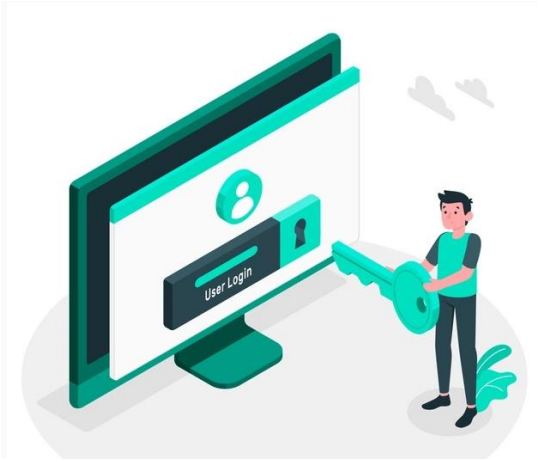
POLÍTICA CONTROL DE ACCESO



AEROPUERTO INTERNACIONAL SANTA ANA

1. Objetivo

El propósito de esta política es delimitar el acceso y uso aceptable de todo el equipamiento computacional, servicios y sistemas de información, así como de las redes de datos del Aeropuerto Internacional Santa Ana S.A.

Estas reglas están orientadas a proteger a los funcionarios y a la Institución sobre el uso inapropiado de la información, los servicios de red y equipos informáticos. ´

2. Alcance

La presente Política de Control de Acceso de la información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información y los sistemas informáticos. Esta Política es aplicable a todo el personal del Aeropuerto, independiente de su calidad contractual. De la misma forma, aplica a todo aquel personal vinculado a tareas de apoyo o asesoría externa.

3. Referencias

– Norma NCh-ISO 27001:2013 Tecnología de la información
- Técnicas de seguridad
- Sistemas de gestión de la seguridad de la información
– Requisitos.
– Norma NCh-ISO 27002:2013 Tecnología de la Información
– Código de prácticas para la gestión de la seguridad de la información.
– DS. 83 aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.

4. Definiciones

Derechos privilegiados: Conjunto de permiso o atributos dados a un usuario, quien de acuerdo con sus funciones y/o tareas encomendadas, puede acceder a un determinado recurso.

Restricciones de acceso: Delimitar el acceso de los usuarios a determinados recursos.

5. Roles y Responsables

Encargado de Seguridad de la Información: Ejecutar labores de coordinación para una adecuada elaboración, revisión e implementación de esta política y las materias que ella comprende.

Comité de Seguridad de la Información: Asegurar que las materias abordadas en esta política se ejecutan y se cumplen, identificar como se manejan los no cumplimientos, promover la difusión y sensibilización de las materias abordadas en este documento, revisar periódicamente la política detectando y proponiendo mejoras.

Personal / Funcionarios: Cumplir cabalmente con las disposiciones y requerimientos establecidos en la presente política. Cada usuario de la información, equipos informáticos y de los servicios de red del Aeropuerto deberá velar por la correcta implementación de las normas de control de acceso promovidas por el Aeropuerto dentro de sus áreas de responsabilidad, así como del cumplimiento por parte de su equipo de trabajo.

6. Modo de Operación

Con el objetivo de proteger la información de la institución previniendo el acceso no autorizado a los equipos y sistemas del Aeropuerto, los usuarios de los sistemas de información de la institución deben poseer una cuenta personal que lo identifique. La identificación se realizará normalmente por un nombre de usuario único. En el presente documento se abordan las siguientes temáticas:
-Política de control de acceso a los sistemas de información.
-Acceso a las redes y a los servicios de la red.
-Uso de información de autenticación secreta.
-Registro de eventos.
-Registros de actividad del administrador y operador del sistema.

6.1 Política de control de acceso a los sistemas de información

Todos los funcionarios del Aeropuerto, incluso terceros, deben tener acceso sólo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de la institución.
La asignación de privilegios y acceso a los activos de información (correo electrónico institucional, software, aplicaciones, carpetas compartidas, etc.) deben estar basados en las necesidades de las áreas y aprobados por el propietario de los activos.

6.2 Acceso a las redes y a los servicios de la red

El acceso a los sistemas y servicios de red de la Institución es otorgado sólo a usuarios identificados y autentificados. Para todo sistema de información de la CNE, el usuario deberá señalar quién es (identificación) y luego deberá comprobar que es quién dice ser (autenticación). La identificación se realizará con una cuenta de usuario asignada a cada funcionario y la autenticación se realizará con una contraseña secreta. Los usuarios deben tener acceso a la red y a los servicios de la red para los que han sido autorizados específicamente, lo cual debe quedar establecido en la asignación de privilegios correspondiente.
Los requisitos de autenticación del aeropuerto son:

- Antes de tener acceso a cualquier sistema o recurso de la red, todos los usuarios deben ser identificados positivamente mediante su cuenta de usuario y su contraseña.
-La cuenta de usuario y la contraseña deben ser individuales.
-La autenticación en sistemas por parte de funcionarios y administradores deben ser registrados en Logs para actividades de auditoria y eventuales análisis forenses.

6.3 Uso de información de autenticación secreta

Los funcionarios y contratistas que desarrollen actividades en la institución deben cumplir las siguientes reglas respecto del uso de la información de autenticación:
-Las cuentas de usuario y las contraseñas son individuales e intransferibles.
-Está prohibido el uso de un nombre de usuario ajeno o facilitar la cuenta de usuario y su contraseña personal a un tercero.
-Queda absolutamente prohibido anotar las contraseñas de acceso en lugares visibles o públicos.
-Las credenciales (usuario y contraseña) no deben ser incluidos en aplicaciones donde puedan quedar expuestas (macros de planillas, documentos o programas de tipo script).
- La composición de las contraseñas debe tener un mínimo de 8 caracteres, alfanumérica, fáciles de recordar, que no se basen en nada que otra persona pueda adivinar u obtener fácilmente mediante la información relacionada con el dueño de la cuenta, que no sean vulnerables a ataques de diccionario (es decir, que no conste de palabras incluidas en los diccionarios).
-El usuario deberá cambiar la información de autenticación secreta cuando exista alguna indicación de su posible compromiso.
-Se recomienda no utilizar las mismas contraseñas para fines laborales y personales.

6.4 Registro de eventos

- Debe monitorearse el uso de las instalaciones de procesamiento de la información, debiendo generar, mantener y revisar registros de las actividades de los usuarios; excepciones, faltas y eventos de seguridad de la información de manera regular.
-Los registros de eventos deberían considerar, entre otros, los siguientes:
- ID de usuarios.
- Actividades del sistema.
- Fecha, horas y detalles de los eventos clave, es decir, el inicio y finalización de la sesión.
- Los registros de los intentos exitosos y rechazados de acceso al sistema.
- Las direcciones y protocolos de redes.
-El Encargado de Seguridad de la Información debe tener acceso a los sistemas y a los registros de actividad, con el objetivo de colaborar en el control y efectuar recomendaciones de mejora.

6.5 Registros de actividad del administrador y operador del sistema.

-Se deben registrar, respaldar, proteger y revisar regularmente, las actividades del administrador y operadores de las distintas plataformas tecnológicas. El Log de actividades debe incluir al menos:

- Identificación del equipo.
- Horario de arranque y finalización de los procesos del sistema.
- Errores del sistema y acciones críticas realizadas.
- Cuenta del operador que realizó la actividad.

7. Periodicidad de evaluación y revisión

-La presente política debe ser evaluada cada dos años como máximo y sus cambios deben ser aprobados por el Gerente.

-Su cumplimiento se debe revisar en forma anual, en reunión de Comité de Seguridad, con la finalidad de asegurar su cumplimiento e incorporación de todas las normas y procedimientos necesarios de implementar en el marco de Ciberseguridad y Seguridad de la Información.

Aprobada en Cartago, a los seis (06) días del mes de diciembre de 2021

JUAN CARLOS ARIAS M.
GERENTE.