IRONCHIP TELCO

www.ironchip.com

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS

ÍNDICE

1. Objeto

Esta política tiene como objeto desarrollar las reglas básicas para el uso aceptable de la información y los activos asociados al tratamiento de ésta. Se busca establecer medidas de seguridad adecuadas para proteger la información y los activos asociados al tratamiento de la misma, asegurando su confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad.

2. Alcance

Este documento aplica a los siguientes activos:

- La información y data, es decir, aquella información o data que permite interactuar con los sistemas de seguridad de la información y las redes de comunicaciones.
- Los asociados para el tratamiento de la citada información (software, hardware, redes de comunicaciones, soportes de información, equipamiento auxiliar e instalaciones).

El tratamiento de la información se deberá realizar atendiendo todas las medidas de seguridad que garanticen su:

- **Confidencialidad:** El acceso a la información estará restringido exclusivamente a personas o procesos que cuenten con la debida autorización, implementando controles de acceso adecuados y métodos de encriptación cuando sea necesario.
- **Integridad:** Se garantizará que la información se mantenga exacta y completa tal como fue generada, aplicando controles de integridad, como firmas digitales y hash, para prevenir y detectar alteraciones no autorizadas.
- **Trazabilidad:** Se registrarán todas las acciones realizadas sobre la información y los sistemas mediante mecanismos de auditoría y logs de actividad, permitiendo así un seguimiento detallado y la identificación de cualquier acceso o modificación no autorizada.
- **Autenticidad:** Se implementarán mecanismos de autenticación robustos, como autenticación multifactor y certificados digitales, para verificar la identidad de usuarios y sistemas antes de permitirles el acceso a la información.
- **Disponibilidad:** La información y los sistemas estarán accesibles a las personas o procesos autorizados en el momento que lo requieran, implementando medidas de redundancia, recuperación ante desastres y planes de continuidad de negocio.

3. Objetivos

Los siguientes objetivos establecidos en este documento dan orientación hacia el cumplimiento de actividades que permiten la gestión adecuada del sistema de seguridad de la información y protección de datos:

- **Identificación y clasificación de la información:** Categorizar la información según su importancia y nivel de sensibilidad para determinar los niveles apropiados de protección y acceso.
- **Políticas y procedimientos de seguridad:** Establecer políticas confiables y procedimientos que aborden aspectos como el acceso autorizado, la gestión de contraseñas, la protección de datos, entre otros.
- **Seguimiento y control:** Implementar un sistema para monitorear, controlar y gestionar las actividades, tareas y acciones de seguridad, asegurando que siempre se apliquen adecuadamente las políticas, procedimientos, protocolos, entre otros.
- **Acceso y permisos:** Definir quién tiene acceso a la información de seguridad y en qué condiciones. Esto puede incluir la implementación de controles de acceso físico y lógico, así como la asignación de roles y responsabilidades.
- **Formación y concienciación:** Proporcionar formación regular a los empleados sobre las políticas de seguridad y los procedimientos para acceder y gestionar la información de manera segura.

4. Identidad Corporativa

4.1. Misión

En Ironchip, nuestra misión es liderar la revolución en seguridad cibernética, proporcionando soluciones innovadoras y de vanguardia basadas en nuestra tecnología LBS (Location Based Security). Nos comprometemos a ofrecer productos y servicios que garanticen la protección de la ubicación y la integridad de los datos de nuestros clientes, contribuyendo así a un entorno digital más seguro y confiable fundamentado en un sistema de gestión de la información y protección de datos alineado con las normas y estándares internacionales.

4.2. Visión

Nuestra visión es ser reconocidos a nivel mundial como el referente en seguridad cibernética basada en ubicación, proporcionando soluciones que establezcan un nuevo estándar en la protección de la identidad y

los activos digitales. Aspiramos a ser líderes en innovación tecnológica, brindando seguridad y tranquilidad a empresas, organizaciones y usuarios finales a través de la gestión adecuada de nuestros procesos establecidos dentro un sistema que continuamente evoluciona para garantizar la seguridad de la información y la protección de datos en un mundo cada vez más interconectado.

4.3. Valores

- **Innovación:** Buscamos constantemente nuevas formas de abordar los desafíos de seguridad cibernética y desarrollar soluciones que superen las expectativas de nuestros clientes.
- **Integridad:** Actuamos con honestidad, ética y transparencia en todas nuestras operaciones y relaciones comerciales.
- **Compromiso:** Nos comprometemos a brindar soluciones de alta calidad y a mantener la confianza y lealtad de nuestros clientes.
- **Colaboración:** Fomentamos un entorno de trabajo colaborativo donde el trabajo en equipo y el intercambio de ideas son valorados y promovidos.
- **Excelencia:** Nos esforzamos por alcanzar la excelencia en todo lo que hacemos, desde la innovación tecnológica hasta la atención al cliente.

5. Normativa Aplicable

5.1. Normativa General

Este documento aplica a los siguientes activos: los datos personales de clientes y empleados, los sistemas de información y redes de la empresa, los servicios de pago ofrecidos, las comunicaciones electrónicas y servicios digitales proporcionados, las infraestructuras y tecnologías de telecomunicaciones utilizadas, así como cualquier otro activo relacionado con la actividad de la empresa de ciberseguridad. Estos activos están sujetos a las disposiciones establecidas en:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Real Decreto 311/2022, de 3 de mayo, por el que se aprueba el Esquema Nacional de Seguridad (ENS).
- ISO/IEC 27001:2022.
- ISO/IEC 27701:2019.

- ISO/ IEC 37001:2016.
- UNE 19601:2017.
- Real Decreto 43/2021, de 26 de enero, por el que se aprueba el Reglamento de la Ley de Servicios de Pago (RLSP).
- Convenio Colectivo de Oficinas y Despachos Bizkaia 2009-2012
- BOE núm. 273, de 14 de noviembre de 1972, páginas 20248 a 20257- Ordenanza Laboral de Oficinas y Despachos.

5.2. Normativa Específica

5.2.1. Uso Apropiado de los Activos

La información y el resto de los activos asociados a la misma deberán ser utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de las personas usuarias.

Se prohíbe expresamente:

- Utilizar los activos proporcionados por Ironchip Telco, S.L. para actividades no relacionadas con su propósito.
- Introducir en los sistemas de información de Ironchip Telco, S.L. contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente en los sistemas de información de Ironchip Telco, S.L. cualquier tipo de malware (virus, gusanos, troyanos, programas espía, ransomware, etc.), dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos.
- Obtener otros derechos o accesos distintos a aquellos que Ironchip Telco, S.L. le haya asignado. En caso de que esto ocurra deberá advertir inmediatamente al equipo de sistemas.
- Acceder a las áreas restringidas de Ironchip Telco, S.L. sin estar autorizado para ello.
- Descifrar las contraseñas, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de Ironchip Telco, S.L.
- Distorsionar o falsear los registros (logs) de los sistemas de información de Ironchip Telco, S.L.

- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otras personas usuarias, dañar o alterar los recursos informáticos de Ironchip Telco, S.L.
- Destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos con información importante para la empresa.
- Guardar información en las unidades locales de disco de dispositivos no autorizados, excepto temporalmente bajo circunstancias excepcionales y expresa autorización necesaria para la programación de proyectos de desarrollo en los que se trabaje y esto se requiera irremediablemente.
- Pasar o intercambiar equipo/accesorio de Ironchip Telco, S.L entre usuarios.

5.2.2. Seguridad de los Dispositivos de Almacenamiento Masivo

El uso de dispositivos de almacenamiento masivo, tales como discos duros externos, unidades USB y otros dispositivos similares, está prohibido salvo autorización expresa. Cualquier uso de estos dispositivos deberá:

- Ser gestionado de acuerdo con la normativa de seguridad de la información de Ironchip Telco, S.L.
- Contar con la autorización expresa del responsable de seguridad: security@ironchip.com.
- Ser utilizado únicamente para los fines específicos autorizados y no para almacenamiento personal o no relacionado con las actividades laborales.

El uso indebido o no autorizado de dispositivos de almacenamiento masivo puede acarrear sanciones, incluyendo el despido.

5.3. Confidencialidad

Los usuarios que tengan acceso a información de Ironchip Telco, S.L. deberá considerar que dicha información, por defecto, tiene el carácter de interna. Sólo se podrá considerar como información no interna o pública aquella información a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos a tal efecto por Ironchip Telco, S.L.

- Se evitará la revelación, modificación, destrucción o mal uso de la información cualquiera que sea el soporte en que se encuentre.
- Se salvaguardará por el tiempo normativo/legal indicado y no se emitirá al exterior información interna sin previa autorización y aplicación de controles de acceso.

Todas estas obligaciones continuarán vigentes tras la finalización de su relación con Ironchip Telco, S.L. Por lo tanto, el incumplimiento de estas obligaciones podrá constituir una falta grave de revelación de secretos.

Además de las consideraciones ya mencionadas, para garantizar la seguridad de los datos de carácter personal, la persona usuaria deberá considerar las siguientes normas de actuación:

- Solo podrá crear ficheros cuando sea necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán guardados por largos periodos de tiempo en unidades locales de disco de los dispositivos autorizados y asignados de la persona usuaria, y deberán ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon. Solo se podrá guardar temporalmente la programación del proyecto de desarrollo en el que trabaja la persona.
- No se albergarán datos de carácter personal en las unidades locales de disco de los dispositivos autorizados y asignados a la persona usuaria, o en cuentas en la nube de servicios autorizados que no tengan que ver con sus actividades laborales o con datos de su propia persona.
- La salida de soportes y documentos fuera de los locales en los que esté ubicada dicha información, únicamente podrá ser autorizada por el responsable de seguridad (security@ironchip.com) valorando las medidas de seguridad contenidas en este documento.
- La transmisión de información interna a través de redes de telecomunicaciones (p.e. Correo electrónico) no se realizará en claro. Se deberá compartir la información interna con terceros a través del Entorno Colaborativo (gestor documental, sincronizador de archivos) autorizado, cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceras personas.

5.4. Procedimiento Disciplinario

La persona usuaria que incumpla la presente normativa estará sujeta al inicio de un proceso disciplinario y, dependiendo de la gravedad del caso, a un proceso sancionador.

Ironchip Telco, S.L. podrá implementar controles para verificar el cumplimiento de esta normativa, garantizando en todo momento el respeto a la legislación vigente en materia de protección de datos personales y el derecho a la intimidad.

Respecto al procedimiento sancionador y sistema disciplinario, estos se regirán por lo señalado en los documentos **C 6 DO - SISTEMA DISCIPLINARIO** y **C 6.1 PR - PROCEDIMIENTO SANCIONADOR.**

6. Seguridad Física y Virtual

Las instalaciones de Ironchip Telco S.L., proporcionarán un espacio con condiciones de temperatura y humedad adecuada para el buen desempeño de los equipos de trabajo técnicos y humanos, así como la protección frente a amenazas identificadas por los análisis de riesgos indicadas en el **A.2 8.2 RE - Análisis y Gestión de Riesgos**. Además, se establecerán las instalaciones adecuadas de cableado eléctrico, y junto a ello, se dispondrá de elementos de seguridad contra incendios e inundaciones suministrados por un proveedor especializado.

6.1. Seguridad Física

El acceso a las áreas de trabajo de Ironchip Telco, S.L. estarán limitadas a través de las siguientes medidas de seguridad:

- **Muros cercados:** funciona como un primer punto de seguridad física, disuade a los intrusos al plantear un daño material.
- **Cerraduras:** contramedida típica, permite solo personas con una llave digital de acceso, las cuales serán entregadas por el departamento de Administración, estando correctamente inventariado en **A.1 8.1.1 RE - Inventario Material** el personal poseedor de cualquier llave de acceso.
- **Alarma de seguridad:** con sensores de acceso y cámaras de vigilancia se pueden rastrear accesos no autorizados, los cuales serían gestionados por la compañía proveedora del servicio alertando a las autoridades y los contactos de emergencia. Como contramedida ante estos accesos no autorizados, el sistema cuenta con unas bombas que cubrirán todo el enclave de un humo que impediría una correcta visión y respiración.
- **Detectores de humo, sistemas de extinción de incendios:** para detener el evento de incendio.

El acceso a la documentación se limitará exclusivamente a las personas autorizadas.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en la respectiva legislación y de acuerdo con los requisitos de las organizaciones cliente. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que impidan su apertura.

Cuando las características físicas de aquéllos no permitan adoptar esta medida, se adoptarán medidas que impidan el acceso de personas no autorizadas.

Mientras los soportes o documentos no se encuentren archivados en los dispositivos de almacenamiento establecidos en el apartado anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de esta deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

En caso de recepción de visitas de clientes, proveedores, invitados, entes institucionales públicos, y hasta el suministro de paquetes por empresas de mensajería, remitirse al **A.1 11.1.6 PR - Procedimiento de Control de Accesos y Recepción de Visitas**.

6.2. Documentos y Dispositivos

Los documentos y dispositivos que contienen información interna deberán permitir identificar su contenido, ser inventariados y solo ser accesibles a las personas autorizadas.

La salida de documentos, incluidos los comprendidos y/o anexos a un correo electrónico, fuera de los locales bajo el control de Ironchip Telco, S.L. deberá realizarse a través del Entorno Colaborativo (gestor documental, sincronizador de archivos) autorizado a correos electrónicos individuales, no compartidos. Una vez finalizada la necesidad de compartir se revocará el acceso.

En el traslado de la documentación se deberán adoptar las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Siempre que vaya a desecharse cualquier documento que contenga información interna deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo documento y/o su recuperación posterior.Además, se tendrán sistemas de alertas para identificar el borrado de información masivo o total sin la respectiva autorización.

La identificación de los soportes que contengan información interna se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan identificar su contenido a las personas usuarias con acceso autorizado a los citados documentos, y que dificulten la identificación para el resto de las personas.

En todo caso, deberá cumplir la **A.1 8.2.1 PO - Política de Clasificación de la Información**.

6.3. Protección Frente al Malware

Se mantendrán los sistemas de información al día con las últimas actualizaciones de seguridad disponibles.

En la microinformática, los sistemas operativos dispondrán de software antimalware. Además, el software antimalware deberá estar siempre habilitado y actualizado, tal y como lo indica el **A.1 12.2.1 PR - Procedimiento ante Software Malicioso**.

6.4. Intercambio de Información

Ninguna persona usuaria deberá ocultar o manipular su identidad bajo ninguna circunstancia.

La distribución de información ya sea en formato electrónico o físico se realizará mediante los recursos determinados en el contrato de prestación de servicio para tal cometido y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato.

En relación con el intercambio de información, se considerarán no autorizadas las siguientes actividades:

- Transmisión o recepción de material por los derechos de autor infringiendo la Ley de Protección Intelectual.
- Transmisión o recepción de toda clase de material pornográfico, de naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Transferencia de información interna a terceras personas no autorizadas.
- Transmisión o recepción de aplicaciones no relacionadas con el negocio.
- Participación en actividades de Internet, como grupos de noticias, juegos u otras que no estén directamente relacionadas con la prestación del servicio.

Todas las actividades que puedan dañar la imagen y reputación de Ironchip Telco, S.L. están prohibidas en Internet y en cualquier otro lugar.

6.5. Uso del Correo Electrónico

Este recurso se utilizará con una finalidad profesional. Cualquier otro uso está prohibido.

Se prohíbe expresamente la interceptación y/o uso no autorizado de mensajes o direcciones de correo electrónico de otras personas usuarias.

La persona usuaria deberá rechazar cualquier mensaje de correo electrónico que provenga de fuentes no fiables, ya que podría contener virus o códigos maliciosos, spam, etc.

La persona usuaria deberá evitar la divulgación innecesaria de la dirección de correo, principalmente no participando en cadenas de mensajes, por altruista que pueda parecer su objetivo.

6.6. Conectividad a Internet

Este recurso se utilizará con una finalidad profesional. Cualquier otro uso está prohibido. Se debe tener en cuenta lo indicado en **A.1 10.1.1 PO - Política de Criptografía y Comunicaciones Protegidas** y en **A.1 9.1 PO - Política de Control de Acceso Lógico**.

En ningún caso deberá accederse a direcciones de Internet no autorizadas, como por ejemplo: de juegos, de contenido sexual, o que resulten ofensivas o que atenten contra la dignidad humana o los derechos fundamentales.

Además, en caso de que alguna de las direcciones de internet que se visiten presenten situaciones anómalas o sospechosas de riesgos que atenten contra la seguridad de la información, es deber y responsabilidad del empleado comunicarlo al responsable de sistemas.

6.7. Seguridad Lógica

Las personas usuarias tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. Se establecerán mecanismos para evitar que una persona usuaria pueda acceder a recursos con derechos distintos de los autorizados.

El responsable de sistemas se encargará de que exista una relación actualizada de personas usuarias y perfiles, y los accesos autorizados para cada una de ellas.

En caso de que existan personas usuarias externas a la Organización deberán estar sometidos a las mismas condiciones y obligaciones de seguridad que las personas internas según los atributos definidos para ellas.

Se deberá establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de toda aquella persona usuaria que intente acceder a los sistemas de información y la verificación de que está autorizada.

El procedimiento de asignación, distribución y almacenamiento de contraseñas garantizará su confidencialidad e integridad, así como lo indica la **A.1 8.3.3 PO - Política de Cifrado y Contraseñas**.

7. Responsabilidades de la Persona Usuaria

7.1. Uso de Contraseñas

La persona usuaria no deberá revelar bajo ningún concepto su identificador y/o contraseña a otra persona usuaria ni mantenerla por escrito a la vista, ni al alcance de terceras personas.

En caso de que el sistema de información no lo solicite automáticamente, la persona usuaria deberá informar a la persona administradora.

Es especialmente importante mantener el carácter secreto de la contraseña. No debe entregarse ni comunicarse a nadie. En caso de haber tenido necesidad de hacerlo, el usuario deberá proceder a cambiarla de forma inmediata.

Si la persona usuaria sospecha que su identificador y contraseña está siendo utilizado por otra persona, inmediatamente deberá proceder al cambio de su contraseña y notificar el incidente a security@Ironchip.com.

Todas las contraseñas propiedad de la compañía deberán de estar almacenadas en la Herramienta de gestión de secretos autorizada y tener el acceso configurado para acceder con la tecnología de autenticación de Ironchip Telco, S.L., tal y como lo indica la **A.1 8.3.3 PO - Política de Cifrado y Contraseñas**.

7.2. Equipos, Dispositivos o Máquinas

La persona usuaria deberá asegurarse de que sus dispositivos autorizados y asignados cumplan las siguientes normas:

- Bloqueo Automático por Inactividad:
    - Los dispositivos deben bloquearse automáticamente tras un periodo máximo de 3 minutos de inactividad.
- Prohibiciones:
    - No deben contener herramientas que puedan transgredir las medidas de seguridad.
    - No deben incluir programas no homologados.

- Seguridad del Sistema:
    - Los dispositivos deben tener antimalware actualizado y activado en los sistemas operativos utilizados para actividades laborales.
    - Deben mantenerse al día con las últimas actualizaciones de seguridad disponibles.
- Responsabilidad y Custodia:
    - La persona usuaria es responsable de su equipo (ordenador) y debe custodiarlo adecuadamente.
    - Idealmente, el equipo siempre debe llevarse a casa por la persona usuaria. Sin embargo, mínimamente debe dejarse el equipo en la oficina bajo llave.
    - En caso de pérdida o sustracción del equipo portátil o dispositivo móvil, llama inmediatamente al equipo de sistemas o al servicio de asistencia técnica de la empresa. Si no puedes llamar, envía un correo electrónico a la dirección de soporte de TI: support@ironchip.com.

      El equipo de sistemas será el encargado de borrar los accesos asociados a ese dispositivo para evitar el acceso no autorizado a los servicios de Ironchip.

En el proceso de vinculación laboral se le informará a la persona futura empleada de Ironchip Telco S.L., que para el acceso a las herramientas o softwares de trabajo, se requiere de la identificación y autorización a través de su dispositivo personal aplicándose el concepto de Bring Your Own Device (BYOD); por lo que en caso de que la persona no esté dispuesta a autorizar la utilización de su dispositivo personal, la empresa le dotará de un dispositivo corporativo para ello, y para la gestión de comunicaciones profesionales, y demás informaciones o temas relacionados con las actividades laborales del cargo respectivo.

7.3. Puesto de Trabajo

La persona usuaria deberá respetar al menos las siguientes normas de escritorio limpio, con el fin de proteger los documentos en papel, soportes informáticos y dispositivos portátiles de almacenamiento y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:

- Almacenar bajo llave los documentos en papel y los medios informáticos, cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Bloquear la sesión o apagar los dispositivos autorizados y asignados de la persona usuaria al dejarlo desatendido.

- Proteger tanto los puntos de recepción y envío de información (correo postal, máquinas de scanner y fax) como los equipos de duplicado (fotocopiadora, fax y scanner).
- Retirar, sin retraso injustificado, cualquier información interna una vez impresa.
- Destruir la información interna una vez deje de ser necesaria.
- No deben haber objetos inflamables o de fácil combustión, ni líquidos o gaseosos, que puedan causar daño a los dispositivos, considerándose por la persona dueña del puesto de trabajo, el debido riesgo de accidentes.

7.4. Devolución de los Activos

La persona usuaria deberá devolver toda la información y los activos asociados que estén en su poder al finalizar su relación con Ironchip Telco, S.L. Como evidencia de dicha devolución por parte de la persona usuaria a la compañía de aquellos activos puestos a su disposición para la ejecución de sus funciones, se deberá completar y firmar el documento de Devolución de Material.

Los accesos a la información y a los activos de tratamiento de cada una de las personas usuarias deberán ser cancelados a la finalización de la relación con Ironchip Telco, S.L., o deberán ser adaptados a los cambios de funciones producidos.

8. Cultura Organizacional

8.1. Formación y Concienciación

- **Responsabilidad de Recursos Humanos:** El departamento de Recursos Humanos es el encargado de realizar las formaciones relativas a la seguridad de la información y protección de datos.
- **Obligatoriedad de la Formación:** Todos los empleados están obligados a participar en las formaciones impartidas por la empresa.
- **Evaluación de la Formación:** Se realizarán periódicamente evaluaciones sobre las formaciones y/o capacitaciones impartidas, las cuales deberán ser superadas por los trabajadores.
- **Concienciación Continua:** El departamento de Recursos Humanos con el apoyo de otros departamentos enviará correos electrónicos de concienciación relacionados con seguridad de la información y protección de datos a los empleados recordándoles su importancia.

Estas medidas son fundamentales para asegurar que todos los empleados de Ironchip Telco, S.L. comprendan y apliquen las políticas de seguridad de la información y protección de datos, garantizando así la seguridad y la integridad de los datos manejados por la empresa.

8.2. Teletrabajo

El teletrabajo se regulará mediante la activación de las siguientes normas:

- Todo el personal de la empresa está autorizado a sacar el equipo (ordenador) asignado fuera de la oficina; ya que para cada empleado dicho equipo (ordenador) es único e intransferible, por lo que la persona usuaria es responsable de su correcta custodia, acceso, manejo de información y adecuado bloqueo, tal como se indica en los anteriores apartados de este documento.
- No se permitirá la utilización de infraestructura (software, hardware y redes de comunicaciones) no controlada por Ironchip Telco, S.L. o que no cumplan con las medidas técnicas de seguridad de la información establecidas por la compañía.
- Se deberá cumplir todo lo definido en este documento, considerándose los deberes y derechos del empleado, así como las responsabilidades de la empresa, así como las sanciones por incumplimiento.
- Se controlará la revocación de derechos de acceso tras la finalización del periodo de necesidad de este.
- Está prohibido almacenar contraseñas en papel en la mesa de trabajo o lugar donde se lleve a cabo el teletrabajo (Mesas limpias).
- El equipo (ordenador, laptop, desktop, dispositivo, máquina) deberá bloquearse si éste no está siendo utilizado cumpliendo los tiempos de inactividad definidos.
- No está permitida la utilización del equipo de trabajo a través de la conexión a redes públicas, o de cualquier otra red que genere riesgo de vulnerabilidad al sistema de información.

Además, Ironchip Telco, S.L. cuenta con una **Política de Teletrabajo** que establece detalladamente los derechos y deberes de los empleados, así como las responsabilidades de la empresa en relación con el teletrabajo.

8.3. Desconexión Digital

Ironchip Telco, S.L. garantizará a cada uno de sus empleados el derecho a no conectarse a ningún dispositivo (Móvil, Ordenador, Tablet, etc.) de la empresa durante su periodo de vacaciones o periodos de descanso.

Por lo tanto, los empleados no deberán responder emails, interactuar con las plataformas de gestión documental, o atender llamadas, entre otras actividades, fuera de su horario laboral, salvo causa de fuerza mayor.

Los empleados estarán en su derecho de desconectar y apagar los dispositivos cuando termine su jornada laboral, respetando el tiempo de descanso de cada uno de ellos (Ley de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) de 2018, artículo 88).

Además, Ironchip Telco, S.L. cuenta con una **Política de Desconexión Digital** que establece detalladamente los derechos y deberes de los empleados, así como las responsabilidades de la empresa en relación con la desconexión digital.

Los empleados pueden consultar dicha política para obtener información más detallada sobre sus derechos, los procedimientos de implementación y las medidas de cumplimiento relacionadas con la desconexión digital.

8.4. Datos Personales

En los casos en los que se deba tratar datos personales, se debe dar oportuna respuesta al ejercicio de los derechos considerándose los documentos **A.1 A7.3.2 DO - Cómo Dar Respuesta a los Derechos RGPD**, **A.1 A7.3.3 DO - Cómo Ejercer los Derechos RGPD** y el **A.1 A7.3.4 FO - Formulario de Ejercicio de Derechos RGPD**, estableciéndose las garantías por la protección de los datos de carácter personal de las personas físicas, así como el aseguramiento del cumplimiento de acordado entre usuarios, clientes y proveedores según lo indicado por el Reglamento General de Protección de Datos.

9. Vigilancia y Control

Se debe gestionar continuamente la configuración de los componentes del sistema, manteniendo las reglas de: funcionalidad mínima y mínimo privilegio. Además, el sistema deberá reaccionar oportunamente ante incidentes y vulnerabilidades según su criticidad y políticas de atención establecidas, por lo que las configuraciones de seguridad solamente podrá editarse por el responsable de Sistemas o los empleados que se hayan autorizado para ello en determinado momento (luego deberán eliminarse atributos de configuraciones y accesos), tal y como lo indica la **A.1 5.1 PO - Política de Desarrollo Seguro**, **A.1 5.1.1 PR - Procedimiento de Despliegue**, **A.1 6.1.3 PR - Procedimiento de Calidad**, **A.1 9.1 RE - Detalle de Permisos en Sistemas** y **A.1 9.1 PO - Política de Control de Acceso Lógico.**

9.1. Software

Exclusivamente las personas autorizadas (administradoras) por el responsable de administración podrá instalar software. La persona usuaria deberá utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

Está terminantemente prohibido:

- Instalar copias ilegales de cualquier programa, incluidos los estandarizados.
- El uso de software no autorizado por el responsable de administración.
- Desinstalar cualquiera de los programas instalados por Ironchip Telco, S.L.

9.2. Sellos de Tiempo

La sincronización de los dispositivos se gestiona a través de Network Time Protocol (NTP), manteniendo trazabilidad temporal sobre los Logs y otros registros de información, garantizando así, la resistencia a los efectos de la latencia variable que pudiese acontecer. La retención de dichos Logs se gestiona hasta que la información protegida ya no sea requerida por el proceso respectivo.

9.3. Incidentes y Vulnerabilidades

Por ***incidente*** se entiende a cualquier suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información. Estos incidentes pueden incluir desde errores en el código del sistema (Bugs/Fixes), producto o servicio detectados, intentos de acceso no autorizado hasta ataques cibernéticos exitosos, pérdida de datos, interrupción del servicio, entre otros eventos que comprometan la integridad, confidencialidad o disponibilidad de la información.

Por ***vulnerabilidad*** se refiere a una debilidad de un activo o de un grupo de activos, o fallo en un sistema, aplicación, red o proceso, que puede ser explotada por una o más amenazas. Las vulnerabilidades pueden surgir de deficiencias en el diseño, implementación, configuración o mantenimiento de los sistemas, y pueden ser de naturaleza técnica, física, administrativa o procedimental. Además, las vulnerabilidades pueden existir en el software, la configuración de los sistemas, los procedimientos operativos o incluso en el comportamiento humano.

Cuando la persona usuaria detecte una posible vulnerabilidad, evento o incidente, deberá seguir lo indicado en el **A.1 16.2 PR Procedimiento de Ticketing** y en el **A.1 16.3 PR Procedimiento de Vulnerabilidades**, o notificar inmediatamente a través de security@ironchip.com.

9.4. Eliminación y Destrucción de Información

La eliminación y destrucción de información se realizará de acuerdo con la **A.1 8.3.2 PO - Política de Eliminación y Destrucción Segura** de Ironchip Telco, S.L.

10. Cumplimiento Normativo

Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por la normativa de propiedad intelectual.

La persona usuaria únicamente podrá utilizar material autorizado por Ironchip Telco, S.L. para el desarrollo de sus funciones.

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia de uso.

Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización por escrito de su persona titular o gestora de derechos.

Se garantizará el cumplimiento de la normativa vigente en materia de protección de datos de carácter personal en el tratamiento de los datos de personas físicas identificadas e identificables.

11. Revisión y Actualización

Esta política será revisada y actualizada periódicamente con espacios de tiempo no superiores a 1 año para garantizar su eficacia y cumplimiento con las normativas vigentes. Cualquier cambio será comunicado a las partes interesadas pertinentes.

Este documento es válido por 1 año a partir del 08 de agosto de 2024