# TEMA DEL LUNES

## Norma ISO 27001 Seguridad de la Información

**En Ingeomega estamos avanzando para lograr la certificación de la norma ISO 27001 de seguridad de la información.**

## ¿Qué significa esta certificación?

Un compromiso para salvaguardar los activos de información ante amenazas que puedan comprometer su integridad, confiabilidad y disponibilidad.

Los cambios que se vienen realizando potencializarán nuestro rendimiento y minimizarán las vulnerabilidades a las que estamos expuestos, si todos seguimos las pautas evitaremos el acceso a nuestros activos de información por personas indebidas.

## Algunos temas importantes que se implementarán con esta certificación son:

- Retirar inmediatamente los documentos enviados para imprimir.
- Es importante la creación de contraseñas según las indicaciones del personal autorizado.
- El escritorio de los equipos no debe tener accesos directos a archivos o aplicativos no autorizados por el personal de las TIC.
- Almacenar bajo llave los documentos físicos cuando no estén siendo utilizados.
- Incentivar el bloqueo de sesión de los computadores cuando no se estén usando.

Identificar los diferentes procesos de seguridad de la información implementados en la organización.

Identificar y controlar las amenazas y vulnerabilidades a las que está expuesta la información de la organización.

## ¿Qué objetivos buscamos alcanzar con esta certificación?

Promover la mejora continua en la implementación y desarrollo del SGSI.

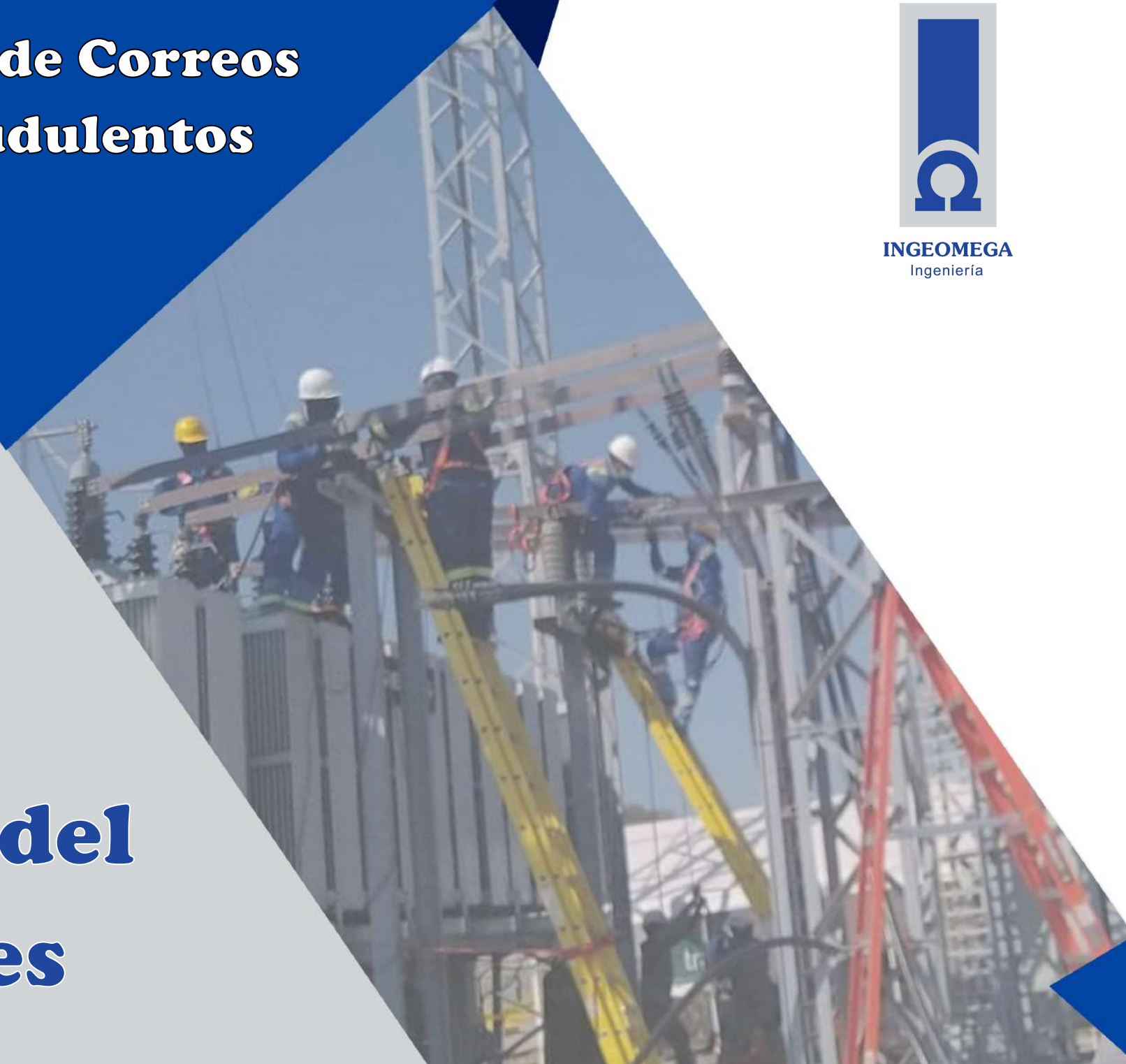
Generar y gestionar mecanismos que permitan el tratamiento adecuado de los incidentes de seguridad de la información.

# ¡Contamos contigo!

Con la ayuda de todos podemos lograr una cultura informática enfocada en la seguridad, con la implementación de buenas prácticas, mitigaremos los riesgos.

# ¡Feliz Semana!

# Tipos de Correos Fraudulentos



INGEOMEGA
Ingeniería

# Tema del Lunes

El correo electrónico es la principal puerta de entrada de los ciberdelincuentes en cualquier organización. Basándose en diferentes técnicas consiguen engañar a los usuarios y robar información confidencial o infectar los equipos con malware. Algunos de los fraudes más comunes son:

## Phishing

Engaño basado, generalmente, en la **suplantación de una empresa, entidad financiera** o red social. La finalidad es **hacerse con claves de acceso o información sensible.** Suele ser por el correo electrónico, SMS o aplicaciones como WhatsApp.

## Scam

Tipo de correos electrónicos cuya única finalidad es **perpetrar engaños y estafas** a sus receptores y obtener información personal, de la empresa o bancaria. El contenido del mensaje son falsos premios de lotería, ofertas de empleo que requieren de desembolsos, etc.

## Malware

Se trata de códigos maliciosos en correos que podrían contener algún tipo de **archivo adjunto o enlaces a webs donde una vez descargado infectará el dispositivo**. Una vez en nuestro equipo, podría distribuirse a través de la red corporativa, infectando todo tipo de dispositivos conectados a la misma.

# ¿Qué podemos hacer para detectar correos fraudulentos?

**1.** Comprobar el remitente del correo algunas veces no tiene que ver con la entidad a la que supuestamente representa. Revisar cada carácter, también son frecuentes suplantaciones cambiando alguna letra o utilizando una letra similar o que suene igual.

**2.** Cuando un correo presenta graves faltas de ortografía es una señal bastante certera de que ese mensaje es fraudulento. Los correos fraudulentos, en ocasiones, utilizan expresiones que no son las habituales en entidades. Ante un correo cuya forma de expresarse no es la común también habrá que comprobar su procedencia

**3.** Comprobar los logos y colores corporativos de la entidad que remite el corre, en algunas ocasiones, usan los elementos de la imagen corporativa de algunas empresas reconocidas para generar confianza, pero modifican y distorsionan colores y dimensiones de dichos elementos.

INGEOMEGA
Ingeniería

# ¡Feliz Semana!

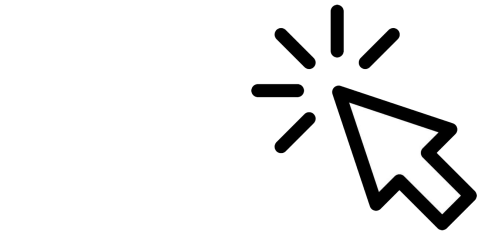
# Tema del Lunes

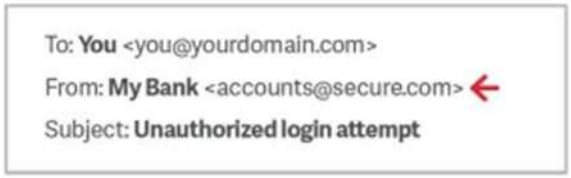
Tips para identificar

Correos Maliciosos

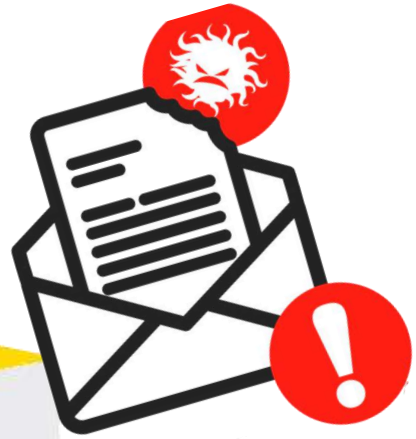
## 1 No confíes en el nombre para mostrar

Debes prestar mucha atención en el nombre y correo, generalmente los cibercriminales imitan perfectamente nombres y puedes confundirte. Verifica la dirección de correo electrónico en el encabezado de: (From:) y, si parece sospechoso, no abras el correo electrónico.






Ejemplo de phishing



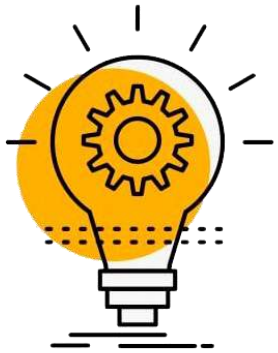
## 2 Mira pero no hagas clic

Mueve el mouse sobre cualquier enlace incrustado en el cuerpo del correo electrónico. Si la dirección del enlace parece rara, no hagas clic en ella.

## 3

## Comprueba si hay errores de ortografía.

Los mensajes legítimos no tienen errores de ortografía importantes o gramática deficiente. Lee tus correos electrónicos cuidadosamente e informa cualquier cosa que parezca sospechosa.



## 4

## Analiza el saludo

Los correos de empresas legítimas a menudo usan un saludo personal con tu nombre y apellido.

## 5

## No envíes información personal

Las organizaciones legitimas nunca solicitarán credenciales personales por correo electrónico. No las envíes.

## 6

## Cuidado con el lenguaje urgente o amenazante en la línea de asunto

Ten cuidado con las líneas de asunto que reclaman que «tu cuenta ha sido suspendida» o tu cuenta tuvo un «intento de inicio de sesión no autorizado».

## 7

## Revisa la Firma

La falta de detalles sobre el firmante o cómo puede ponerse en contacto con una empresa sugiere un problema. Las empresas legítimas siempre proporcionan datos de contacto.

## 8

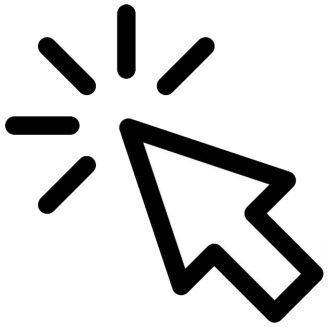
## No hagas clic en los archivos adjuntos

Incluir adjuntos maliciosos que contienen virus y malware es una táctica común. El malware puede dañar los archivos en tu computadora, robar tus contraseñas o espiarte sin tu conocimiento. No abras ningún archivo adjunto de correo electrónico que no estuvieras esperando.

## 9

## No confíes en el encabezado de la dirección de correo electrónico

Los estafadores no solo falsifican marcas en el nombre para mostrar, sino también marcas falsas en el encabezado de la dirección de correo electrónico debes prestar mucha atención en errores en la escritura de los dominios y correos electrónicos.



## 10

## No creas todo lo que ves

Los delincuentes son extremadamente buenos en lo que hacen. El hecho de que un correo electrónico tenga logotipos de empresa, lenguaje y una dirección de correo electrónico aparentemente válida, **no** significa que sea legítimo. Sé escéptico cuando se trata de tus mensajes de correo electrónico: si parece incluso sospechoso, no lo abras.

# Tema del Lunes

Tips para identificar

Correos Maliciosos

# Tema del Lunes

INGEOMEGA
Ingeniería

# Gestión de Contraseñas

En el trabajo diario se requiere el acceso a distintos servicios, dispositivos y aplicaciones para los cuales utilizamos la dupla: usuario y contraseña. Garantizar la seguridad de estos es fundamental para la empresa y la primera medida de seguridad a tomar es utilizar contraseñas seguras, por esto es indispensable tener buenas prácticas en el uso de estas claves:

## Robustez

La complejidad de la contraseña es una de las principales medidas de seguridad. En muchas ocasiones, se eligen contraseñas débiles fáciles, esto supone un riesgo, ya que los ciberdelincuentes pueden adivinarlas muy rápido, por ejemplo, comúnmente usado 123456 es descubierta en segundos.

Para conseguir una contraseña robusta se han de seguir las siguientes recomendaciones:

- Longitud mínima de 8 caracteres.
- utilizar combinaciones de letras mayúsculas, minúsculas, números y símbolos.
- Utilizar reglas nemotécnicas aplicadas a una frase, por ejemplo, «EuldlMCd2019!» que sale al comprimir la frase « En un lugar de la Mancha Correo de 2019!»;

## No compartir contraseñas

Las contraseñas deben ser una seña secreta, es decir, no se debe compartir con nadie, este es un principio básico, pero que muchas veces se omite. La contraseña debe ser intransferible y nadie bajo ningún concepto debe saber cuál es.


## No usar la misma contraseña

Utilizar la misma clave para acceder al correo electrónico y a otras plataformas que requiere de autenticación no es una práctica segura y supone uno de los errores más comunes en las personas.

Si un ciberdelincuente consigue hacerse con la contraseña en uno de estos servicios, por ejemplo, todos los servicios que utilizan la misma ían comprometidos, por eso, cada servicio debe ntraseña de acceso.

# ¡Feliz Semana!



INGEOMEGA
Ingeniería

# Tema del Lunes

INGEOMEGA
Ingeniería

# Dispositivos Móviles

Equipos portátiles, smartphones, tablets, terminales, etc permiten a los colaboradores desempeñar su trabajo en cualquier sitio, como si estuviera en las instalaciones de la empresa, lo que trae nuevos riesgos para la empresa asociados a la seguridad de la información.

# Riesgos en los dispositivos móviles

- **Los sitios web fraudulentos,** la publicidad agresiva o las páginas web de tipo phishing son las principales amenazas a las que se exponen

- **Utilizar redes wifi inseguras** puede poner en riesgo la privacidad de las comunicaciones, ya que los ciberdelincuentes pueden estar «escuchando» todo lo que se envía y recibe.

- El **robo o pérdida** de los móviles, tabletas, portátiles y dispositivos especializados. Este puede ser el riesgo más importante al que se exponen estos dispositivos debido a los datos sensibles que puedan estar almacenados en el equipo.

- **La infección por malware** siempre es un riesgo a tener en cuenta, pues el software malicioso puede robar información confidencial de la empresa y claves de acceso a diferentes recursos

- **Aplicaciones para uso personal** y que necesitan acceder a determinados permisos del dispositivo, en ocasiones excesivos o innecesarios (como acceso a la cámara, los contactos o los archivos).

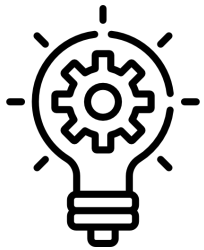
# Medidas de protección

## Desactivar función "Recordar contraseña"

La función de «Recordar contraseña» no debe usarse nunca en dispositivos móviles, ya que alguien no autorizado podría acceder a todos los servicios donde se haya activado esta función.

## Uso para fines corporativos

Hacer un uso adecuado de los dispositivos móviles y exclusivamente para actividades laborales, disminuye la probabilidad de acceder a contenidos malicioso que llegan por mensajería.



## No utilizar redes wifi inseguras

No es recomendable utilizar estas conexiones wifi que nos encontramos en hoteles, restaurantes, aeropuertos, etc., con dispositivos empresariales, ya que no conocemos su seguridad, ni su legitimidad y la privacidad de la información que enviamos o recibimos puede verse comprometida.

## No realizar modificaciones en el software

Los dispositivos cuentan con restricciones de fábrica que aumentan su seguridad y la de la información que manejan.

# Tema del Lunes

INGEOMEGA
Ingeniería

# ¡Feliz Semana!

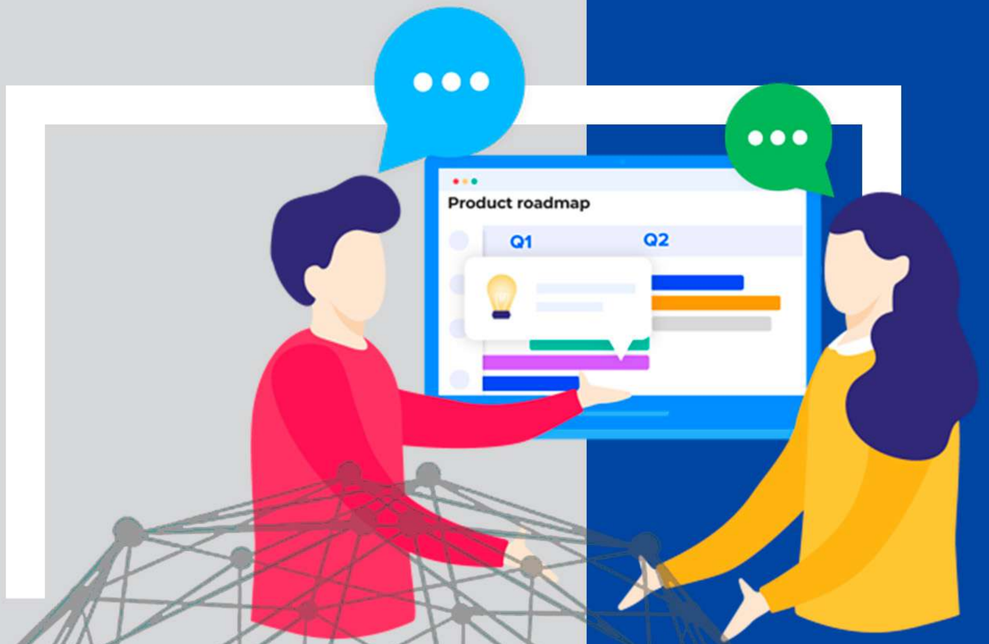
INGEOMEGA
Ingeniería

# Tema del Lunes

Conoce el proceso para administrar archivos o carpetas en la herramienta

**OneDrive**

¡Es momento de conectarnos!




# ¡Es momento de conectarnos!

OneDrive

Conoce información importante sobre **OneDrive** y la manera como esta herramienta puede ayudar en el desarrollo de las actividades laborales de una manera más óptima.

INGEOMEGA
Ingeniería

INGEOMEGA
Ingeniería

OneDrive

# Administrar archivos y carpetas en OneDrive

***¿Sabías que ahora puedes compartir archivos con tus compañeros sin necesidad de enviarlos por correo electrónico? Aprende a realizarlo:***

a. Ingresa a OneDrive y busca el archivo que necesites compartir o cárgalo.
b. Una vez lo tengas identificado, da clic derecho en el archivo y selecciona la opción compartir.
c. Ingresa el correo de la persona con la que vayas a compartir el archivo y da en la opción enviar y listo, has compartido tu archivo.

## ¡Es momento de conectarnos!

**Nota:** Office 365 ofrece diferentes tipos de licencias, depende del tipo de licencia que tengas podrás trabajar desde tu escritorio o simplemente en modo online.

INGEOMEGA
Ingeniería

OneDrive

# ¡Es momento de conectarnos!

## Si necesitas que tu archivo compartido tenga una configuración especial, ten presente los siguientes pasos:

a. Busca o carga el archivo que vas a compartir.

b. Una vez lo tengas identificado, da clic derecho en el archivo y selecciona la opción compartir.

c. En el cuadro de diálogo que se abre, ve a la opción del lápiz y después da clic a la opción **configuración de vínculo**.

d. Una nueva ventana se abrirá y podrás elegir una de las siguientes opciones:

- *¿Para quién quieres que funcione este vínculo?:* alguien de la organización, quien tenga el link o personas determinadas.

- *Establece si la persona a quien le compartes la información puede ver, editar o revisar la información.*

- *¿Quieres que el archivo sea compartido por un tiempo limitado?* Colócale una fecha de expiración.

- Para mayor seguridad podrás establecer una *contraseña* para abrir el documento o bloquear la descarga del archivo.

INGEOMEGA
Ingeniería

# Tema del Lunes

Conoce el proceso para administrar archivos o carpetas en la herramienta

**OneDrive**

¡Es momento de conectarnos!

# Tema del Lunes

INGEOMEGA
Ingeniería

## Seguridad de la Información

Al obtener la certificación en la norma ISO 27001, como organización hemos adoptados algunos compromisos esenciales para la protección y seguridad de los activos de información, por eso, es necesario recordar nuestra política de seguridad de información y todas las responsabilidades que esta implica en el uso o manejo de diferentes dispositivos.

## Política de Seguridad de la Información

Ingeomega S.A.S. está comprometida en proteger los recursos de información ante amenazas que puedan comprometer su integridad, confidencialidad y disponibilidad, implementando y manteniendo un sistema de gestión de seguridad de la información - SGSI, para intervenir oportunamente los incidentes, cumplir los requisitos legales, operar de forma segura las actividades contractuales, a partir de controles que reduzcan los riesgos en las transacciones internas y externas de información que involucran a las partes interesadas.

Los colaboradores asumen la responsabilidad de alinearse al SGSI en el acceso, uso y circulación de la información y de propender por la seguridad de esta, notificando oportunamente todas las condiciones e incidentes de seguridad que puedan generar consecuencias e impactos negativos para Ingeomega S.A.S.

Ten presente las siguientes recomendaciones :

## Uso del Celular

Como organización no se desconoce la importancia de la comunicación y la conectividad en los procesos y actividades realizadas por los colaboradores, pero se hace necesario establecer criterios básicos en el uso de dispositivos móviles.

- Para el uso del celular se debe respetar las normas y recomendaciones del plan de movilidad segura y SST (Seguridad social en el trabajo)
- El consumo de los servicios móviles debe tener como prioridad la utilización para fines estrictamente laborales.
- No está permitido el almacenamiento de información de Ingeomega S.A.S. en los dispositivos móviles.

## Activos de Información

En Ingeomega se establecen algunas medidas para el uso de equipos de procesamiento de información, como medida de prevención y cuidado de la seguridad de los activos de información.

- El uso del equipo será para que el usuario pueda llevar a cabo las funciones descritas para su cargo.
- No está permitido el almacenamiento local de información de Ingeomega S.A.S. en los equipos, la información debe permanece almacenada en los medios dispuestos en el Manual de almacenamiento en medios magnéticos

## Escritorio y Pantallas Limpias

Contar con escritorios y pantallas limpias va a permitir reducir los riesgos de acceso indebido, pérdida o daño en la información, por eso, siempre tenga presente:

- Almacenar bajo llave los documentos físicos cuando no estén siendo utilizados.
- Bloquear la sesión de los computadores cuando no se esté usando. Automáticamente se tiene configurado que el equipo se bloquea después de 5 minutos de inactividad, pero es responsabilidad del usuario bloquear el equipo cuando se ausente.
- Retirar inmediatamente los documentos enviados para imprimir. De los sitios de

## Mensajería Electrónica

La difusión y transmisión de información usando canales de mensajería electrónica, se realizará a través de mecanismos implementados por la organización, los cuales deben garantizar que el activo utilizado como medio responda a las exigencias de confidencialidad e integralidad en la información del mensaje transmitido.

# ¡Feliz Semana!

INGEOMEGA
Ingeniería