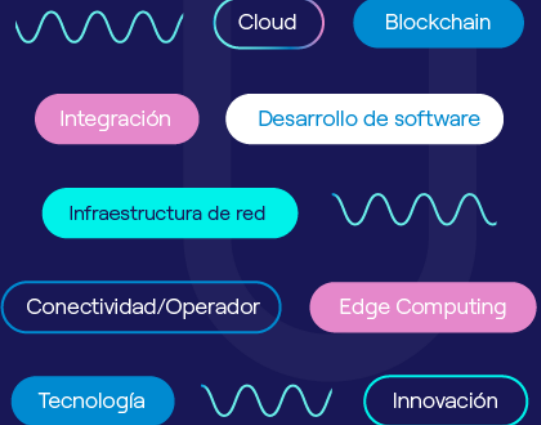


# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

TRC

Pasión por la **tecnología.**



## DATOS DE CONTROL

CLIENTE	TRC
REFERENCIA	
TIPO DE TRABAJO	
FECHA	29/09/2025

<b>REALIZADO POR</b>	<b>SUPERVISADO POR</b>	<b>AUTORIZADO POR</b>	<b>REVISADO POR</b>
Dpto. Ciberseguridad	Carlos Díaz	Carlos Díaz	Carlos Díaz

## REGISTRO DE EDICIONES

EDICIÓN	FECHA	PARTES QUE CAMBIAN	DESCRIPCIÓN DE CAMBIOS
7.0	29/09/2025	Todo el documento	Nueva Plantilla, adecuación a la nueva guía 805, adaptación ISO27001:2022 y directiva NIS2.
7.0	15/12/2025	Fecha aprobación comité de dirección	

# ÍNDICE DE CONTENIDO

1.	<b>Aprobación y entrada en vigor</b> .....	3
2.	<b>Objeto</b> .....	3
3.	<b>Alcance</b> .....	3
4.	<b>Misión y objetivos de la organización</b> .....	4
4.1.	<b>Misión</b> .....	4
4.2.	<b>Objetivos de seguridad de la información</b> .....	5
5.	<b>Principios rectores de la política</b> .....	6
6.	<b>Marco normativo</b> .....	7
6.1.	<b>Identificación de legislación aplicable</b> .....	8
7.	<b>Organización de la seguridad</b> .....	9
8.	<b>Organización e implantación del proceso de seguridad</b> .....	10
9.	<b>Estructura de la documentación de seguridad</b> .....	11
10.	<b>Categorización de los sistemas</b> .....	12
10.1.	<b>Información</b> .....	12
10.2.	<b>Servicios</b> .....	13
11.	<b>Clasificación de la Información</b> .....	14
12.	<b>Datos de carácter personal</b> .....	15
13.	<b>Gestión del Riesgo</b> .....	16
14.	<b>Gestión del personal y Profesionalidad</b> .....	17
15.	<b>Concienciación</b> .....	18
16.	<b>Autorización y gestión de acceso</b> .....	19
17.	<b>Protección de las instalaciones</b> .....	20
18.	<b>Adquisición de productos de seguridad y contratación de servicios de seguridad</b> .....	21
19.	<b>Mínimo privilegios</b> .....	22
20.	<b>Integridad y actualización del sistema</b> .....	23
21.	<b>Protección de la información almacenada y en tránsito</b> .....	24
22.	<b>Prevención ante otros sistemas de información interconectados</b> .....	25
23.	<b>Registro de la actividad y detección de código dañino</b> .....	26
24.	<b>Gestión de incidentes de seguridad</b> .....	27
25.	<b>Continuidad de la actividad</b> .....	28
26.	<b>Mejora continua del proceso de seguridad</b> .....	29
27.	<b>Revisión y evaluación de la política de seguridad</b> .....	30

## 1. Aprobación y entrada en vigor

La presente política ha sido aprobada el día 15/12/2025 por el comité de dirección de TRC como adaptación a la nueva guía del CCN-STIC 805 Política de Seguridad de la Información actualizada en junio de 2025 y teniendo en cuenta el reglamento de ejecución que se tomará como punto de partida como preparación al cumplimiento de la Directiva NIS2.

## 2. Objeto

La evolución de la sociedad y las tecnologías de la información demanda a las organizaciones que forman parte de dicho entorno, para enfrentar los riesgos y amenazas del manejo de la información, entendida como el principal activo para las empresas respecto a su operativa de negocio y clientes.

La Política de Seguridad de la información es una declaración de principios para una gestión adecuada de la seguridad de la información en TRC, alineada con las directrices estratégicas de la Organización y la normativa legal vigente.

La política se refleja en una serie de políticas, normas, y procedimientos a seguir basadas en estándares reconocidos, donde se definen las medidas a tomar para proteger la seguridad de la información que maneja TRC y los sistemas que opera.

La Política de Seguridad de TRC debe ser conocida y es de obligado cumplimiento para todos sus empleados y colaboradores internos o externos.

Cualquier plan específico sobre Seguridad de la Información deberá ajustarse a las disposiciones y recomendaciones, de carácter más general y superior del presente documento. Ante la existencia de contradicciones o discrepancias, se aplicará la política o medida de carácter más restrictivo.

El objeto de esta política es alcanzar la protección adecuada, proporcionada y razonable de la Información de TRC, mediante la preservación de sus requisitos básicos de seguridad: confidencialidad, integridad y disponibilidad.

## 3. Alcance

Esta Política de seguridad TIC es de aplicación, con carácter obligatorio, sobre todos los sistemas TIC, servicios y procesos de negocio, activos de información e instalaciones responsabilidad de las empresas que conforman TRC, además de aplicar a todo el personal interno o externo que tenga acceso a la información o a los sistemas de TRC.

Cualquier empresa o entidad con acceso a la información y a los sistemas de TRC también deben cumplir con la siguiente política.

## 4. Misión y objetivos de la organización

TRC entiende la Seguridad como un elemento fundamental para proteger los activos de la organización, considerándola como un proceso integral basado en la gestión y el control de riesgos con el fin de lograr sus objetivos y cumplir con su misión

TRC se compromete a disponer de los recursos técnicos y humanos necesarios para garantizar una adecuada gestión de la seguridad en la organización.

### 4.1. Misión

Nuestra amplia trayectoria abarca desde la ciberseguridad de vanguardia hasta la defensa del ciberespacio, traduciéndose en la integración estratégica de la Inteligencia Artificial en todos nuestros productos. Como líderes en seguridad y transformación digital, creamos soluciones basadas en IA para simplificar la toma de decisiones en entornos complejos. Diseñamos y construimos arquitecturas digitales seguras, robustas y personalizadas, ofreciendo proyectos que garantizan la máxima protección y eficiencia, y estableciendo alianzas sólidas para el éxito de proyectos complejos.

Las actividades desarrolladas por TRC engloba:

- **Implementación y despliegue con personal propio y certificado por fabricante.** El respaldo con ingeniería propia y no sólo de fabricante, garantiza la mayor cobertura y flexibilidad en nuestras instalaciones.
- **Servicios Profesionales con un equipo multidisciplinar especializado en nuestras tecnologías core** con el objetivo de ofrecer servicios de consultoría tecnológica con un alto nivel de atención y personalización, ajustándonos a las necesidades de nuestros clientes y con muy alto grado de satisfacción.
- **Servicios Gestionados con personal cualificado**, capacitado para ofrecer un servicio personalizado sobre los sistemas de nuestros clientes. Proveemos servicios gestionados y de atención ante incidencias 24x7, acortando los tiempos de respuesta, subsanando los fallos en tiempo y garantizando la continuidad de sus procesos.

## 4.2. Objetivos de seguridad de la información

Los objetivos en materia de seguridad que TRC pretende garantizar con la presente política serán:

1. Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.
2. Minimizar el riesgo a través de la implantación de medidas de seguridad.
3. Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
4. Apoyar la innovación tecnológica.
5. Implementar el sistema de gestión de seguridad de la información ajustado a las necesidades y dimensión de las empresas de TRC.
6. Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas
7. Proteger los activos tecnológicos a través de la implantación de medidas físicas y lógicas.
8. Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
9. Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.
10. Establecer las políticas, procedimientos e instrucciones en materia de seguridad de la información que ayude a incrementar el nivel de madurez de todos los procesos de la organización.
11. Fortalecer la cultura de seguridad de la información de la empresa. Formando y concienciando a los integrantes de TRC respecto a la seguridad de la información.
12. Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
13. Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos

## 5. Principios rectores de la política

En materia de seguridad de la información TRC deberá tener en cuenta los siguientes principios de seguridad:

1. **La seguridad como un proceso integral.** La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información.
2. **Gestión de la seguridad basada en los riesgos.** El análisis y la gestión de los riesgos es parte fundamental del ciclo de vida de los procesos de la organización. Basándonos en los resultados, se establecerá, aplicará y supervisará un plan de tratamiento de riesgos.
3. **Prevención, detección, respuesta y conservación.** Se establecerán, documentarán y aplicarán procesos, políticas y/o procedimientos para la prevención y Gestión de Incidentes de Ciberseguridad, para detectar, analizar, contener o responder a Incidentes, recuperarse de ellos, documentarlos y notificarlos oportunamente.
4. **Existencia de líneas de defensa.** Los sistemas de información deben disponer de una estrategia de defensa basada en *zero-trust*, que permita reducir la probabilidad de ocurrencia de una amenaza y minimizar su impacto. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, lógica y física.
5. **Vigilancia continua.** La vigilancia continua a través de una monitorización permitirá la detección de actividades o comportamientos anómalos y su respuesta.
6. **Reevaluación periódica.** Obtener una mejora continua en los procesos es el finde por el que las medidas de seguridad se reevaluarán y actualizarán periódicamente.
7. **Diferenciación de responsabilidades.** La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información.

## 6. Marco normativo

Las empresas de TRC velarán por el cumplimiento de la legislación vigente y la normativa interna en materia de tecnologías de la información y las comunicaciones.

En el ejercicio de sus competencias las empresas de TRC gestiona datos de carácter personal siéndole de aplicación los principios básicos y requisitos legales exigidos por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) y anteriormente la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD).

TRC ofrece servicios relacionados con los sectores de Gestión de servicios de TIC e infraestructura digital, por lo que la directiva NIS2 le es de aplicación. El objeto de esta directiva es alcanzar un elevado nivel común de ciberseguridad en toda la UE para mejorar el funcionamiento del mercado interior.

En una organización como TRC, que presta soluciones tecnológicas innovadoras y avanzadas, resulta imprescindible dar cumplimiento al RIA, con el fin de abordar los riesgos vinculados a los usos de la IA, de forma que los productos que sean lanzados al mercado sean seguros y confiables, y puedan proporcionar un valor añadido al consumidor final. Con el RIA, se pretende garantizar que los sistemas de IA desarrollados y utilizados dentro de la UE sean seguros y no causen daños a la seguridad, ni a los derechos fundamentales de las personas. Es por ello por lo que, las empresas de TRC se comprometen a utilizar la IA de manera ética, responsable y transparente, garantizando que todas las herramientas de IA cumplan con la legislación vigente y la normativa interna en materia de tecnologías de la información y las comunicaciones.

Dado que TRC desarrolla y gestiona sistemas y modelos de inteligencia artificial, se compromete a respetar en todo momento la normativa vigente en materia de propiedad intelectual, en particular lo establecido en el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, y sus posteriores modificaciones, incluyendo el Real Decreto-ley 6/2022, de 29 de marzo.

También, se tendrá en cuenta la ISO 42001:2023, que establece los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Inteligencia Artificial (SGIA) en las organizaciones. TRC identificará si los sistemas y modelos de IA utilizados o desarrollados, se constituyen conforme a los modelos de propósito general IA (GPAI).

TRC adquiere y explota material de terceros cumpliendo en todo momento la ley de propiedad intelectual, aprobado por el Real Decreto Legislativo N.º 1/1996 de 12 de abril de 1996, y modificado por el Real Decreto-ley N.º 6/2022, de 29 de marzo de 2022.

Además, TRC dispone de las siguientes ISO:

- ISO 9001. Esta norma está enfocada a la consecución de la calidad en una organización mediante la implementación de un método o Sistema de Gestión de la calidad (SGC).
- ISO 27001. La norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI).

- ISO 20000. Esta norma garantiza que los servicios y procesos que realiza una empresa de gestión de servicios TI son realizados bajo unas condiciones de buenas prácticas, garantizando un nivel alto de calidad en los mismos
- ISO 15504. Normativa de desarrollo de estándar para la determinación de la Capacidad de Mejora del Proceso de Software.

### 6.1. Identificación de legislación aplicable

TRC deberá identificar y documentar el marco normativo aplicable a sus sistemas de información, considerando tanto la legislación nacional como sectorial que afecte al tratamiento de la información y la prestación de servicios electrónicos.

## 7. Organización de la seguridad

En la Seguridad de la Información todos los empleados tienen un papel relevante. Para garantizar la seguridad de la información tratada y los servicios prestados, existen distintas figuras, dependiendo de la responsabilidad que tienen en la especificación, supervisión y operación de la seguridad de la información en la organización.

La Dirección de TRC dispondrá de una estructura organizativa para la adecuada gestión de la Seguridad de la Información, en la que se definan las funciones, responsabilidades y procedimientos de designación de todos los participantes.

A continuación, se enumeran cada una de las figuras que forman la organización de la seguridad

- Comité de Dirección
- Responsable de la Información (CIO).
- Responsable de Seguridad CISO).
- Director de Tecnología (CTO).
- Responsable del Servicio.
- Responsable del Sistema.
- Administrador de Seguridad (ASS).
- Jefe de Seguridad (DSSG)
- Responsable de Seguridad Física (RSF).

## 8. Organización e implantación del proceso de seguridad

La implantación de la política de seguridad en la organización establece en tres niveles mediante, políticas, normas y procedimientos operativos de seguridad que afronten aspectos específicos según el marco legal y regulatorio vigente:

- Las Políticas, como el presente documento, son un conjunto de reglas y directrices generales que guían la toma de decisiones y el comportamiento. Establecen los principios que se deben seguir para alcanzar los objetivos de la organización.
- Las Normas son documentos que sirven para indicar cómo se debe actuar de manera adecuada, especialmente en el caso de que una cierta circunstancia no esté recogida en un procedimiento específico. Son el conjunto de regulaciones que desarrollan la política de seguridad y privacidad y tratan de su aplicación.
- Los Procedimientos Operativos son el conjunto de documentos que describen explícitamente y paso a paso como realizar una cierta actividad, según las directrices de carácter técnico o procedimental que se deben observar. Define claramente quien debe realizar cada tarea.

Estos documentos son obligado cumplimiento y deben ser conocidos y estar disponibles para su consulta por aquellas personas que los tienen que aplicar.

---

## 9. Estructura de la documentación de seguridad

TRC dispone de una estructura normativa aplicable a todas las empresas que conforman el grupo, así como a los proveedores y socios que presenten servicios para o se relacionen con TRC.

La documentación de seguridad se almacena en SharePoint y Factorial. En Factorial se encuentra toda la información que debe ser de fácil acceso para los empleados como la política y la normativa. Se dispone de un SGSI que almacena toda la documentación de seguridad accesible para los responsables de las áreas.

## 10. Categorización de los sistemas

Todos los sistemas de TRC que deban cumplir el Esquema Nacional de seguridad tendrán una categorización adecuada a la información y servicios que proporcionan. La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa.

Los criterios de valoración se han definido siguiendo la guía "CCN-STIC-803" que establece criterios comunes y específicos de información y servicios:

### 10.1. Información

Los requisitos de confidencialidad, integridad, trazabilidad y autenticidad sobre un servicio derivan de la información que maneja. Se valorará el impacto sobre:

- La capacidad de la organización para el logro de sus objetivos.
- Los activos
- El cumplimiento de la normativa que le sea de aplicación, incluyendo el perjuicio sobre los derechos y libertades de las personas.

CRITERIOS COMUNES A TODAS LAS DIMENSAIONES				
IMPACTO	No aplicable	BAJO	MEDIO	ALTO
		Perjuicio limitado	Perjuicio grave	Perjuicio muy grave
La capacidad para alcanzar objetivos.	No existe un impedimento	Existe algún inconveniente leve para alcanzarlo, pero que es subsanable a corto plazo	Existe una pérdida de la capacidad que es subsanable a medio plazo	Existe una pérdida de la capacidad no subsanable a medio plazo.
Los activos	No existe perjuicio	Existe un perjuicio leve y subsanable	Existe un daño importante, aunque subsanable	Existe un daño grave de difícil o imposible reparación
Cumplimiento normativo	No implica un incumplimiento	Incumplimiento leve de una regulación, de carácter subsanable.	Incumplimiento material de una regulación, no subsanable.	Incumplimiento formal y material de una regulación, no subsanable.

Tabla 1 - Criterios Valoración

## 10.2. Servicios

La valoración de todos los servicios será sobre su disponibilidad tomando como referencia

<b>IMPACTO</b>	<b>BAJO</b>	<b>MEDIO</b>	<b>ALTO</b>
Tiempo de recuperación del servicio	1 días < RTO < 5 días	4 horas < RTO < 1 día	< 4 horas

Tabla 2 - Tabla impacto servicios

## 11. Clasificación de la Información

La información de TRC está catalogada en tres categorías, dependiendo de su uso/manejo y grado de confidencialidad. Todo empleado debe ser conocedor de esta clasificación:

- **Confidencial (C):** Esta categorización se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos que precisen del más alto grado de protección por su excepcional importancia y cuya revelación no autorizada pudiera dar lugar a riesgos o perjuicios para los intereses del negocio.
- **Uso interno (UI):** Esta categorización se aplicará a documentación interna de TRC que por intereses del negocio no debe ser compartida con personas ajenas a la organización.
- **No clasificada:** Esta categorización se aplicará a la información que puede ser compartida externamente, sin restricciones. Información de uso promocional, presentaciones comerciales, etc.

El Responsable de la Información define los tipos de información que se considera Confidencial, además de definir tipos de información que serán clasificadas como uso interno.

Cuando se reciba información clasificada de terceros (diferente de aquella sujeta a lo dispuesto por la Ley de Secretos Oficiales -Ministerio de Defensa o del Interior-), será manejada de acuerdo con lo requerido por su originador.

El manejo y tratamiento de información clasificada en concursos y licitaciones de la Administración General del Estado (AGE), será según lo dispuesto en su normativa. En dos últimos casos serán gestionados por el Jefe de Seguridad.

---

## 12. Datos de carácter personal

En el ejercicio de sus competencias las empresas de TRC gestiona datos de carácter personal. La organización dispone de un DPO notificado a la AEPD. Se dispone de un registro de actividades de tratamiento (RAT) al que solo accederá el personal autorizado, recoge los ficheros afectados y los responsables correspondientes.

Cuando un sistema trate datos personales, el responsable del servicio contactará con el DPO para recopilar los requisitos de protección de los datos que serán notificados e implantados a través del responsable de seguridad.

## 13. Gestión del Riesgo

TRC efectuará evaluaciones formales de riesgo, identificando las amenazas a las que se encuentran expuestos sus activos, cuantificando posibles impactos y priorizando la asignación de los recursos disponibles para su subsanación.

La metodología utilizada para la gestión del Riesgo será MAGERIT. Esta es la metodología de análisis y gestión de riesgos elaborada en su día por el antiguo Consejo Superior de Administración Electrónica y actualmente mantenida por la Secretaría General de Administración Digital (Ministerio de Asuntos Económicos y Transformación Digital) con la colaboración del Centro Criptológico Nacional (CCN).

Para el análisis y la gestión de riesgos se seguirá las metodologías establecidas en el Procedimiento de análisis y gestión de riesgos. La organización dispone de un Análisis de Riesgos corporativo, además de uno para cada uno de los servicios dentro del alcance del Esquema Nacional de Seguridad.

- El ciclo de vida de la gestión de riesgos es la siguiente:
- Identificación de activos, en la que se determinaran los activos relevantes, su valor y amenazas.
- Análisis de riesgos inicial, los resultados iniciales del análisis.
- Plan de tratamiento, acciones del plan de tratamiento.
- Riesgo residual, cálculo del riesgo después de aplicar el tratamiento.
- Reevaluación del análisis de riesgos de manera anual.

## 14. Gestión del personal y Profesionalidad

El personal de TRC relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Esto se realizará en la firma del contrato. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos. Las responsabilidades y deberes estarán relacionadas con cada puesto de trabajo.

Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar el puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias, de conformidad con el ordenamiento jurídico y el respeto a los derechos fundamentales.

Todo el personal está sujeto al conocimiento y cumplimiento de toda la Política de Seguridad y normativa relacionada con el uso de los medios TIC que se le asignen, y de los sistemas y servicios TIC de uso en la empresa. También se dispone de una política de mesas limpias, cuyo fin es mantener el puesto de trabajo despejado.

A efectos de trazabilidad, todo usuario que acceda a la información del sistema estará identificado de forma única, lo que permitirá en caso de que fuera necesario realizar un seguimiento de sus acciones para poder corregir acciones o exigir responsabilidades en caso de incumplimiento de la normativa y política de seguridad.

Se dispondrá de un procedimiento sancionador orientado al incumplimiento de las medidas de seguridad, que será conforme a la legislación aplicable, convenio colectivo en vigor y Estatuto de los Trabajadores, que deberá ser conocido por todo el personal de la empresa.

El personal recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de TRC:

- La seguridad de los sistemas está atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

Los departamentos encargados de estas tareas son, Ciberseguridad, Sistemas y Networking. El personal de estos departamentos tiene la experiencia y formación necesaria para realizar estas tareas. Además, el personal cuenta con certificaciones de seguridad, y de productos de seguridad según el rol que desempeñe.

- El personal que se incorpore a estos departamentos recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas.
- TRC exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

---

## 15. Concienciación

La Concienciación del personal es fundamental en la Seguridad de la Información y forma parte de las medidas de Prevención de la empresa.

Dado que los vectores de ataque a los sistemas IT se sirven en multitud de casos de la ingeniería social (engaño al personal), disponer de trabajadores que conozcan y sepan cómo actuar ante las amenazas y ataques que puedan producirse, resulta prioritario.

El responsable de Seguridad y el Departamento de Ciberseguridad realizarán las acciones necesarias para lograr la adecuada concienciación del personal de la empresa y del conocimiento de la Cultura de Ciberseguridad de TRC.

Cada nuevo empleado de la organización recibe un curso de concienciación a través de una solución especializada. Además, a lo largo del año, a petición del responsable de seguridad o dirección se realizan varias simulaciones de Phishing. Todo esto viene definido en el Plan de concienciación impulsado por Recursos Humanos.

---

## 16. Autorización y gestión de acceso

El acceso a los sistemas y servicios están controlados y limitados a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas

Cada persona dentro de la organización recibe un usuario único con su correspondiente contraseña, para acceder a la información del sistema. Cuando se accede por primera vez se solicita el cambio de contraseña. Una vez establecida la nueva contraseña se solicitará un cambio según lo establecido en la política de contraseñas y directiva aplicada al dominio.

El acceso a servicios que requieren un usuario diferente al corporativo se registrará por los mismos principios y medidas de seguridad.

De esta forma puede ser identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

Los servicios accesibles desde internet están protegidos con doble factor de autenticación, los de intranet solo serán accesibles a través de VPN.

## 17. Protección de las instalaciones

Las instalaciones de TRC se encuentran protegidas con un sistema de control de acceso. Además, antes de acceder al edificio hay una garita con personal de TRC para controlar la entrada de las visitas, la recepción del material, y la entrada al parking.

Las visitas llevan una tarjeta identificativa de visita además de una cinta naranja que los distingue del personal de la organización.

Toda la sede de TRC cuenta con un sistema de videovigilancia. Dentro de las instalaciones, los sistemas se encuentran en el CPD, que cuenta con un lector de tarjetas como sistema de control de acceso. Solo el personal autorizado tiene permitido el acceso al CPD. Además, hay personal del SAT vigilando el acceso al CPD.

El CPD cuenta con las siguientes características:

- Acondicionamiento de temperatura y humedad.
- Suministro de potencia eléctrica en caso de fallo del suministro general, garantizando el tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información.
- Protección frente a incendios.
- Registro de entrada y salida de equipamientos.

## 18. Adquisición de productos de seguridad y contratación de servicios de seguridad

TRC cuenta con un procedimiento de adquisiciones que busca regular la adquisición de bienes y servicios dentro de TRC, así como la relación con los proveedores y suministradores de estos, garantizando que los procesos sean ordenados, eficientes y conforme a la normativa vigente.

El procedimiento establece el proceso formal que va a regir la gestión de las adquisiciones de bienes, servicios y suministros por parte de TRC, determinando las responsabilidades y criterios que son de aplicación. Esto obedece a la necesidad de adecuación a la normativa aplicable, asegurando la calidad, eficiencia y seguridad.

A la hora de una adquisición se tendrá en cuenta:

- Necesidades técnicas, de formación y financiación.
- Requisitos de seguridad
- Aspectos ambientales
- Requisitos PECAL

Además, los componentes críticos para la seguridad de las redes y sistemas de la información pasarán un proceso de gestión de riesgos derivados de su adquisición. En cada adquisición de un componente crítico se considerará el posible impacto de la nueva incorporación antes de su compra. Por tanto, se ha de revisar y confirmar, que la nueva adquisición se ajusta a la arquitectura de seguridad de la organización y no implica nuevas vulnerabilidades para el sistema.

Se identifican y gestionan los riesgos de una manera global, es decir, atendiendo a toda la cadena de suministro del componente a adquirir. Es indispensable no sólo realizar un estudio al proveedor, sino también a sus subcontratistas y a toda la cadena de suministro.

## 19. Mínimo privilegios

Los sistemas de TRC están diseñados y configurados de forma que se garantice la seguridad por defecto y mínimos privilegios.

El sistema proporciona la mínima funcionalidad requerida para que la organización alcance sus objetivos. Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados.

En los sistemas de explotación se desactivan las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Cuando sea posible se aplicarán guías de seguridad específicas para las diferencias tecnológicas, en función de la categorización del sistema.

El personal solo tendrá los privilegios asociados a su labor diaria, solo los usuarios administradores dispondrán de un mayor privilegio.

## 20. Integridad y actualización del sistema

Todo elemento físico y lógico requiere autorización formal previa a su instalación en el sistema como se define dentro del procedimiento de autorización y quedará registrado en la herramienta de *ticketing* interna.

Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de este.

Trc dispone de varias tecnologías para realizar de forma continua una evaluación y monitorización del estado de los sistemas, lo que permite adecuar su estado de seguridad atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

Todo el software y el hardware deberá estar actualizado con los últimos parches de seguridad, debidamente licenciado y con soporte del fabricante. Se mantendrá un adecuado control y gestión de la obsolescencia, disponiendo de una planificación con las necesidades de mantenimiento de licencias de software y de mantenimiento y sustitución de hardware.

En caso de tener algún sistema obsoleto por requisitos de servicio, cliente o del producto, se tomarán las medidas compensatorias que se consideren más adecuadas para mitigar el riesgo asociado.

## 21. Protección de la información almacenada y en tránsito

En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Se consideran entornos inseguros, los equipos portátiles o móviles, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

Para garantizar la seguridad de los equipos portátiles, las comunicaciones, y los soportes de información, se cumplen con las medidas de seguridad establecidas en el Anexo II del Real Decreto 3/2010 que aplican a nuestros sistemas según su categoría.

Se dispone de un procedimiento de sanitización y destrucción de soportes de información conforme a la normativa aplicable y guías del CCN en función de los distintos tipos de información, incluyendo una herramienta de borrado incluida en el catálogo de productos y servicios STIC.

---

## 22. Prevención ante otros sistemas de información interconectados

Los sistemas cuentan con una protección del perímetro, en particular, en las conexiones a redes de comunicaciones públicas. Se entiende por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones disponibles para los clientes.

En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Los sistemas de TRC a los que el ENS les es de aplicación, dispone de una arquitectura compatible con el Real Decreto para la conexión de los sistemas con otros sistemas de clientes, o proveedores. Para la elaboración de la arquitectura de red se tienen en cuenta la conectividad mínima necesaria, los mecanismos de cifrado, el aislamiento, la segmentación y la anonimización de redes, así como los mecanismos de monitorización y de protección perimetral que sean necesarios. En la medida de lo posible, se aplicarán criterios de ZeroTrust o alternativamente, de mínimos privilegios

En el organigrama de red de la organización se detallan los puntos de interconexión a otros sistemas o a otras redes, y los firewalls utilizados.

## 23. Registro de la actividad y detección de código dañino

Todos los sistemas de TRC, físicos o virtuales, estarán protegidos contra código dañino. Con la finalidad exclusiva de lograr el cumplimiento del objeto del Real Decreto 3/2010, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registran las actividades de los usuarios, utilizando una solución especializada líder en el sector.

Esta solución, recopila la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

---

## 24. Gestión de incidentes de seguridad

TRC dispone de un marco de referencia para el tratamiento de los incidentes de seguridad en los sistemas de información, desde su identificación hasta su cierre y posterior análisis.

Para ello establece un modelo general de respuesta a los incidentes de seguridad asociados a los sistemas de información gestionados por TRC basado en la guía CCN-STIC 817 y teniendo en cuenta los requisitos de la directiva NIS2.

Este modelo especifica los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se emplea para la mejora continua de la seguridad del sistema

Los sistemas de la organización cuentan con protección endpoint de última generación, que, junto con la protección del correo, el procedimiento de gestión de incidentes de seguridad, y los análisis de vulnerabilidades periódicos que se realizan proporcionan un sistema muy fiable de detección y reacción antes amenazas.

---

## 25. Continuidad de la actividad

Los sistemas disponen de copias de seguridad y mecanismos para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

La organización dispone de un procedimiento de copias de backup, un BIA y un plan de continuidad del negocio.

El plan de continuidad definirá cada una de las estrategias de recuperación y los modos de funcionamiento alternativo para todos aquellos sistemas críticos que deben seguir operando a pesar de su degradación hasta poder recuperar la normalidad en el servicio.

---

## 26. Mejora continua del proceso de seguridad

TRC cuenta con la certificación ISO 27001, y la certificación del ENS nivel Medio y nivel Alto para algunos de sus servicios. Lo que hace el proceso integral de seguridad implantado se actualice y mejore de forma continua.

El equipo de auditoría interna dentro del área de ciberseguridad realizará auditorías periódicas a las auditorías de certificación para detectar puntos de mejora.

---

## 27. Revisión y evaluación de la política de seguridad

La Política de Seguridad se revisará de forma anual o a petición del Responsable de Seguridad de TRC o dirección. Un cambio en la normativa aplicable también puede producir una revisión en la política de seguridad.

De forma previa a la aprobación de los cambios por el Comité de Dirección, debe determinarse el impacto que dichos cambios puedan producir en el resto de Las políticas de Seguridad de TRC.

Tras su aprobación se comunicarán los cambios a los empleados de TRC y se subirá la nueva política a Factorial.