IRONCHIP TELCO

www.ironchip.com

POLÍTICA DE SEGURIDAD

Índice

1. Objetivo

El propósito de esta política es establecer un marco integral para la gestión de la seguridad de la información, garantizando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de nuestros datos y sistemas. Este marco asegura que Iron Chip maneje de manera efectiva los riesgos asociados con la seguridad de la información.

2. Alcance

Esta política es aplicable a todos los empleados de IronChip y a terceros externos que accedan a nuestros sistemas y datos. Tanto el personal interno como el subcontratado son responsables de cumplir con esta política. El incumplimiento puede dar lugar a procesos sancionadores y disciplinarios según lo establecido. La política abarca todas las normativas de seguridad de la información de la empresa, garantizando la protección de nuestros activos digitales y la integridad de nuestros sistemas.

3. Documentos de Referencia

- A.2 8.0 DO - Metodología de Análisis y Gestión de Riesgos
- BOE.1 0 RE - Declaración de Aplicabilidad ENS
- A.1 6.1.1 MA - Manual de Organización y Funciones
- A.1 6.1.2 RE - Detalle de Personas y Plan de Capacitación
- Lista de obligaciones legales, normativas y contractuales
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

4. Normativa General

Este documento aplica a los siguientes activos:

- Datos personales de clientes y empleados
- Sistemas de información y redes de la empresa
- Servicios de pago ofrecidos
- Comunicaciones electrónicas y servicios digitales proporcionados

- Infraestructuras y tecnologías de telecomunicaciones utilizadas
- Cualquier otro activo relacionado con la actividad de la empresa de ciberseguridad

Estos activos están sujetos a:

- 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. Identidad Corporativa

5.1. 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.

5.2. 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.

6. Terminología básica sobre seguridad de la información

- **Confidencialidad**: Garantiza que la información esté disponible solo para personas o sistemas autorizados.
- **Integridad**: Asegura que la información sea modificada solo por personas o sistemas autorizados, manteniendo su exactitud y completitud.
- **Disponibilidad**: Permite que la información sea accesible y utilizable por personas autorizadas cuando sea necesario.
- **Autenticidad**: Verifica que la información proviene de la fuente anunciada, validando la identidad de usuarios y sistemas.
- **Trazabilidad**: Permite registrar todas las acciones realizadas sobre la información y los sistemas, facilitando la reconstrucción del historial de actividades.
- **Seguridad de la Información**: Preserva la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.
- **Sistema de Gestión de Seguridad de la Información (SGSI)**: Conjunto de procesos para planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

Principios, Compromisos y Objetivos

- **Confidencialidad**: Protección de la información contra el acceso no autorizado.
- **Integridad**: Asegurar la exactitud y completitud de la información.
- **Disponibilidad**: Garantizar el acceso autorizado a la información cuando sea necesario.

- **Trazabilidad y Autenticidad**: Registro de acciones sobre la información y verificación robusta de identidad.
- **Cumplimiento de Medidas de Seguridad**: Adherencia a las medidas de seguridad establecidas.
- **Cumplimiento de Requisitos Legales y Contractuales**: Observancia de requisitos legales, reglamentarios y contractuales en materia de seguridad de la información.
- **Mejora Continua**: Evaluación y mejora constante del rendimiento.
- **Liderazgo**: Modelo de comportamiento de los responsables de personas y procesos.
- **Participación de las Personas**: Fomentar la participación en la gestión de la seguridad de la información.
- **Relaciones Mutuamente Beneficiosas**: Establecimiento de relaciones basadas en la confianza con clientes y proveedores.

7. Organización de Seguridad

7.1. Comité de Seguridad de la Información y sus funciones

El Comité de Seguridad de la Información, compuesto por un grupo multidisciplinario, supervisa y dirige la política de seguridad de la información, promoviendo una cultura de seguridad en toda la organización. El comité está integrado por:

1. Jose Fernando Gomez, Responsable de Seguridad - Presidente del Comité
2. Miguel Martinez, Responsable del Sistema de Información y de los Servicios
3. Íñigo Maiso, Responsable de Sistemas TI
4. Urko San Miguel, Responsable de la información
5. Andoni Martín Reboredo, Persona de contacto POC
6. Leasba Consulting S.L., Delegado de Protección de Datos

Adicionalmente, el comité cuenta con el apoyo de:

- Nora Delgado - Apoyo de Protección de Datos Internos

- Jaime Venegas - Apoyo de Protección de Datos Externos y Secretario del Comité

El cometido principal de este comité es supervisar y dirigir la política de seguridad de la información, promoviendo una cultura de seguridad robusta en toda la organización. Entre sus funciones destacan:

- Desarrollar, aprobar y mantener las políticas de seguridad de la información alineadas con los principios y requisitos.
- Definir la estrategia global de seguridad de la información de la organización.
- Identificar y evaluar riesgos relacionados con la seguridad de la información.
- Asegurar la implementación de controles adecuados para mitigar los riesgos identificados.
- Revisar periódicamente los riesgos y actualizar las evaluaciones de riesgo según sea necesario.
- Garantizar el cumplimiento de todas las normativas y estándares aplicables.
- Supervisar la implementación de las medidas de seguridad exigidas por el ENS y otras normativas relevantes.
- Establecer procedimientos para la gestión de vulnerabilidades o incidentes de seguridad de la información.
- Supervisar la respuesta a vulnerabilidades o incidentes y garantizar que se tomen las acciones correctivas necesarias.
- Realizar revisiones post-vulnerabilidades o incidentes para identificar mejoras y prevenir recurrencias.
- Fomentar una cultura de seguridad dentro de la organización.
- Revisar la justificación y necesidad del cambio.
- Evaluar el posible beneficio o impacto en la seguridad de la información.
- Analizar los riesgos asociados y proponer medidas de mitigación.
- Verificar la viabilidad financiera según el presupuesto requerido.
- Realizar una evaluación de riesgos detallada para cambios significativos utilizando la matriz de A.2 8.2 RE - Análisis y Gestión de Riesgos.

- Organizar y supervisar programas de formación y concienciación en seguridad de la información para todo el personal.
- Realizar revisiones periódicas de las políticas, procedimientos y controles de seguridad.
- Identificar oportunidades de mejora y promover la implementación de mejoras continuas en la gestión de la seguridad de la información.
- Colaborar con otras áreas de la organización, como recursos humanos, tecnología y operaciones, para asegurar una gestión integral de la seguridad de la información.
- Coordinar con los responsables de la protección de datos y el cumplimiento normativo para asegurar la coherencia en las medidas de seguridad.
- Informar regularmente a la alta dirección sobre el estado de la seguridad de la información y el cumplimiento del ENS.
- Mantener una comunicación fluida con todas las partes interesadas internas y externas en materia de seguridad de la información.

7.1.1. Responsable de Seguridad y Presidente del Comité de Seguridad

El Responsable de Seguridad en una empresa desempeña un papel crucial en la implementación y mantenimiento de políticas de seguridad informática, asegurando la conformidad con las regulaciones y un manejo seguro de la información de los clientes. Este puesto se centra en garantizar que los sistemas y datos sean gestionados de manera adecuada, protegiendo la privacidad y la seguridad dentro de la organización. Además, el rol incluye funciones de Presidente del Comité de Seguridad, coordinando y documentando sus actividades y decisiones, y liderando las iniciativas para identificar y mitigar riesgos de seguridad.

- Crear y gestionar políticas y procedimientos de seguridad informática para proteger los activos tecnológicos de la empresa.
- Monitorizar los sistemas y redes de la empresa para detectar y responder a actividades sospechosas o no autorizadas.
- Liderar la respuesta a incidentes de seguridad, incluyendo la identificación, análisis y mitigación de amenazas.
- Realizar y supervisar auditorías internas y externas de seguridad para asegurar el cumplimiento con normativas y estándares de la industria.

- Asegurar que todos los sistemas y software estén actualizados con los últimos parches y medidas de seguridad.
- Organizar programas de formación y concienciación en seguridad para el personal de la empresa.
- Realizar evaluaciones de riesgos y desarrollar planes de mitigación para proteger los sistemas y datos de la empresa.
- Administrar y controlar los accesos a sistemas y datos sensibles, asegurando la integridad de los perfiles de usuario y los controles de acceso.
- Desarrollar y mantener planes de continuidad del negocio y recuperación ante desastres.
- Mantener registros detallados de incidentes, evaluaciones de riesgos, auditorías y preparar informes para la alta dirección.
- Investigar nuevas amenazas y vulnerabilidades, recomendando mejoras para fortalecer la seguridad de la empresa.
- Implementar y mantener herramientas de seguridad como firewalls, sistemas de detección de intrusos y antivirus.
- Coordinar y programar las reuniones del comité de seguridad, asegurando que todos los miembros sean notificados con anticipación.
- Preparar y distribuir agendas detalladas antes de cada reunión del comité
- Tomar notas precisas durante las reuniones, incluyendo decisiones tomadas, tareas asignadas y plazos acordados.
- Redactar y distribuir las actas de las reuniones del comité de seguridad en un plazo razonable después de cada sesión.
- Asegurar que las decisiones y recomendaciones del comité de seguridad se documenten y sigan adecuadamente.
- Coordinar la implementación de las recomendaciones y decisiones del comité de seguridad, trabajando en estrecha colaboración con los departamentos relevantes.
- Mantener un registro organizado y accesible de toda la documentación y correspondencia relacionada con el comité de seguridad.

- Asistir al presidente del comité de seguridad en la preparación de informes y presentaciones para la alta dirección.
- Monitorear el seguimiento de las acciones acordadas en las reuniones del comité y asegurar su cumplimiento.

7.1.2. Responsable del Sistema de Información

El Responsable del Sistema en una empresa desempeña un papel crucial en la implementación y cumplimiento de políticas de gestión de sistemas, asegurando que los sistemas y datos sean manejados de manera eficiente y conforme a las regulaciones vigentes. Esta posición se centra en mantener la integridad, disponibilidad y confidencialidad de los recursos tecnológicos, liderando y colaborando estrechamente con diferentes equipos para asegurar el cumplimiento normativo y la gestión adecuada de las operaciones y mantenimiento de los sistemas.

- Desarrollar y aplicar políticas y procedimientos para la gestión eficaz de los sistemas informáticos de la empresa.
- Asegurar que todos los sistemas y software estén actualizados y funcionando de manera óptima, incluyendo la instalación de actualizaciones y parches.
- Supervisar el rendimiento de los sistemas para detectar y solucionar problemas de manera proactiva.
- Liderar la respuesta y resolución de incidentes relacionados con el funcionamiento de los sistemas.
- Realizar auditorías internas de los sistemas para asegurar el cumplimiento con normativas y estándares de la industria.
- Implementar y mantener medidas de seguridad para proteger los sistemas contra accesos no autorizados y amenazas.
- Evaluar el rendimiento y la capacidad de los sistemas para asegurar que puedan satisfacer las necesidades de la empresa.
- Mantener una documentación detallada de la configuración, operación y mantenimiento de los sistemas.
- Coordinar con proveedores externos para la adquisición y mantenimiento de hardware y software.
- Proporcionar formación y soporte técnico a los usuarios de los sistemas de la empresa.

- Desarrollar y mantener planes de recuperación ante desastres y continuidad del negocio relacionados con los sistemas.
- Identificar oportunidades para mejorar la eficiencia y optimizar el uso de los recursos tecnológicos.
- Investigar y recomendar nuevas tecnologías y soluciones para mejorar la gestión y operación de los sistemas de la empresa.
- Trabajar con otros departamentos para asegurar que los sistemas soporten las necesidades operativas y estratégicas de la empresa.
- Planificar y ejecutar proyectos de implementación y mejora de sistemas dentro de los plazos y presupuestos establecidos.

7.1.3. Responsable del Servicio

El Responsable de los Servicios en una empresa desempeña un papel crucial en la implementación y cumplimiento de políticas de gestión de servicios, asegurando que los servicios ofrecidos sean manejados de manera eficiente y conforme a las regulaciones vigentes. Esta posición se centra en mantener la calidad, disponibilidad y confiabilidad de los servicios proporcionados, liderando y colaborando estrechamente con diferentes equipos para asegurar el cumplimiento normativo y la gestión adecuada de las operaciones y mantenimiento de los servicios.

- Desarrollar e implementar estrategias de gestión de servicios alineadas con los objetivos de la empresa.
- Evaluar y mejorar continuamente los procesos de entrega de servicios.
- Asegurar que los servicios cumplan con los estándares de calidad establecidos.
- Realizar evaluaciones periódicas para identificar áreas de mejora.
- Monitorear y mantener la disponibilidad de los servicios.
- Implementar medidas para minimizar las interrupciones y garantizar la continuidad del servicio.
- Asegurar que los servicios cumplan con todas las regulaciones y normativas vigentes.
- Mantenerse actualizado sobre cambios en las leyes y regulaciones que afectan la prestación de servicios.

- Coordinar la respuesta a incidentes y problemas que afectan los servicios.
- Desarrollar planes de acción para resolver problemas recurrentes y prevenir futuros incidentes.
- Gestionar las expectativas y la satisfacción del cliente, recogiendo feedback y ajustando los servicios según sea necesario.
- Trabajar estrechamente con otros equipos y departamentos para asegurar la entrega de servicios cohesivos y efectivos.
- Facilitar la comunicación y coordinación entre diferentes áreas de la empresa.
- Supervisar y gestionar las relaciones con los proveedores de servicios externos.
- Evaluar y seleccionar proveedores que cumplan con los estándares y requisitos de la empresa.
- Asegurar que el equipo de servicios esté adecuadamente capacitado y actualizado en las mejores prácticas y tecnologías relevantes.
- Fomentar el desarrollo profesional continuo dentro del equipo.
- Supervisar los presupuestos relacionados con la entrega de servicios.
- Optimizar los costos operativos sin comprometer la calidad del servicio.
- Identificar oportunidades para la innovación en la prestación de servicios.
- Implementar mejoras continuas en los procesos y tecnologías utilizadas en la gestión de servicios.

7.1.4. Responsable de Sistemas TI

El Responsable de Sistemas IT en una empresa desempeña un papel crucial en la implementación y cumplimiento de políticas de gestión de sistemas, asegurando que los sistemas informáticos sean manejados de manera eficiente y conforme a las regulaciones vigentes. Esta posición se centra en mantener la integridad, disponibilidad y confiabilidad de los sistemas tecnológicos, liderando y colaborando estrechamente con diferentes equipos para asegurar el cumplimiento normativo y la gestión adecuada de las operaciones y mantenimiento de los sistemas IT.

- Desarrollar y aplicar políticas y procedimientos para la gestión eficaz de los sistemas informáticos de la empresa.

- Asegurar que todos los sistemas y software estén actualizados y funcionando de manera óptima, incluyendo la instalación de actualizaciones y parches.
- Supervisar el rendimiento de los sistemas para detectar y solucionar problemas de manera proactiva.
- Liderar la respuesta y resolución de incidentes relacionados con el funcionamiento de los sistemas.
- Realizar auditorías internas de los sistemas para asegurar el cumplimiento con normativas y estándares de la industria.
- Implementar y mantener medidas de seguridad para proteger los sistemas contra accesos no autorizados y amenazas.
- Evaluar el rendimiento y la capacidad de los sistemas para asegurar que puedan satisfacer las necesidades de la empresa.
- Mantener una documentación detallada de la configuración, operación y mantenimiento de los sistemas.
- Coordinar con proveedores externos para la adquisición y mantenimiento hardware y software
- Proporcionar formación y soporte técnico a los usuarios de los sistemas de la empresa.
- Desarrollar y mantener planes de recuperación ante desastres y continuidad del negocio relacionados con los sistemas.
- Identificar oportunidades para mejorar la eficiencia y optimizar el uso de los recursos tecnológicos.
- Investigar y recomendar nuevas tecnologías y soluciones para mejorar la gestión y operación de los sistemas de la empresa.
- Trabajar con otros departamentos para asegurar que los sistemas soporten las necesidades operativas y estratégicas de la empresa.
- Planificar y ejecutar proyectos de implementación y mejora de sistemas dentro de los plazos y presupuestos establecidos.
- Identificar y evaluar amenazas y riesgos potenciales, y desarrollar estrategias para mitigarlos.

- Asegurar la correcta configuración y gestión de las redes informáticas para garantizar una comunicación eficiente y segura.
- Diseñar, implementar y gestionar soluciones TI que optimicen los procesos y operaciones de la empresa.
- Supervisar y coordinar al equipo de TI para asegurar que todas las tareas y proyectos se completen de manera eficiente.
- Monitorear y evaluar el desempeño de los sistemas IT para asegurar su alineación con los objetivos estratégicos de la empresa.

7.1.5. Responsable de la Información

El Responsable de la Información (information owner) tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

- El Responsable de la Información tiene la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información.
- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
- La determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares

7.1.6. Delegado de Protección de Datos (DPO)

El Delegado de Protección de Datos (DPO, por sus siglas en inglés) es una figura clave en la protección de datos personales dentro de una organización, tal como se establece en el Reglamento General de Protección de Datos (RGPD).

- Supervisar la conformidad de la organización con el RGPD y otras normativas de protección de datos aplicables.

- Asegurar que se implementen y mantengan políticas y procedimientos adecuados para la protección de datos personales.
- Proporcionar asesoramiento sobre las obligaciones relacionadas con la protección de datos.
- Formar y sensibilizar al personal de la organización sobre las prácticas de protección de datos.
- Supervisar y asesorar en la realización de Evaluaciones de Impacto sobre la Protección de Datos.
- Identificar y mitigar riesgos relacionados con el tratamiento de datos personales.
- Asistir en la gestión de brechas de seguridad y violaciones de datos personales.
- Coordinar la notificación a las autoridades de protección de datos y a los afectados, cuando sea necesario.
- Actuar como punto de contacto para la Autoridad de Protección de Datos.
- Cooperar con la autoridad en cualquier investigación o consulta.
- Monitorizar las actividades de procesamiento de datos para asegurar que se realicen conforme a las leyes aplicables.
- Asegurar que los contratos con terceros que manejan datos personales incluyan cláusulas adecuadas de protección de datos.

7.1.7. Apoyo de Protección de Datos Internos

El Apoyo de Protección de Datos Internos en una empresa desempeña un papel crucial en la implementación y cumplimiento de políticas de protección de datos, asegurando que se manejen de manera segura y conforme a las regulaciones vigentes. Este puesto se centra en mantener la confidencialidad y seguridad de la información interna, colaborando estrechamente con diferentes equipos para asegurar el cumplimiento normativo y la gestión adecuada de datos sensibles.

- Colaborar con diferentes departamentos para garantizar que los procesos internos cumplan con las regulaciones de privacidad, incluyendo la asignación de responsabilidades, la concienciación y formación del personal involucrado en las operaciones de tratamiento, y las correspondientes auditorías.
- Apoyar en la implementación y mantenimiento de políticas y procedimientos de protección de datos.

- Servir como punto de contacto interno para consultas relacionadas con la protección de datos.
- Identificar y evaluar las actividades de tratamiento de datos de la empresa.
- Capacitar al personal en temas de protección de datos y manejo seguro de la información.
- Contribuir en la preparación y gestión de evaluaciones de impacto de privacidad y evaluaciones de riesgos.
- Supervisar los procedimientos de gestión de datos y su cumplimiento en la empresa.
- Garantizar que respondemos a todas las consultas de los interesados dentro de los plazos legales (por ejemplo, eliminar sus datos de nuestras bases de datos).
- Redactar y actualizar guías detalladas sobre políticas de protección de datos
- Realizar auditorías periódicas y reportar hallazgos y recomendaciones para determinar si necesitamos modificar nuestros procedimientos para cumplir la normativa.
- Participar en la elaboración de planes de acción para la corrección de vulnerabilidades de seguridad.
- Colaborar con el equipo de IT para implementar controles de seguridad técnicos y medidas de mitigación

7.1.8. Apoyo de Protección de Datos Externos y Secretario del Comité de Seguridad

El Apoyo de Protección de Datos Externos en una empresa desempeña un papel crucial en la implementación y mantenimiento de políticas de protección de datos, asegurando la conformidad con las regulaciones y un manejo seguro de la información de los clientes. Este puesto se centra en garantizar que los datos sean gestionados de manera adecuada, protegiendo la privacidad y la seguridad dentro de la organización. Además, el rol incluye funciones de secretario del comité de seguridad, coordinando y documentando sus actividades y decisiones.

- Colaborar con equipos multidisciplinarios para asegurar que los procesos de manejo de datos cumplan con las regulaciones locales.
- Prestar asesoramiento sobre la evaluación de impacto relativa a la protección de datos cuando se solicite y supervisar su aplicación.
- Identificar y evaluar las actividades de tratamiento de datos de la empresa.

- Proporcionar ayuda para realizar evaluaciones de impacto de la protección de datos.
- Actuar como punto de contacto para clientes externos en temas relacionados con la protección de datos.
- Supervisar los procedimientos de gestión de datos y su cumplimiento en la empresa.
- Garantizar que respondemos a todas las consultas de los interesados dentro de los plazos legales (por ejemplo, eliminar sus datos de nuestras bases de datos).
- Monitorear y analizar incidentes de seguridad de datos, proponiendo medidas correctivas y preventivas.
- Redactar y actualizar guías detalladas sobre políticas de protección de datos.
- Desarrollar y conducir sesiones de capacitación sobre protección de datos y privacidad para el personal y los clientes.
- Realizar auditorías periódicas y reportar hallazgos y recomendaciones para determinar si necesitamos modificar nuestros procedimientos para cumplir la normativa.
- Mantenerse actualizado/a sobre cambios en las leyes y regulaciones de protección de datos y asegurar que la empresa esté en cumplimiento continuo.
- Asistir en la preparación y gestión de evaluaciones de impacto de privacidad y evaluaciones de riesgos.
- Colaborar con el equipo de IT para implementar y revisar controles de seguridad técnica.
- Elaborar informes y presentaciones sobre el estado de cumplimiento y seguridad de datos para la alta dirección.
- Coordinar y programar las reuniones del comité de seguridad, asegurando que todos los miembros sean notificados con anticipación.
- Preparar y distribuir agendas detalladas antes de cada reunión del comité.
- Tomar notas precisas durante las reuniones, incluyendo decisiones tomadas, tareas asignadas y plazos acordados.

- Redactar y distribuir las actas de las reuniones del comité de seguridad en un plazo razonable después de cada sesión.
- Asegurar que las decisiones y recomendaciones del comité de seguridad se documenten y sigan adecuadamente.
- Coordinar la implementación de las recomendaciones y decisiones del comité de seguridad, trabajando en estrecha colaboración con los departamentos relevantes.
- Mantener un registro organizado y accesible de toda la documentación y correspondencia relacionada con el comité de seguridad.
- Asistir al presidente del comité de seguridad en la preparación de informes y presentaciones para la alta dirección.
- Monitorear el seguimiento de las acciones acordadas en las reuniones del comité y asegurar su cumplimiento.

7.1.9. Representante de la Dirección

Tiene la máxima responsabilidad sobre la seguridad de la empresa, abarcando está, entre otros aspectos, la seguridad de la información, velando por el compromiso de la entidad con la seguridad y su adecuada implementación, gestión y mantenimiento.

Cada uno de estos roles es vital para la robustez y efectividad de nuestro sistema de seguridad, garantizando que Ironchip no solo cumple con las normativas y estándares, sino que también protege proactivamente sus activos más valiosos.

7.2. Mecanismos de coordinación

Para garantizar una gestión integral y eficaz de la seguridad de la información, se establecen mecanismos de coordinación específicos:

- **Reuniones periódicas**: El comité se reúne regularmente para revisar y discutir el estado de la seguridad de la información, las evaluaciones de riesgos, los incidentes y las medidas correctivas.
- **Documentación y seguimiento**: Se mantiene una documentación detallada de todas las actividades, decisiones y tareas del comité. Las actas de las reuniones se distribuyen y se asegura el seguimiento de las acciones acordadas.

- **Comunicación transversal**: Se promueve una comunicación fluida entre todos los departamentos y responsables, asegurando que las políticas y medidas de seguridad sean coherentes y se implementen de manera efectiva en toda la organización.

- **Evaluación continua**: Se realizan auditorías internas y externas, evaluaciones de riesgos y revisiones periódicas de las políticas y procedimientos de seguridad para identificar oportunidades de mejora y asegurar el cumplimiento continuo de las normativas aplicables.

Estos mecanismos aseguran que todas las áreas de la organización trabajen en conjunto para mantener un alto nivel de seguridad de la información, cumpliendo con las normativas y protegiendo los activos más valiosos de la empresa.

7.3. Procedimiento de designación de personas

El procedimiento de designación de personas establece las directrices para la asignación inicial y la renovación de los roles clave dentro del Comité de Seguridad de la Información, asegurando una estructura clara de responsabilidades y el cumplimiento de las normativas internas y externas. La designación inicial y cualquier renovación se realizan mediante una decisión de la Junta Directiva, con un acta detallada que especifica las personas designadas y la duración de sus mandatos. Esta acta es firmada por los miembros presentes de la Junta Directiva y por los individuos designados. Posteriormente, se distribuye una copia electrónica del acta a todos los interesados y se comunica internamente a los empleados pertinentes. Las actas firmadas se archivan de manera segura en el sistema de gestión documental de la empresa, manteniendo un registro actualizado de los roles asignados. Este procedimiento se revisará anualmente para asegurar su relevancia y efectividad, con actualizaciones según los cambios organizacionales o normativos. Para mayor información, se podrá revisar el documento **A.1 6.1.1 MA - Manual de Organización y Funciones.**

8. Formación y Desarrollo Profesional

En Ironchip, reconocemos que la formación y el desarrollo profesional son componentes fundamentales para el crecimiento tanto individual como organizacional. Por ello, nos comprometemos a proporcionar oportunidades de aprendizaje continuo y desarrollo de habilidades a nuestro personal, necesarias para mejorar sus conocimientos en ciberseguridad y otras áreas relevantes para nuestra empresa. Realizamos regularmente programas de formación y capacitación diseñados específicamente para el personal, abarcando desde las últimas tendencias y tecnologías en seguridad informática hasta habilidades blandas y gestión de proyectos.

Además, fomentamos y apoyamos la obtención de certificaciones reconocidas en la industria de la ciberseguridad, las cuales no solo validan el conocimiento de nuestros empleados, sino que también contribuyen al prestigio de Ironchip como empresa líder en seguridad informática.

Toda la formación y capacitación que ofrecemos está cuidadosamente planificada y documentada. Para mayor información, pueden revisar el documento **A.1.6.1.2 RE - Detalle de Personas y Plan de Capacitación**, que proporciona una visión general de las necesidades de formación de cada empleado y las acciones planificadas para abordarlas.

En Ironchip, creemos que invertir en el desarrollo de nuestro personal es clave para mantenernos a la vanguardia en un entorno empresarial cada vez más competitivo y dinámico.

9. Gestión de Riesgos

La gestión de riesgos es un componente fundamental para garantizar la seguridad de la información dentro de IronChip. Conforme al Esquema Nacional de Seguridad (ENS), el análisis de riesgos es la base para determinar las medidas de seguridad a adoptar, además de los mínimos establecidos por el ENS, según lo previsto en el Artículo 6 del ENS.

9.1. Compromiso del Organismo

IronChip se compromete a mantener una cultura de seguridad robusta, en la que todos los responsables de los sistemas de información realizan análisis de riesgos de forma regular y atienden a sus conclusiones. Este compromiso incluye la implementación de medidas correctivas y preventivas para mitigar los riesgos identificados.

9.2. Objetivos y Medición

Los objetivos generales para el sistema de gestión de seguridad de la información son los siguientes: crear una mejor imagen de mercado y reducir el daño ocasionado por potenciales incidentes; las metas están en línea con los objetivos comerciales, con la estrategia y los planes de negocio de la organización. El responsable de la oficina de seguridad de la información es el responsable de revisar estos objetivos generales del SGSI y de establecer nuevos.

Los objetivos para controles individuales de seguridad o grupos de controles son propuestos por el responsable de la oficina de seguridad de la información y son aprobados por comité de seguridad en la Declaración de aplicabilidad. Todos los objetivos deben ser revisados al menos una vez al año.

IronChip medirá el cumplimiento de todos los objetivos de acuerdo con **A.2 9.1 RE - KPIs de la Seguridad de la Información**. Además, complementará los análisis considerando los riesgos y la metodología aplicada para ello de acuerdo con el documento **A.2 8.0 DO - Metodología de Análisis y Gestión de Riesgos**. El responsable de la oficina de seguridad de la información es el responsable de definir el método para medir el cumplimiento de los objetivos; la medición se realizará al menos al menos una vez al año y el responsable de la oficina de seguridad de la información analizará y evaluará los resultados y los reportará al comité de seguridad como material para la revisión por parte de la Dirección.

9.3. Controles de seguridad de la información

El proceso de escoger los controles está definido en la metodología de evaluación y tratamiento de riesgos. Los controles seleccionados y su estado de implementación se detallan en la Declaración de aplicabilidad.

9.4. Registro de la Actividad

9.4.1. Generación de Registros de Auditoría

En Ironchip, todas las actividades relevantes del sistema serán registradas meticulosamente para garantizar la trazabilidad y seguridad de nuestros procesos. Los registros de auditoría incluirán la siguiente información mínima:

- **Identificador del Usuario o Entidad:** Cada evento será asociado con el identificador único del usuario o entidad que lo generó.
- **Fecha y Hora del Evento:** Se registrará la fecha y hora exacta de cada evento, utilizando un formato de tiempo estandarizado.
- **Información sobre el Evento:** Se detallará sobre qué información o recurso se realizó el evento.
- **Tipo de Evento:** Se especificará la naturaleza del evento (e.g., acceso, modificación, eliminación, intento de acceso fallido).
- **Resultado del Evento:** Se indicará si el evento fue exitoso o fallido.

9.4.2. Activación de Registros en los Servidores

Los registros de actividad estarán activados en todos los servidores que forman parte de nuestra infraestructura. Esta activación se realizará de forma continua y sin interrupciones para asegurar la integridad de los datos recolectados.

9.4.3. Refuerzos

Revisión de los Registros

De manera periódica, se realizarán revisiones informales de los registros de actividad. Estas revisiones serán llevadas a cabo por el equipo de seguridad, buscando identificar patrones anormales que puedan indicar posibles amenazas o vulnerabilidades.

Sincronización del Reloj del Sistema

El sistema contará con una referencia de tiempo confiable y precisa (por ejemplo, servidores NTP, sellado de tiempo, etc) para facilitar las funciones de registro de eventos y auditoría. La modificación de esta referencia de tiempo será una función de administración y se realizará utilizando mecanismos de autenticación e integridad para asegurar la exactitud y coherencia de los registros.

Retención de Registros

En la documentación de seguridad del sistema, se detallarán los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados. El tiempo de retención será de dos años.

Control de Acceso

Los registros de actividad y sus copias de seguridad sólo podrán ser accedidos, alterados o eliminados por personal debidamente autorizado. Este control de acceso se implementará utilizando mecanismos robustos de autenticación y autorización.

Revisión Automática y Correlación de Eventos

El sistema implementará herramientas avanzadas para analizar y revisar la actividad del sistema y la información de auditoría. Estas herramientas buscarán identificar comprometimientos de la seguridad, tanto posibles como reales. Además, se dispondrá de un sistema automático para la recolección de registros, correlación de eventos y respuesta automática ante incidentes detectados.

9.5. Responsabilidades

Las responsabilidades para el SGSI son las siguientes:

- **Comité de Seguridad:** Asegura la implementación y mantenimiento del SGSI, define la comunicación de información de seguridad.
- **Responsable de la Oficina de Seguridad de la Información:** Coordina operativamente el SGSI, gestiona informes de incidentes y debilidades.
- **Alta Dirección:** Revisa el SGSI anualmente y tras cambios significativos.
- **Departamento de Recursos Humanos:** Implementa programas de capacitación y concienciación en seguridad de la información en colaboración con el responsable de la Oficina de Seguridad de la Información. Es responsable de adoptar e implementar el Plan de Capacitación y Concienciación para todos los involucrados en la gestión de la seguridad de la información.
- **Propietarios de Activos:** Protegen la integridad, disponibilidad y confidencialidad de los activos bajo su control.

Para obtener una visión más detallada de los roles y responsabilidades, consulte el documento **A.1 6.1.1 MA - Manual de Organización y Funciones.**

9.6. Comunicación de la Política

El departamento de Recursos Humanos es responsable de asegurar que todos los empleados de IronChip, así como los participantes externos relevantes, estén debidamente informados y familiarizados con esta Política. Además, la política, junto con las normativas, procedimientos e instrucciones relacionadas, se pondrán a disposición de todos los empleados y partes interesadas de manera accesible y apropiada. La comunicación efectiva de estos documentos es esencial para garantizar su comprensión y cumplimiento en toda la organización.

10. Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la información, será resuelto por la Dirección de IronChip y prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

11. Obligaciones del personal

Todo el personal con responsabilidad en el uso, operación, o administración de sistemas de tecnologías de la información y las comunicaciones tienen la obligación de conocer y cumplir esta **A.1 5.1 PO - Política de Seguridad** y la **A.1 5 PO - Normativa de Seguridad de la Información y Protección de Datos**, independientemente del tipo de relación jurídica que les vincule con las empresas.

Todas las personas recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo, para mayor información acceder a **A.1 6.1.2 RE - Detalle de Personas y Plan de Capacitación.**

La Política de Seguridad estará accesible para todo el personal que preste sus servicios en los órganos y entidades a que se refiere el punto relativo al 'Alcance'.

Con el objetivo de fomentar la 'Cultura de la seguridad', el Comité de Seguridad de la Información promoverá un programa de concienciación continúa para formar a todo el personal.

El incumplimiento de la **A.1 5.1 PO - Política de Seguridad** y su **A.1 5.3 PO - Política de Desarrollo Seguro** dará lugar al establecimiento de medidas preventivas y correctivas encaminadas a salvaguardar y proteger las redes y sistemas de información, sin perjuicio de la correspondiente exigencia de responsabilidad disciplinaria, aplicando lo señalado en **C 6 DO - Sistema Disciplinario y C 6.1 PR - Procedimiento Sancionador.**

12. Validez y gestión de documentos

Esta política se revisa al menos anualmente y siempre que se considere necesario, en función de cambios en los riesgos de seguridad de la información. El responsable de este documento es el Responsable de la Oficina de Seguridad de la Información, quien debe verificar y actualizar el documento al menos una vez al año.

Los criterios para evaluar la efectividad y adecuación de este documento incluyen:

- La cantidad de empleados y participantes externos que desempeñan funciones en el SGSI pero que no están familiarizados con el documento.
- Incumplimiento del SGSI con leyes, normas, obligaciones contractuales y documentos internos.
- Ineficacia en la implementación y mantenimiento del SGSI.
- Ambigüedad en las responsabilidades para la implementación del SGSI.

La Dirección de la organización se compromete a cumplir con la legislación aplicable en protección de información personal y con los términos contractuales acordados con socios, subcontratistas y terceros (clientes, proveedores, etc.), y a asignar claramente las responsabilidades correspondientes.

Este documento es válido por 1 año a partir del 28 de mayo del 2025.