POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

1. Objeto

El objeto de este documento es desarrollar la política de clasificación de la información de cara a garantizar que esta se encuentre siempre protegida a un nivel apropiado.

2. Alcance

Este documento se aplica a todo el ámbito del Sistema de Gestión de la Seguridad de la Información (SGSI), es decir, a todo tipo de información, independientemente de la forma: documentos en papel o electrónicos, aplicaciones y bases de datos, conocimiento de las personas, etc.

Siendo los usuarios de este documento todos los empleados de **IRONCHIP TELCO, S.L.**

3. Información clasificada

1.1. Clasificación de la información

1.1.1. Criterios de clasificación

El nivel de confidencialidad se determina en función de los siguientes criterios:

- **Valor de la información:** basado en los impactos analizados durante la evaluación de riesgos
- **Sensibilidad y criticidad de la información:** basada en el riesgo más alto calculado para cada elemento de información durante la evaluación del riesgo
- **Obligaciones legales y contractuales:** basadas en la **18.1.1 RE - Listado requisitos legales**.

1.1.2. Niveles de confidencialidad

Toda la información debe clasificarse en niveles de confidencialidad.

Nivel de confidencialidad	Etiquetado	Criterios de clasificación	Restricción de acceso
Público	PÚBLICO	Hacer pública la información no puede dañar a la organización de ninguna manera	La información está disponible para el público
Interno	INTERNO	El acceso no autorizado a la información puede causar daños menores y/o inconvenientes a la organización	La información está disponible para todos los empleados y terceros seleccionados
Restringido	RESTRINGIDO	El acceso no autorizado a la información puede dañar considerablemente el negocio y / o la reputación de la organización	La información está disponible solo para un grupo específico de empleados y terceros autorizados

Confidencial	CONFIDENCIAL	El acceso no autorizado a la información puede causar daños catastróficos (irreparables) a las empresas y/o a la reputación de la organización	La información está disponible solo para algunos individuos de la organización

La regla básica es utilizar el nivel de confidencialidad más bajo que garantice un nivel adecuado de protección, a fin de evitar costos de protección innecesarios.

1.1.3. Listado de personas autorizadas

La información clasificada como "Restringido" y "Confidencial" debe ir acompañada de un Listado de Personas Autorizadas en la que el propietario de la información especifique los nombres o funciones laborales de las personas que tienen derecho a acceder a esa información.

La misma regla se aplica al nivel de confidencialidad “Interna" si personas ajenas a la organización debieran de tener acceso a dicho documento.

1.1.4. Reclasificación

Los propietarios de activos deben revisar el nivel de confidencialidad de sus activos de información cada dos años y evaluar si se puede cambiar el nivel de confidencialidad. Si es posible, debe reducirse el nivel de confidencialidad.

1.2. Etiquetado de la información

No es obligatorio el etiquetado de la información del nivel “Interno”, sobreentendiéndose que es de esta categoría.

Los niveles de confidencialidad se etiquetan de la siguiente manera:

- **Documentos en papel:** el nivel de confidencialidad se indica claramente en cada página del documento.
- **Documentos electrónicos:** el nivel de confidencialidad se indica claramente en cada página del documento.
- **Sistemas de información:** el nivel de confidencialidad en las aplicaciones y bases de datos debe indicarse en la pantalla de acceso al sistema si es posible Cada información contenida en el mismo tendrá su correspondiente etiqueta indicando el nivel de la información contenida.
- **Correo electrónico:** en el caso de que la información a tratar sea de carácter “Restringida” o “Confidencial”, el nivel de confidencialidad se indicará en la primera línea del cuerpo del correo electrónico.
- **Medios de almacenamiento electrónico (discos, tarjetas de memoria, etc.):** el nivel de confidencialidad deberá indicarse en la superficie superior de dicho medio en función de su contenido.
- **Información transmitida oralmente:** el nivel de confidencialidad de la información confidencial que debe transmitirse cara a cara, por teléfono o algún otro medio de comunicación, debe comunicarse antes de la información en sí.

1.3. Manejo de información clasificada

Todas las personas que accedan a información clasificada deben seguir las reglas enumeradas en la siguiente tabla. El Comité de Seguridad de la Información debe iniciar una acción disciplinaria cada vez que se infrinjan las reglas o si la información se comunica a personas no autorizadas. Cada incidente relacionado con el manejo de información clasificada debe ser reportado de acuerdo con el Procedimiento de Gestión de Incidentes.

Los activos de información sólo pueden ser retirados de las instalaciones después de obtener la autorización de acuerdo con la Política de Seguridad de TI.

El método para el borrado seguro y la destrucción de medios se prescribe en el documento Política de eliminación y destrucción segura.

	Interno	***Restringido****	***Confidencial****
Documentos en papel	• Sólo las personas autorizadas pueden tener acceso • Si se envía fuera de la organización, el documento debe enviarse como correo certificado • Los documentos sólo pueden conservarse en salas sin acceso público • Los documentos deben retirarse con frecuencia de impresoras o máquinas de fax	• El documento debe almacenarse en un archivador cerrado con llave • Los documentos pueden transferirse dentro y fuera de la organización sólo en un sobre cerrado con la clasificación correctamente indicada • Si se envía fuera de la organización, el documento debe enviarse por correo con un servicio de acuse de recibo de devolución • Los documentos deben retirarse inmediatamente de las impresoras o máquinas de fax • Sólo el propietario del documento puede copiar el documento • Sólo el propietario del documento puede destruir el documento	• El documento debe almacenarse en un archivador cerrado con llave • El documento puede ser transferido dentro y fuera de la organización sólo por una persona de confianza en un sobre cerrado y sellado con la clasificación correctamente indicada • Si se envía fuera de la organización, el documento debe enviarse por correo con un servicio de acuse de recibo de devolución • No se permite enviar por fax el documento • El documento sólo podrá imprimirse si la persona autorizada está de pie junto a la impresora • Sólo el propietario del documento puede copiar el documento • Sólo el propietario del documento puede destruir el documento
Documentos electrónicos	• Sólo las personas autorizadas pueden tener acceso	• Sólo las personas autorizadas para este documento podrán acceder a la parte del sistema de información	• Sólo las personas autorizadas para este documento podrán acceder a la parte del sistema de información en

	• Cuando los archivos se intercambian a través de servicios como FTP, mensajería instantánea, etc., deben estar protegidos con contraseña • El acceso al sistema de información donde se almacena el documento debe estar protegido por una contraseña segura • La pantalla en la que se muestra el documento debe bloquearse automáticamente después del tiempo de inactividad definido	en la que esté almacenado el presente documento • Cuando los archivos se intercambian a través de servicios como FTP, mensajería instantánea, etc., deben cifrarse • La pantalla en la que se muestra el documento debe bloquearse automáticamente después del tiempo de inactividad definido • Sólo el propietario del documento puede borrar el documento	la que esté almacenado el presente documento • El documento debe almacenarse en forma cifrada • El documento sólo puede almacenarse en servidores controlados por la organización • El documento no debe ser intercambiado a través de servicios como FTP, mensajería instantánea, etc. • La pantalla en la que se muestra el documento debe bloquearse automáticamente después del tiempo de inactividad definido • Sólo el propietario del documento puede borrar el documento
Sistemas de información	• Sólo las personas autorizadas pueden tener acceso • El acceso al sistema de información debe estar protegido por una contraseña segura • La pantalla debe bloquearse automáticamente después del tiempo de inactividad definido • El sistema de información sólo podrá estar situado en salas con acceso físico controlado	• Sólo las personas autorizadas pueden tener acceso • El acceso al sistema de información debe estar protegido por una contraseña segura • La pantalla debe bloquearse automáticamente después del tiempo de inactividad definido • Los usuarios deben cerrar la sesión del sistema de información si han abandonado temporal o permanentemente el lugar de trabajo • El sistema de información sólo podrá estar situado en salas con acceso físico controlado • Los datos deben borrarse solo con un algoritmo que garantice una eliminación segura	• Sólo las personas autorizadas pueden tener acceso • La pantalla debe bloquearse automáticamente después del tiempo de inactividad definido • Los usuarios deben cerrar la sesión del sistema de información si han abandonado temporal o permanentemente el lugar de trabajo • El sistema de información sólo puede instalarse en servidores controlados por la organización • El sistema de información sólo podrá ubicarse en salas con acceso físico controlado y control de identidad de las personas que accedan a la sala • Los datos deben borrarse solo con un algoritmo que garantice una eliminación segura

Correo electrónico	• Sólo las personas autorizadas pueden tener acceso • El remitente debe comprobar cuidadosamente el destinatario • Se aplicarán todas las normas establecidas en "Sistemas de información"	• Sólo las personas autorizadas pueden tener acceso • El remitente debe comprobar cuidadosamente el destinatario • El correo electrónico debe cifrarse si se envía fuera de la organización • Se aplicarán todas las normas establecidas en "Sistemas de información"	• Sólo las personas autorizadas pueden tener acceso • El remitente debe comprobar cuidadosamente el destinatario • Todos los correos electrónicos deben estar cifrados • Se aplicarán todas las normas establecidas en "Sistemas de información"
Medios de almacenamiento electrónico	• Sólo las personas autorizadas pueden tener acceso • Los medios y archivos deben estar protegidos con contraseña • Si se envía fuera de la organización, el medio debe enviarse como correo certificado • El medio sólo podrá conservarse en habitaciones con acceso físico controlado	• Sólo las personas autorizadas pueden tener acceso • Los medios y archivos deben estar cifrados • Los medios deben almacenarse en un armario cerrado con llave • Si se envía fuera de la organización, el medio debe enviarse por correo con un servicio de recibo de devolución • El medio sólo podrá conservarse en habitaciones con acceso físico controlado • Sólo el propietario del medio puede borrar o destruir el medio	• Sólo las personas autorizadas pueden tener acceso • Los medios y archivos deben estar cifrados • Los medios deben almacenarse en un armario cerrado con llave • Los medios de comunicación pueden ser transferidos dentro y fuera de la organización solo por una persona de confianza en un sobre cerrado y sellado. • El medio sólo podrá conservarse en habitaciones con acceso físico controlado • Sólo el propietario del medio puede borrar o destruir el medio
Información transmitida oralmente	• Sólo las personas autorizadas pueden tener acceso a la información • Las personas no autorizadas no deben estar presentes en la sala cuando se comunique la información	• Sólo las personas autorizadas pueden tener acceso a la información • Las personas no autorizadas no deben estar presentes en la sala cuando se comunique la información • La habitación debe estar insonorizada • La conversación no debe grabarse	• Sólo las personas autorizadas pueden tener acceso a la información • Las personas no autorizadas no deben estar presentes en la sala cuando se comunique la información • La habitación debe estar insonorizada • La conversación no debe grabarse • La conversación realizada a través de un medio de

			comunicación debe estar encriptada ● No se puede conservar ninguna transcripción de la conversación

* Los controles se implementan acumulativamente, lo que significa que los controles para cualquier nivel de confidencialidad implican la implementación de controles definidos para niveles de confidencialidad más bajos: si se prescriben controles más estrictos para