



Susuerte Digital

Susuerte S.A. en 2024
continúa con su

***DIRECCIONAMIENTO
ESTRATÉGICO VIGENTE***

***¡Tú también
haces parte del cambio!***

Susuerte 
Siempre te da más!

 **SuperGIROS**
Club de Fútbol

Nuestro Direccionamiento Estratégico

Nuestra razón de ser:

Propósito

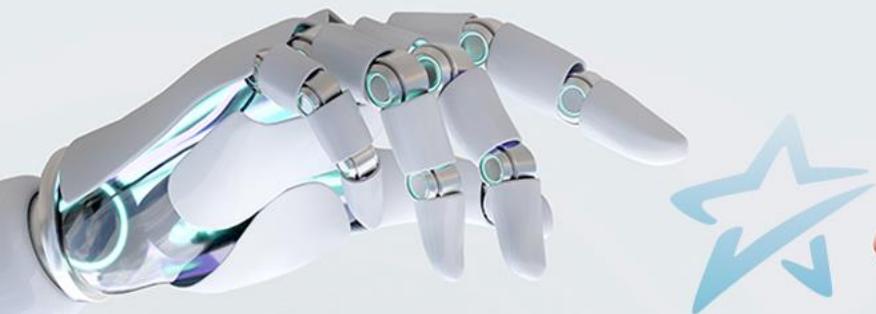
Cerca de ti, facilitamos tu vida y transformamos sueños en realidad.

Desafíos

Crear un portafolio de modelos de negocios disruptivos

Acelerar la velocidad de innovación

Transformación digital



Principios Generales

Los principios representan nuestra
filosofía empresarial
¿Qué nos diferencia de otras
organizaciones?

Transparencia
Respeto
Excelencia

Valores Institucionales

Los siguientes valores enmarcan
nuestra razón de ser

Pasión

Confianza

Vocación de Servicio

Resiliencia

Mapa de procesos

Misionales

- Gestión Comercial
- Gestión del Cliente
- Gestión Humana



Estratégicos

- Planeación Estratégica
- Sistema de Gestión



Apoyo

- Gestión Administrativa y Financiera
- Gestión Operativa
- Gestión Tecnológica y Analítica
- Cumplimiento



Evaluación

- Auditoría Interna



Alcance del Sistema de Gestión de seguridad de la información SGSI

El Sistema de Gestión de seguridad de la información, enmarcado por la NTC ISO/IEC 27001, se encuentra alineado con nuestro direccionamiento estratégico definido, gracias a esto brinda cobertura en la siguiente actividad:

***Operación y ejecución de contratos
comerciales de juegos de suerte y azar en
la sede principal de Susuerte S.A. de la
ciudad de Manizales***

Susuerte 
Siempre te da más!

 **SuperGIROS**[®]
Colombia Antioquia



Sistema de Gestión de Seguridad de la información SGSI

¿Qué beneficios trae?

- ✓ Mejora de la gestión de riesgos.
- ✓ Incremento de la confianza de los clientes y partes interesadas.
- ✓ Cumplimiento de requisitos legales y regulatorios.
- ✓ Reducción de incidentes de seguridad y pérdida de datos.

Pasos clave en la implementación del SGSI

Mejora y
capacitación
continua

Implementación
de controles de
seguridad

Desarrollo de
políticas y
procedimientos

Análisis de riesgos y
evaluación de la
seguridad de la
información

Susuerte 
Siempre te da más!

 **SuperGIROS**
Laboratorio Nacional

Política de Seguridad de la Información

Susuerte S.A., conoce el valor de la información y la importancia de proteger la confidencialidad, integridad y disponibilidad de esta, por esto, se compromete a salvaguardar los datos e información de las diferentes partes interesadas, además de dar cumplimiento a las obligaciones legales, normativas y contractuales aplicables, fomentando la mejora continua del sistema de gestión de seguridad de la información y apuntando a la transformación digital.



¿A qué ciberamenazas más frecuentes estamos expuestos?

Phising

Es aquella forma de fraude en la que el atacante intenta obtener información particular haciéndose pasar por una entidad o persona de confianza a través del correo electrónico u otros canales.

Ransomware

Programa informático malintencionado que infecta el sistema y restringe accesos a archivos y partes afectadas. Se pide un rescate a cambio de quitar esta restricción.

Scam

Engaños o estafas de internet que pueden llegar a través de spam o técnicas de ingeniería social. Buscan acceder a tu información personal convenciendo al usuario de la prestación de un servicio.

Robo de información

La información, sin precaución, puede ser siempre interceptada por terceros, que suele ir enfocada al robo de datos personales o fuga de información.



¿Cómo apporto al cumplimiento del SGSI?

2

Reportando inmediatamente cualquier anomalía o falla que puedan comprometer la seguridad de la empresa.

1

Conociendo y aplicando los procedimientos apropiados en relación con el manejo de la información y los sistemas informáticos.

3

Cuidando la información de la empresa y evitando difusión de datos confidenciales a terceros





Buenas prácticas de seguridad de la información

Uso de contraseñas seguras.

Encriptación de datos sensibles.

Mantenimientos y actualizaciones de los sistemas de forma regular.

Reporte y gestión de incidentes de seguridad.

Uso adecuado de los activos de información

Respaldo de la información, Back up

¿Cómo reportar eventos o incidentes de seguridad de la información?



Todo colaborador al identificar un posible evento o incidente de seguridad de la información se encuentra en la obligación de realizar este proceso.

Reportar a través de su equipo de soporte

Enviar un correo electrónico al líder del SGSI

Informar al Coordinador de Soporte o al Director de Seguridad según sea la naturaleza del evento o incidente

Crear ticket

MANIZALES

ADMINISTRATIVA

Sistemas de gestión

EVENTO/INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN



***¡Tú también haces
parte de nuestra
transformación digital!***

Susuerte 
Siempre te da más!

 **SuperGIROS**[®]
Colaboración Tecnológica