racks & containers

Política de seguridad

Gerencia:

23 de marzo de 2025

Contenido

Historial de versiones

Fecha - versión	Responsable de revisión	Cambios
27/03/2025 – Rev.0.1	dooingIT	Elaboración de documento

1. Política de Seguridad de la Información

1.1. Objeto

El propósito de este documento es definir la política de seguridad global, estableciendo directrices y medidas específicas para el uso de los sistemas de información y la protección de activos.

En este documento se define, además, el alcance del SGSI (Sistema de Gestión de Seguridad de la Información)

2. Responsabilidades

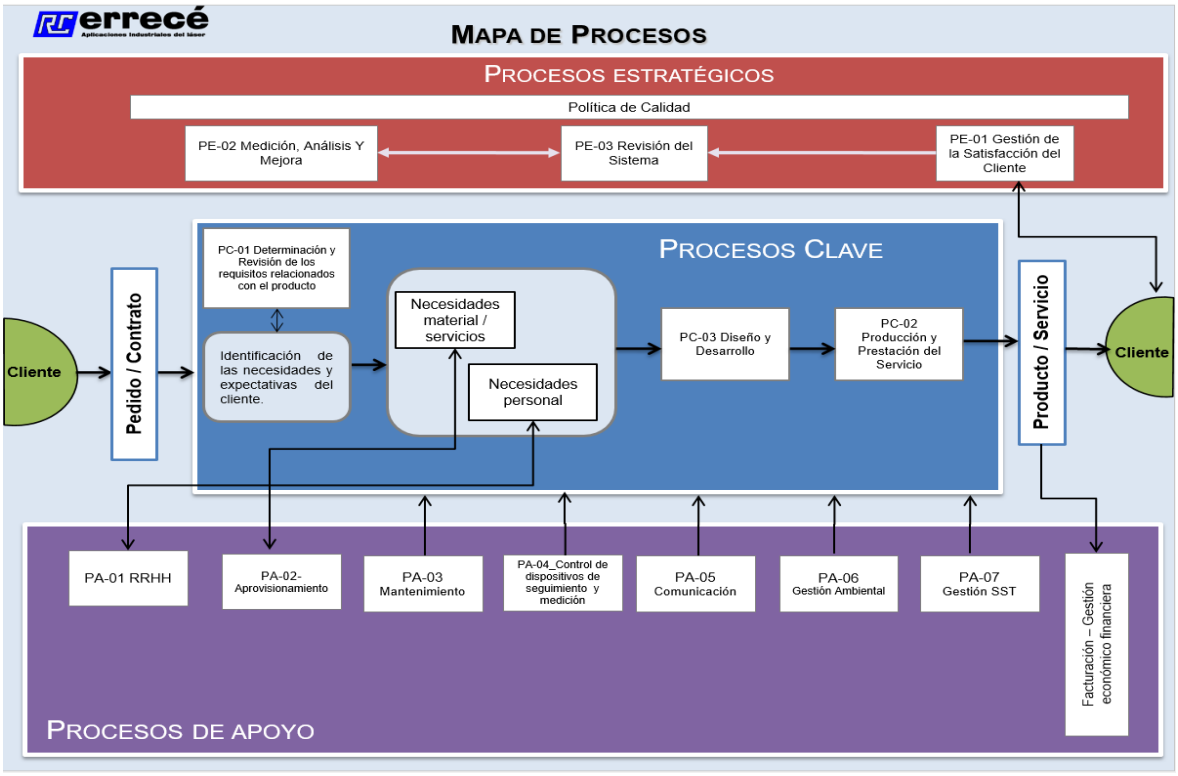
Responsable	Tarea
Dirección	▪ Definir los objetivos de la política de seguridad global ▪ Aprobar el documento de política de seguridad global
RSI	▪ Diseñar y aprobar el documento de política de seguridad global ▪ Implementar y monitorear el documento aprobado ▪ Revisar el documento como mínimo una vez al año ▪ Velar por el cumplimiento de la política ▪ Difundir el documento en ERRECÉ
Responsable de Sistemas	▪ Conocer el documento de política de seguridad global ▪ Actuar de acuerdo con las instrucciones contenidas en el documento ▪ Identificar cualquier riesgo en los procesos de TI y proponer posibles acciones de mitigación de riesgos
Empleados	▪ Conocer y cumplir las políticas y normas de uso de los equipos y sistemas de ERRECÉ definidos en la política de seguridad global

3. Ámbito y alcance de aplicación

Las medidas y directrices establecidas en este documento se aplican a los sistemas de información de ERRECÉ y a todos aquellos que utilizan estos sistemas para interactuar con la información de la organización.

Para comprender mejor el alcance, se presenta a continuación el diagrama de procesos de ERRECÉ:

Imagen. Diagrama de procesos ERRECÉ.



De este modo, el alcance del SGSI se limita a los procesos clave PC-01 Determinación y revisión de los requisitos relacionados con el producto, PC-03 Diseño y Desarrollo y PC-02 Producción y Prestación del Servicio, tal y como se muestra en la anterior imagen. Además, se incluye parte de aquellos procesos estratégicos y de apoyo que se ven involucrados en los procesos clave.

4. Desarrollo

4.1. Equipos informáticos, comunicaciones y software

Con el fin de garantizar un uso adecuado y eficiente de los recursos tecnológicos, se establecen las siguientes directrices:

- Todos los dispositivos, sistemas y aplicaciones que se entregan al personal estarán previamente configurados para su correcto funcionamiento.
- El equipamiento tecnológico propiedad de ERRECÉ se asigna exclusivamente para el desempeño de funciones laborales, quedando restringido su uso a dicho propósito.
- Todo software utilizado, ya sea preinstalado o añadido posteriormente, deberá contar con su correspondiente licencia de uso y/o mantenimiento, emitida por el proveedor oficial.
- No está permitida la modificación, manipulación o intervención técnica sobre el hardware o software de los dispositivos sin la autorización expresa del Responsable del Sistema Responsable de Seguridad.
- El traslado de equipos fuera del entorno laboral (como tabletas, dispositivos USB, etc.) requerirá autorización previa por parte del responsable de sistemas, la cual deberá ser tramitada por correo electrónico. En el caso de ordenadores portátiles y dispositivos móviles, se entenderá que la autorización ha sido concedida con la entrega del equipo al usuario.

4.2. Escritorios limpios y área de trabajo despejada

Con el objetivo de preservar la confidencialidad de la información y mantener un entorno de trabajo seguro y profesional, todo el personal de ERRECÉ deberá cumplir con las siguientes prácticas:

- Es obligatorio bloquear la sesión del equipo informático cada vez que el usuario se ausente de su puesto, aunque sea por un breve periodo de tiempo.
- El uso de los dispositivos asignados debe limitarse exclusivamente a tareas relacionadas con la actividad profesional. Queda expresamente prohibido acceder a contenidos personales o que puedan infringir derechos de propiedad intelectual o industrial.
- Toda documentación en soporte físico que contenga información sensible o interna deberá ser eliminada mediante métodos seguros, como las destructoras de papel disponibles en algunos despachos.

Estas medidas son especialmente relevantes en áreas como la oficina técnica, administración o producción, donde se maneja información técnica, planos y documentación de clientes.

4.3. Uso seguro del correo electrónico

Las comunicaciones electrónicas dentro de ERRECÉ deben realizarse exclusivamente a través de las plataformas autorizadas por la organización, como Outlook, las cuales cuentan con mecanismos de cifrado para proteger la integridad y confidencialidad de los mensajes.

Para asegurar un uso adecuado del correo electrónico, se establecen las siguientes normas:

- Las cuentas de correo electrónico asignadas a los empleados son propiedad de ERRECÉ y deben utilizarse únicamente para fines profesionales.
- La organización se reserva el derecho de auditar y supervisar el uso del correo electrónico corporativo, incluyendo el acceso a los contenidos, con el fin de garantizar el cumplimiento de las políticas internas y la normativa vigente.
- Cada usuario recibirá una cuenta de correo con credenciales personales e intransferibles. Es obligatorio cambiar la contraseña en el primer acceso, siguiendo las directrices de seguridad establecidas.

- Como medida preventiva, se recomienda no abrir archivos adjuntos ni hacer clic en enlaces incluidos en correos electrónicos de origen desconocido o sospechoso. Los mensajes procedentes del exterior estarán debidamente identificados para facilitar su reconocimiento.

Estas prácticas son esenciales para prevenir ataques de phishing, fugas de información y otros riesgos identificados en el entorno digital de ERRECÉ.

4.4. Actualización y mantenimiento de sistemas operativos y herramientas

El Responsable de Sistemas de ERRECÉ es el encargado de garantizar que todos los equipos informáticos y utilidades tecnológicas se mantengan actualizados, con el fin de reducir la exposición a vulnerabilidades conocidas.

Para ello:

- Se realiza un seguimiento continuo de las actualizaciones críticas mediante sistemas de alerta y monitorización.
- Se aplican parches de seguridad y actualizaciones de software de forma planificada, priorizando los sistemas más sensibles, como servidores, equipos de producción y dispositivos con acceso remoto.
- Se verifica que todos los sistemas operativos utilizados en la organización cuenten con soporte oficial y estén alineados con las recomendaciones del fabricante.
- En caso de detectar versiones obsoletas o sin soporte, se procede a su sustitución o actualización conforme al plan de bastionado definido.

Estas acciones forman parte de la estrategia de ciberseguridad de ERRECÉ y son fundamentales para garantizar la continuidad operativa y el cumplimiento normativo.

4.5. Acceso a la red

El acceso a la infraestructura tecnológica de ERRECÉ está restringido a usuarios previamente autorizados. No se permite la conexión a la red corporativa, a los sistemas, a las aplicaciones ni al acceso a la información sin la correspondiente validación y asignación de permisos conforme a las funciones del usuario.

Con el fin de garantizar un acceso controlado y minimizar los riesgos de seguridad, la organización dispone de redes diferenciadas según su uso:

Red corporativa principal (192.168.1.0/24), utilizada actualmente para los sistemas productivos, los servicios centrales y los puestos de trabajo.

Red Wi-Fi de invitados (192.168.155.0/24), destinada a personal externo que requiera conectividad temporal a Internet.

La red Wi-Fi de invitados se encuentra segregada de la red corporativa y no permite el acceso a los sistemas internos ni a la información sensible, incluyendo el controlador de dominio, los sistemas de almacenamiento o las aplicaciones de gestión.

Adicionalmente, el acceso remoto a la red corporativa se realiza exclusivamente mediante VPN gestionada en el firewall perimetral, aplicándose controles de autenticación, autorización y registro de accesos.

4.6. Uso aceptable de los recursos

ERRECÉ promueve un uso profesional, eficiente y seguro de los recursos tecnológicos, asegurando que su capacidad y disponibilidad estén alineadas con las necesidades operativas de la organización. Para ello, se establecen las siguientes normas de uso:

- Queda prohibido el uso personal de los recursos informáticos, de red o de comunicación proporcionados por la empresa.
- Todo dispositivo entregado al personal (ordenadores, móviles, tablets, etc.) deberá ser devuelto en el momento de la finalización de la relación laboral.
- El número de teléfono corporativo no podrá utilizarse para fines personales, salvo autorización expresa.
- El acceso a la información de la organización debe limitarse exclusivamente a fines laborales, incluso si el empleado tiene permisos para visualizarla.
- No está permitido el uso de dispositivos de almacenamiento externo (como USB, discos duros o tarjetas de memoria) sin la autorización previa del Responsable de Sistemas.
- El almacenamiento de información en servicios en la nube queda restringido, y solo podrá realizarse con la aprobación del Responsable de Sistemas, garantizando que se cumplan los requisitos de seguridad y trazabilidad.
- Toda comunicación realizada a través de los sistemas y dispositivos de la organización se considera propiedad de ERRECÉ y podrá ser auditada en el marco de las políticas de seguridad y cumplimiento.
- El acceso a internet debe realizarse de forma responsable y exclusivamente para fines relacionados con la actividad profesional. El uso personal está expresamente prohibido.
- La organización pone a disposición del personal herramientas corporativas para el almacenamiento de información, las cuales cuentan con sistemas de respaldo automático y control de versiones.

4.7. Gestión de accesos y seguridad física del entorno

Para garantizar un entorno seguro y proteger los activos de información y producción, ERRECÉ mantiene medidas de seguridad física adecuadas en todas sus ubicaciones, tanto en las oficinas centrales de Aradas como en las instalaciones del Polígono do Tambre.

Estas medidas tienen como objetivo:

- Prevenir accesos no autorizados a zonas sensibles, como el CPD, oficinas técnicas, áreas de producción o almacenes.
- Evitar interferencias externas que puedan comprometer la continuidad operativa o la integridad de los sistemas.

- Asegurar que únicamente el personal autorizado pueda acceder a las instalaciones, mediante mecanismos de control como llaves, tarjetas de acceso, cerraduras electrónicas o sistemas de videovigilancia.

El acceso a determinadas zonas está restringido según el perfil del empleado o proveedor, y será supervisado por el Responsable de Seguridad o el Responsable de Sistemas, según corresponda.

4.8. BYOD

Debido a las necesidades de negocio, en ERRECÉ se permite el uso de forma voluntaria de dispositivos móviles personales para el uso corporativo. Es por ello por lo que se siguen una serie de directrices recogidas en esta política, que el usuario comprende y firma mediante un documento anexo al contrato.

4.8.1. Requisitos de seguridad

- Correo corporativo: El acceso al correo debe realizarse exclusivamente a través de aplicaciones autorizadas por ERRECÉ.
- Aplicación de autenticación: En caso de necesitar una aplicación de autenticación, el trabajador debe instalar y configurar la aplicación para el doble factor de autenticación autorizada por ERRECÉ.
- Bloqueo del dispositivo: El equipo debe estar protegido, preferiblemente de forma biométrica con huella dactilar o reconocimiento facial y con PIN numérico o patrón.
- Actualizaciones: El trabajador es responsable de mantener el sistema operativo actualizado.
- Aplicaciones no autorizadas: No se permite el uso de aplicaciones no aprobadas para gestionar datos corporativos. Solo se pueden instalar las aplicaciones que se encuentran preautorizadas en el documento Listado de software preaprobado.
- Almacenamiento: El trabajador debe evitar la descarga en el propio dispositivo de documentación corporativa. En caso de hacerlo, debe eliminarla del dispositivo una vez terminado su fin.
- Eliminación de datos: La empresa se reserva el derecho de eliminar remotamente cualquier información corporativa almacenada en el dispositivo personal del trabajador en caso de salida de la organización, pérdida o amenaza de seguridad.

4.8.2. Responsabilidades del trabajador

- Notificar inmediatamente la pérdida o robo del dispositivo a la empresa para que puedan tomarse las medidas necesarias.
- Instalar y configurar las aplicaciones corporativas necesarias según las directrices de ERRECÉ.
- Mantener el teléfono móvil protegido mediante bloqueo biométrico, PIN o patrón.
- Cifrar el dispositivo
- Mantener el sistema operativo en su última versión estable
- Evitar el acceso compartido de su teléfono móvil mientras esté configurado para uso corporativo.
- Garantizar el correcto uso del dispositivo conforme a las políticas de privacidad y confidencialidad de la empresa.

- Evitar la conexión a redes wifi públicas como hoteles, aeropuertos o restaurantes. En caso de hacerlo, la conexión será a través de la VPN.
- Evitar el almacenamiento interno de la documentación corporativa, utilizando las soluciones cloud proporcionadas por la empresa.

4.9. Identificación y autenticación de usuarios

Con el fin de garantizar un acceso seguro y controlado a los sistemas de información, ERRECÉ establece las siguientes directrices para la identificación y autenticación de usuarios:

- A cada usuario se le asigna un identificador único (nombre de usuario) y una contraseña personal e intransferible. Esta contraseña deberá ser modificada obligatoriamente en el primer inicio de sesión.
- Cada cuenta está vinculada a un perfil de usuario, el cual define los permisos, privilegios y roles necesarios para el desempeño de sus funciones, en base al principio de mínimo privilegio.
- Las contraseñas deben ser definidas por el propio usuario siguiendo los criterios establecidos por ERRECÉ, los cuales incluyen requisitos de complejidad, longitud y caducidad periódica.
- Siempre que sea técnicamente viable, el acceso a los sistemas deberá realizarse mediante canales seguros (por ejemplo, conexiones cifradas o VPN).
- En las aplicaciones críticas o con acceso a información sensible, se implementará autenticación multifactor (2FA), combinando credenciales con un segundo factor como token, aplicación móvil o código temporal.

4.10. Filtrado de contenido

ERRECÉ dispone de mecanismos de defensa perimetral y de endpoint para prevenir la entrada y propagación de software malicioso o contenido no autorizado en su red corporativa.

Para ello:

- Se utilizan soluciones antivirus actualizadas en todos los equipos, con capacidad de detección en tiempo real y análisis.
- La red está protegida mediante un firewall que filtra el tráfico entrante y saliente, bloqueando accesos no autorizados y contenidos potencialmente peligrosos.
- Estas herramientas permiten identificar, aislar y eliminar amenazas como malware, spyware, ransomware o intentos de intrusión, contribuyendo a la protección de los sistemas y la información crítica de la organización.

4.11. Gestión de la información

Con el objetivo de salvaguardar la propiedad intelectual, los datos sensibles y la información estratégica de ERRECÉ, se aplican las siguientes medidas fundamentales:

- **Clasificación de la información:** Toda la información gestionada por la organización debe estar correctamente clasificada según su nivel de confidencialidad (confidencial, interna o pública), conforme al inventario de activos y a los criterios definidos en el SGSI.

- **Compromiso de confidencialidad:** Todo el personal, así como colaboradores externos con acceso a información de la empresa, deben firmar un acuerdo de confidencialidad que garantice el uso responsable y la no divulgación de datos protegidos.

- **Control de accesos y trazabilidad:** Se realiza un seguimiento continuo de los accesos a la información, aplicando controles técnicos y organizativos que aseguran que solo las personas autorizadas puedan acceder, modificar o transmitir datos según su perfil y nivel de privilegio.

4.11.1. Clasificación de la información

- **Confidencial**: Información a la que solo pueden tener acceso ciertas personas o departamentos dentro de la organización. Si un tercero accede a él, puede tener consecuencias negativas para la organización.
    - Ejemplos: Información estratégica, información de clientes, datos personales, etc.
- **Interna**: Información de uso interno a la que solo puede acceder el personal de la organización. Si un tercero accede a él, puede tener consecuencias para la organización.
    - Ejemplos: Políticas de la empresa, normas y procedimientos internos del área, etc.
- **Pública**: Información sin restricciones de acceso, sin consecuencias para la organización en caso de acceso por parte de terceros.
    - Ejemplos: Información estratégica, información de clientes, datos personales, etc.

4.11.2. Transmisión de información según su clasificación:

La transmisión de información dentro y fuera de ERRECÉ debe realizarse de forma segura y conforme a su nivel de clasificación, con el fin de evitar accesos no autorizados o fugas de datos. Para ello, se establecen las siguientes directrices:

- **Información confidencial:** Su transmisión, ya sea por medios físicos o digitales, requiere la aprobación expresa del responsable del activo. Además, debe garantizarse que el canal utilizado esté cifrado y que el destinatario esté debidamente autorizado.
- **Información interna:** Solo podrá compartirse a través de los canales corporativos habilitados por ERRECÉ, como el correo electrónico, la red interna o las plataformas de colaboración autorizadas. No se permite su envío por medios personales o no controlados.
- **Información pública:** No requiere medidas especiales para su transmisión, ya que está destinada a ser accesible por cualquier persona, tanto interna como externa a la organización.

4.12. Cifrado de dispositivos

- Todo equipo que pueda contener información clasificada como confidencial o interna y que esté destinado a salir de las instalaciones de ERRECÉ, ya sea de forma habitual o puntual, deberá contar con mecanismos de cifrado que garanticen la protección de los datos almacenados frente a accesos no autorizados en caso de pérdida, robo o acceso indebido.

  Además:

    - El acceso a estos dispositivos deberá estar protegido mediante credenciales personales (usuario y contraseña, PIN o mecanismo equivalente), conforme a las políticas de control de acceso establecidas por la organización.

- Esta medida aplica especialmente a ordenadores portátiles, teléfonos móviles corporativos, tablets y cualquier otro dispositivo susceptible de pérdida o robo que pueda almacenar o acceder a información corporativa.
- El cifrado podrá ser proporcionado por los mecanismos nativos del sistema operativo, siempre que estos garanticen un nivel adecuado de protección de la información.
- Los dispositivos deberán contar con bloqueo automático tras un periodo de inactividad, evitando accesos no autorizados en caso de descuido del usuario.
- El cifrado y las medidas de protección asociadas deberán ser gestionadas, verificadas y documentadas por el Responsable de Sistemas, quien se encargará de asegurar su correcta implementación, mantenimiento y revisión periódica.
- Cualquier excepción a esta norma deberá ser debidamente justificada, documentada y aprobada por el Responsable de Sistemas, aplicando medidas compensatorias cuando proceda.

4.13. Mantenimiento de Equipos y Archivos

El mantenimiento de los equipos informáticos y la correcta gestión de los archivos son fundamentales para garantizar la continuidad operativa y la seguridad de la información en ERRECÉ. En este sentido, se establecen las siguientes directrices:

- El personal del área de sistemas, previa autorización de la dirección o del departamento correspondiente, podrá formatear, reasignar o reconfigurar cualquier equipo con el fin de optimizar su uso o asignarlo a otro usuario.
- Es responsabilidad de cada usuario almacenar su documentación en las ubicaciones habilitadas por la organización, como las unidades de red o plataformas corporativas con respaldo automático. En caso de pérdida de información por no seguir estas indicaciones, ERRECÉ no asumirá responsabilidad alguna.
- Cada empleado es responsable del buen uso y conservación del equipo que le ha sido asignado. Ante cualquier incidencia técnica, mal funcionamiento o daño, deberá comunicarlo de inmediato al Responsable de Sistemas para su evaluación y resolución.

4.14. Contraseñas

En cuanto a la elección de la **contraseña,** se recomienda:

- Siempre que el sistema no lo exija, debe contener al menos 8 caracteres alfabéticos y numéricos, no repetidos consecutivamente.
- Evite crear contraseñas que contengan datos que sean muy fáciles de adivinar (nombre de la organización, nombre de usuario, nombre o apellido, fecha de nacimiento, cargo, etc.)

En cuanto a la protección que se debe dar a las contraseñas, se deben cumplir los siguientes requisitos:

- Las contraseñas son personales e intransferibles, y se debe garantizar su seguridad para que solo sean conocidas por su propietario.
- Las contraseñas no deben registrarse por escrito ni almacenarse sin cifrar.
- Se debe guardar la contraseña en un gestor de contraseñas.

- Cuando se utiliza una cuenta por primera vez, se debe cambiar la contraseña inicial. Se aplicarán todos los ajustes técnicos posibles para que el sistema obligue al usuario a cambiar su contraseña la primera vez que inicie sesión. Las contraseñas iniciales se enviarán por correo electrónico al responsable de sistemas para que el usuario pueda iniciar sesión en el momento del registro.
- Se debe evitar habilitar la opción "Recordar contraseña" a menos que las necesidades comerciales lo requieran.
- Si un usuario sospecha que una contraseña puede haberse visto comprometida, el cambio de contraseña debe realizarse en todas las cuentas en las que utilice.
- La contraseña se cambiará cada 3 meses.

4.15. Gestión de incidentes e incidencias

Cualquier empleado de ERRECÉ que detecte o sospeche de un incidente relacionado con la seguridad, ya sea de carácter físico, lógico (software o sistemas), o vinculado a servicios de soporte, deberá comunicarlo de forma inmediata al Departamento de IT.

La notificación debe realizarse preferentemente a través de los siguientes canales:

- Correo electrónico corporativo dirigido al área de IT.
- Llamada telefónica.

Una vez recibido el aviso, el equipo de sistemas evaluará la situación, aplicará las medidas correctivas necesarias y registrará el incidente conforme al Procedimiento de Gestión de Incidentes de Seguridad definido en ERRECÉ.

Este proceso garantiza una respuesta rápida, documentada y eficaz ante cualquier amenaza que pueda comprometer la disponibilidad, integridad o confidencialidad de los activos de la organización.

4.16. Continuidad del negocio

En caso de que se produzca una situación que pueda interrumpir o comprometer los procesos clave de ERRECÉ, ya sea por causas técnicas, operativas o externas, se activarán las medidas recogidas en el Plan de Continuidad de Negocio.

Este plan contempla:

- La identificación de los procesos críticos.
- La asignación de responsabilidades específicas a las áreas implicadas.
- Procedimientos de actuación para minimizar el impacto de la interrupción y restablecer la operativa en el menor tiempo posible.

Las medidas de contingencia se comunican previamente a los responsables de cada área, quienes deben conocer y aplicar los protocolos establecidos. Este enfoque permite a ERRECÉ mantener su capacidad de respuesta ante incidentes graves y asegurar la continuidad de los servicios esenciales para sus clientes.

4.17. Conformidad

ERRECÉ, sus empleados y empresas colaboradoras, asumen la responsabilidad de tratar los datos personales de forma ética, segura y conforme a la normativa vigente, en especial el Reglamento General de Protección de Datos (RGPD) y la legislación nacional aplicable.

Para ello:

- Se aplican medidas técnicas y organizativas que garantizan un nivel adecuado de protección de los datos personales tratados en el marco de la actividad empresarial.
- Todos los usuarios deben cumplir con las políticas internas de seguridad y protección de datos, actuando siempre dentro del marco legal y de los principios establecidos por la organización.
- Cualquier incumplimiento, duda o sospecha relacionada con el tratamiento de datos o con el uso indebido de la información debe ser comunicado a los responsables correspondientes a través de los canales establecidos.

Además, ERRECÉ pone a disposición de empleados, colaboradores y terceros un canal de comunicación confidencial, accesible para reportar de buena fe cualquier no conformidad, queja o sugerencia relacionada con la seguridad de la información, la protección de datos o el cumplimiento normativo. Este canal garantiza la confidencialidad del informante y permite a la organización actuar con diligencia ante cualquier posible desviación.

4.18. Medidas Disciplinarias

El incumplimiento de las políticas y procedimientos de seguridad de la información establecidos por ERRECÉ puede comprometer la integridad, confidencialidad o disponibilidad de los activos de información de la organización. Por ello, se contemplan medidas correctoras y disciplinarias proporcionales a la gravedad de la infracción.

El procedimiento a seguir se ajusta a lo establecido en el convenio colectivo aplicable y en las políticas internas de recursos humanos, e incluye las siguientes fases:

- Información inicial: Al inicio de la relación laboral, se comunican de forma clara las normas, expectativas y responsabilidades en materia de seguridad de la información.
- Investigación del incidente: Ante una posible infracción, se llevará a cabo una investigación detallada y documentada. La reincidencia de faltas leves puede ser considerada como una falta moderada o grave.
- Evaluación y comunicación: Se valorará la gravedad del incumplimiento y se informará al empleado de:
    - Qué conducta ha sido inapropiada y por qué.
    - Qué cambios se esperan en su comportamiento.
    - Qué norma disciplinaria se ha infringido.
    - Qué consecuencias podrían derivarse en caso de repetición o agravamiento.

En función de la naturaleza y reiteración de la infracción, podrán aplicarse las siguientes medidas:

- Advertencia verbal.
- Advertencia escrita.

- Suspensión temporal de empleo.
- Extinción del contrato laboral.

En todos los casos, ERRECÉ priorizará la formación y la concienciación como primera medida correctora, fomentando una cultura de seguridad basada en la responsabilidad compartida.