACCESO

Los controles de acceso deben incluir los siguientes aspectos:

- Requerimientos de seguridad específicos para cada Sistema de Información y aplicación, considerando el consumo de recursos internos.
- Definición de perfiles de acceso y privilegios para los usuarios, basados en su perfil de cargo dentro de la organización, para acceder a Sistemas de Información, carpetas compartidas y aplicaciones.
- Regulación de accesos para la interacción de equipos de Infraestructura de Comunicaciones.

4.1.2 NORMA N°2: ADMINISTRACIÓN DE ACCESOS DE USUARIOS

La organización implementa procedimientos formalizados para gestionar y controlar la asignación de permisos y accesos a los sistemas de información, servicios de información y activos de información, garantizando así una gestión segura y controlada de los accesos.

4.1.3 NORMA N°3: CREACIÓN DE USUARIOS

La creación de usuarios deberá cumplir con los siguientes requerimientos:

- La organización mantendrá registros detallados de acceso a los recursos internos, donde se refleje la autorización explícita de los responsables de los procesos involucrados, tanto para personal interno como externo. La organización será cuidadosa al otorgar accesos, diferenciando su consumo para preservar la confidencialidad, integridad y disponibilidad de la información.
- Los datos de acceso a los sistemas de información deberán consistir en un ID o nombre de usuario único y una contraseña asociada, también única para cada usuario.
- Cuando un empleado de la organización sea desvinculado o cambie de contrato, se deberán eliminar o modificar sus privilegios de acceso a los sistemas de información correspondientes.
- El Oficial de Seguridad de la Información y el Comité de Gestión de Seguridad de la Información (CGSI) deberán realizar revisiones periódicas de los privilegios de acceso a los sistemas de información, manteniendo registros de las revisiones y hallazgos para garantizar la seguridad y control de los accesos.

4.1.4 NORMA N°4: GESTIÓN DE CONTRASEÑAS DE USUARIO

La organización implementará una política de gestión de contraseñas que cumplirá con los siguientes requisitos:

- Las contraseñas de acceso deben tener un mínimo de 8 caracteres y combinar números, letras mayúsculas y minúsculas, y preferiblemente incluir caracteres especiales.

- Todas las contraseñas de acceso a recursos internos y públicos de la organización deben cambiarse cada 3 meses como mínimo.
- Sin embargo, para aquellos accesos que contengan información confidencial, el cambio de contraseña debe realizarse mensualmente.
- Los sistemas de información deben bloquear permanentemente a los usuarios después de 5 intentos fallidos de autenticación, excepto para aquellos que contengan información confidencial o sensible, en cuyo caso el bloqueo se realizará después de 3 intentos fallidos.

4.1.5 NORMA N°5: USO DE CONTRASEÑAS

Los usuarios que acceden a recursos de la organización deben cumplir con las siguientes normas de seguridad:

- Mantener la confidencialidad de sus datos de acceso, ya que la divulgación no autorizada puede generar responsabilidades y sanciones según las políticas de la organización.
- No utilizar contraseñas basadas en información personal fácilmente accesible, como nombres, números de teléfono o fechas de nacimiento.
- Crear contraseñas que sean fáciles de recordar para el usuario, pero difíciles de adivinar para terceros.
- Notificar inmediatamente cualquier incidente de seguridad relacionado con sus contraseñas, como pérdida, robo o sospecha de pérdida de confidencialidad.

4.1.6 NORMA N°6: EQUIPOS DESATENDIDOS EN ÁREAS DE USUARIOS

Los usuarios deben seguir las siguientes normas para proteger adecuadamente los equipos desatendidos:

- Los equipos instalados en áreas de usuarios, como estaciones de trabajo, servidores de archivos en el Datacenter y otros, requieren medidas de protección específicas para prevenir accesos no autorizados cuando se encuentren desatendidos.
- Cada computadora asignada a un colaborador estará equipada con candados especiales para controlar el acceso. Solo las personas autorizadas tendrán acceso a las llaves para trasladar los activos o, en el caso de laptops, para transportarlos a reuniones o visitas a clientes dentro o fuera de la organización.
- Para obtener más información sobre el tratamiento de equipos desatendidos, se recomienda revisar la Política de Puesto de Trabajo Desatendido y Bloqueo de Pantalla.

4.1.7 NORMA N°7: CONTROL DE ACCESO A RED

La organización implementará medidas de control de acceso para garantizar el acceso a la red:

- Se bloqueará el acceso a sitios web de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente un riesgo potencial para la organización.
- El bloqueo se realizará mediante la configuración de reglas de filtrado de contenido en el Firewall.
- El acceso a carpetas de contenido crítico y sensible, como la Carpeta de Proyectos, Carpeta de Licitaciones y Carpetas de áreas Administrativas y Contabilidad, estará restringido solo a personal autorizado, mediante la configuración de permisos sobre la carpeta.

- Los permisos de acceso contendrán derechos diferenciados de lectura o escritura, previa evaluación y autorización por parte de las autoridades pertinentes de la organización: Jefe de Área inmediato y el Comité de Gestión de Seguridad de la Información (CGSI).
- Las excepciones de acceso serán evaluadas y aprobadas por el Jefe de Área inmediato, según la necesidad del cargo y previa verificación de que las páginas solicitadas no contengan código malicioso, con la aprobación del Oficial de Seguridad de la Información.

4.1.8 NORMA N°8: AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS

La autenticación de usuarios remotos requerirá la aprobación previa del Jefe inmediato del usuario que solicita el acceso. Es importante tener en cuenta que existe una Política de Teletrabajo que establece las normas y requisitos específicos para garantizar una conexión segura desde el exterior.

4.1.9 NORMA N°9: CONTROL DE CONEXIÓN A REDES

La organización implementará una estrategia de sectorización de redes, dividiéndolas en áreas separadas para diferentes grupos de usuarios, servidores, DMZ (servidores de uso público) y otras áreas que se consideren necesarias. Esto permitirá garantizar la confidencialidad de los datos transmitidos entre redes, reforzada por reglas de firewall que controlen y regulen el tráfico de datos.

4.1.10 NORMA N°10: SEGURIDAD EN LOS SERVICIOS DE RED

La organización implementará las siguientes medidas para controlar la seguridad en los servicios de red:

- Solo se mantendrán instalados y habilitados los servicios y puertos que sean estrictamente necesarios para el funcionamiento de los sistemas de información y software de la organización.
- Se controlará el acceso lógico a los servicios, tanto para su uso como para su administración, mediante la implementación de medidas de seguridad como el bloqueo de puertos en el firewall de la entidad o la creación de listas de acceso controladas mediante el Switch de Core.

4.1.11 NORMA N°11: CONTROL DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

La organización implementará las siguientes medidas para controlar el acceso e identificación de Usuarios:

- Todos los usuarios, incluyendo el personal de soporte técnico, tales como operadores, administradores de red, programadores de sistemas y administradores de bases de datos, tendrán un identificador único (ID de usuario) para su uso personal exclusivo, lo que permitirá la trazabilidad de sus actividades.
- La estructura del identificador único (ID de usuario) será definida y administrada por la organización a través de un procedimiento interno específico.
- La información detallada sobre la estructura del identificador único (ID de usuario) estará disponible a través del área de Soporte Técnico.

4.1.12 NORMA N°12: SISTEMA DE ADMINISTRACIÓN DE CONTRASEÑAS

La organización implementará un Sistema de Administración de Contraseñas que cumplirá con los siguientes requisitos:

- Exigirá el uso de un Identificador Único (ID de Usuario) y contraseñas individuales para determinar responsabilidades y garantizar la autenticidad de los usuarios.

- Permitirá a los usuarios seleccionar y cambiar sus propias contraseñas después de un plazo mínimo establecido o cuando consideren que la contraseña ha sido comprometida.
- Incluirá un procedimiento de confirmación para detectar errores de ingreso y registrará los eventos de contraseñas mal ingresadas en el sistema.
- Obligará a los usuarios a cambiar las contraseñas provisionales o predeterminadas asignadas por el administrador del sistema de información.
- No permitirá mostrar las contraseñas en texto claro durante el ingreso.
- Almacenará las contraseñas de manera cifrada para garantizar su confidencialidad y seguridad.

4.1.13 NORMA N°13: SESIONES INACTIVAS

La organización empleará las siguientes directivas para el control de sesiones inactivas:

- Cuando un usuario deba abandonar su estación de trabajo temporalmente, deberá activar un protector de pantalla con contraseña para evitar que personas no autorizadas puedan acceder a su trabajo o continuar con la sesión de usuario activa.
- Los sistemas de información deben estar configurados para detectar inactividad y, si transcurren cinco minutos o más sin actividad, deben automáticamente cerrar la sesión de usuario ("timeout") para garantizar la seguridad y confidencialidad de la información.

4.1.14 NORMA N°14: REGISTRO DE CONEXIÓN A SISTEMAS DE INFORMACIÓN

Los accesos a recursos internos, incluyendo sistemas de información y carpetas compartidas en servidores que contienen información crítica y confidencial, serán registrados en todo momento. Esto se logrará mediante el envío de registros de inicio de sesión (login) al Sistema de Control de Eventos o registros, lo que permitirá auditar y controlar el acceso a estos recursos sensibles.

4.1.15 NORMA N°14: ACCESOS A INFRAESTRUCTURA DE COMUNICACIONES

El acceso a los equipos que componen la Infraestructura de Comunicaciones estará sujeto a las siguientes normas:

- Todos los accesos de configuración a los equipos requerirán la validación del Identificador Único (ID de Usuario) previa autorización.
- Todas las actividades realizadas en los equipos se registrarán en los logs de eventos del Servidor, para su posterior auditoría.
- Cuando sea necesario acceder físicamente a los servidores, el personal autorizado será acompañado por un técnico de soporte técnico (en el caso de proveedores externos) o por personal propio de la empresa autorizado.
- El personal que acceda físicamente a los recursos deberá llenar un formulario de ingreso que incluya su nombre completo, documento de identidad, motivo del ingreso, hora de ingreso y salida, y empresa (en el caso de personal externo).
- La organización considerará la implementación de un Sistema Biométrico para controlar el acceso físico a las instalaciones del Datacenter.

5. CUMPLIMIENTO DE POLÍTICA

5.1 MEDICIÓN DEL CUMPLIMIENTO

La organización realizará un seguimiento y verificación del cumplimiento de esta política mediante una variedad de métodos, incluyendo:

- Visitas periódicas
- Monitoreo de video
- Informes generados por herramientas comerciales
- Auditorías internas y externas
- Inspecciones

Los resultados de estas actividades serán comunicados al propietario de la política y al gerente de la unidad de negocio correspondiente, con el fin de garantizar el cumplimiento y la mejora continua de la política.

5.2 EXCEPCIONES

Cualquier excepción a esta política deberá ser sometida a aprobación previa por parte del Gerente de área correspondiente y el Grupo Interdisciplinario de Seguridad de la Información (GISI), quienes evaluarán y autorizarán las excepciones de acuerdo con las necesidades y riesgos de la organización.

5.3 INCUMPLIMIENTO

Cualquier empleado que incumpla o viole esta política estará sujeto a medidas disciplinarias, que pueden incluir desde advertencias hasta el despido, dependiendo de la gravedad de la infracción y la discreción de la organización.

6. APROBACIÓN

Elaborado por	Verificado por	Aprobado por
Nombre **Oficial de Seguridad de la Información** Fecha:	Nombre **Gerente Administrativo** Fecha:	Nombre **Gerente General** Fecha: