Capacitación mes de Febrero

2024

POLITICAS DEL SISTEMA INTEGRADO DE GESTIÓN

En Seguridad Imperio Ltda., somos conscientes de la responsabilidad que como empresatenemos frente a nuestros clientes, empleados, asociados de negocio y la comunidad en general.Es por esto que nos apoyamos en un Sistema Integral de Gestión QHSSE-ALA/CFT/FP (Calidad,Seguridad y Salud en el Trabajo, Seguridad y Control, SIPLAFT, Protección & Medio Ambiente), através del cual buscamos ser mejores cada día y así asegurar nuestra sostenibilidad.

- Política integral de gestión.
- Política de alcohol y drogas
- Política de responsabilidad social
- Política de sellos y firmas.
- Política de seguridad vial.

Todas nuestras políticas están publicadas en nuestra página web: www.seguridadimperio.com.co y puedes acceder a ellas con el siguiente link

Nuestro deber con las políticas de la empresa.

Cuando formalizamos nuestra vinculación con Seguridad Imperio; adquirimos una serie de responsabilidades para que nuestra relación laboral, cumpla con los parámetros establecidos.

Hablando específicamente frente a las políticas, nos encontramos que el Reglamento interno de trabajo nos dice:

Articulo 50 numeral 26: . Acoger, respetar y dar cumplimiento cabal a las políticas que, para la adecuación y desarrollo de su objeto social, implemente la empresa.

Articulo 54. constituyen faltas graves y son causales de despido justificado. Numeral 5. Cuando no cumpla las políticas y lineamientos de la empresa cliente y de SEGURIDAD IMPERIO. Numeral 7 Cuando se viole cualquiera de las políticas presentes o futuras que SEGURIDAD IMPERIO LIMITADA implemente.

Las políticas, le permiten a nuestra empresa garantizar el desarrollo necesario de estrategias que faciliten el cumplimiento de los objetivos institucionales; por otra parte a nosotros como trabajadores, nos garantiza la claridad en cuanto a las funciones y responsabilidades que debemos desarrollar.

Nuestros derechos frente a las Políticas de la empresa.

- Estar informados.
- Ser tenidos en cuenta.
- Ser escuchados para el mejoramiento de las mismas.
- Al debido proceso frente al supuesto incumplimiento de las políticas

Manejo de la información

La información es un bien que involucra los niveles económicos, intelectuales de una compañía y trascienden al ámbito personal; por esta sensibilidad, el manejo de la información ocupa un lugar muy critico en la toma de decisiones y la solución de problemas, siendo una clave para el desarrollo organizacional. Existen amenazas y vulnerabilidades que ponen en peligro el uso de la información siendo responsabilidad de todos los trabajadores de seguridad Imperio la confidencialidad, integridad y respeto sobre la información que se maneja.

Confidencialidad. Garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona.

Integridad. Manejo responsable que impide la modificación de manera intencional o accidental. Rigurosidad posible en el tratamiento de la información para evitar consecuencias tales como: Costos adicionales por errores, Trabajo duplicado, Malas tomas de decisiones, Daños de imagen de la marca frente a clientes, sociedad, autoridades y socios.

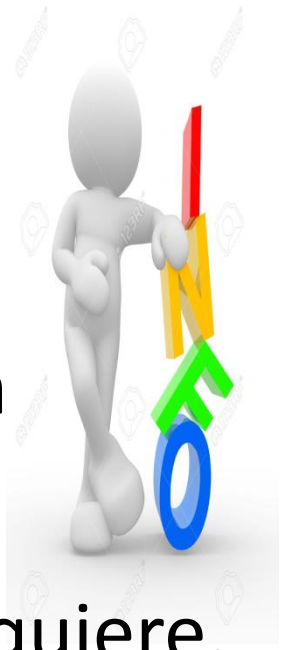
Respeto. Acatamiento que se debe tener frente a la comprensión de los datos públicos y privados que por ocasión del trabajo están bajo nuestro conocimiento y custodia.

Debemos asegurar que la información, independientemente de su fuente, en todo momento este protegida.

Nuestra empresa maneja una POLÍTICA DE TRATAMIENTO DE DATOS Y SEGURIDAD DE LA INFORMACIÓN.

El correcto manejo de la información con el cliente.

- Informar basado en el servicio
- Decir siempre la verdad
- Saber escuchar con respeto y atención
- Coherencia y reserva adecuada
- No decir ni hablar más de lo que se requiere.



Que no debemos hacer con la información.

- Mal interpretar la información
- Corromper las fuentes de la in-

Formación.

- Vulnerar los derechos de los demás con información sensible.
- Sustraer información propia de la empresa
- Violentar los mecanismos de protección de la información.

Proteger la información de la ciber criminalidad.

Sentarse, cerrar los ojos y... ¿tener suerte? Bueno, es un plan... pero conlleva una gran cantidad de riesgos, puesto que un ataque exitoso puede causar considerables daños:

- Sitios web y cuentas de redes sociales comprometidos (relativamente inofensivo)
- Pérdida de confianza debido a la filtración de información de clientes o datos de tarjetas de crédito
- Pago de “rescates” para recuperar el acceso a sus sistemas
- La necesidad de desarrollar nuevas estrategias tras el robo de secretos comerciales
- Pérdidas de ventas debido a las actividades afectadas de la compañía tras ataques
- Amplio daño a la propiedad, lesiones o incluso muertes debido a la piratería de infraestructuras críticas
- Responsabilidad personal que puede incluir implicaciones penales si no se han respetado los requisitos legales

Proteger la información de la ciber criminalidad.

Pautas para cuidarnos de la corrupción informática y evitar vulnerabilidades :

- Ver la seguridad informática como una tarea que nunca termina
- Crear una seguridad integral para frustrar los ataques a la red
- Convertir la seguridad informática en un tema clave
- Adherirse al uso de tecnología de última generación
- Generar una cultura de prevención y protección de datos sensibles.
- Verificación constante de fuga de información que atente contra la seguridad de las claves y muros de protección.
- Abstenerse de ingresar a páginas sospechosas o links que le pidan información.
- Dar informe de manera inmediata al jefe de medios tecnológicos de cualquier sospecha de vulneración de seguridad que pueda afectar a la empresa y/o los clientes.

Frase Final

En un mundo tan complejo; ser conscientes de la exposición al riesgo que tenemos y efectuar los debidos controles para disminuir nuestras vulnerabilidades; nos permiten cumplir tanto los objetivos de la empresa como nuestros objetivos personales.

Cumplamos nuestras políticas con decisión y reforcemos el buen manejo de la información