POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN y

ESQUEMA NACIONAL DE SEGURIDAD

La Dirección de **Eurona**, consciente de la necesidad de promover, mantener y mejorar el enfoque hacia el cliente en todas sus actividades, ha implantado un Sistema de Gestión Integrado (SGI) conforme al estándar cuyo **objetivo** final es asegurar que entendemos y compartimos las necesidades y metas de nuestros clientes, intentando prestar servicios que cumplan sus expectativas trabajando en la mejora continua. Manifiesta expresamente su compromiso de potenciar la **Seguridad y Ciberseguridad** de la Información del servicio prestado, y se compromete a satisfacer las necesidades y expectativas de las partes interesadas, a mantener alta nuestra competitividad en los servicios de **Mantenimiento, Soporte, Operación y administración de infraestructura de red y Servicio de diseño, arquitectura y desarrollo de soluciones software.**

MISIÓN y OBJETIVOS*:*

- Fomentar la mejora continua de los servicios y soporte al cliente.
- Continuar el posicionamiento de **Eurona** como referente en el sector.
- Proporcionar una protección adecuada de la información de **Eurona**, el operador de telecomunicaciones, experto en servicios y soluciones de conectividad a través de tecnologías como internet satelital y Wifi.
- Tener una prestación del servicio basada en nuestro compromiso con la mejora continua de nuestros sistemas, con **la seguridad y ciberseguridad de la información** como pilar central y por defecto.

Nuestra **misión** y objetivos lo conseguiremos a través de:

- Un sistema de **objetivos**, métricas e indicadores de mejora continua, seguimiento, medición de nuestros procesos internos, así como de la satisfacción de nuestros clientes. Estableciendo y supervisando el cumplimiento de los requisitos contractuales para asegurar un servicio eficaz y seguro.
- Formando y concienciando continuamente a nuestro equipo para tener el mayor grado de profesionalidad y especialización posible, además teniendo nuestras infraestructuras en un estado adecuado y en concordancia con los requerimientos de nuestros clientes.
- Con un procedimiento seguro de gestión de adquisición de productos.
- Cumpliendo las exigencias de la legislación vigente, especialmente con el **GDPR** y el cumplimiento de nuestra **Documentación de Seguridad**.
- Introduciendo los procesos de mejora continua que permitan un avance permanente en nuestra gestión de Seguridad de la Información.
- Gestionando y elaborando planes para la gestión y tratamiento de los riesgos con una metodología de análisis y gestión de riesgos utilizada, basada en estándares.
- Gestionando las comunicaciones internas y externas e información almacenada y en tránsito.
- Gestionando y monitorizando la actividad con la gestión de logs.
- Con especial atención a la gestión de incidentes de seguridad
- Asegurando la continuidad y disponibilidad del negocio y de los servicios.
- Asegurar que nuestros Activos y Servicios cumplen con las medidas del **ENS** de **Nivel MEDIO** para las dimensiones de **Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad**.

Así mismo, estos principios se deberán contemplar en las siguientes áreas de seguridad:

- **Física**: Comprendiendo la seguridad de las dependencias, instalaciones, sistemas hardware, soportes y cualquier activo de naturaleza física que trate o pueda tratar información, así como los accesos físicos.
- **Lógica**: Incluyendo los aspectos de protección de aplicaciones, redes, comunicación electrónica, sistemas informáticos y con los accesos lógicos.
- **Político-corporativa:** Formada por los aspectos de seguridad relativos a la propia organización, a las normas internas, regulaciones y normativa legal.

El objetivo último de la seguridad de la información es asegurar que una organización pueda cumplir sus **objetivos** utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad integral.
b) Gestión de riesgos.
c) Prevención, reacción y recuperación.
d) Líneas de defensa.
e) Reevaluación periódica.
f) Función diferenciada.

Roles o funciones de seguridad:
Responsable de la Información: Determinar los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS.

- Implantar y mantener el Sistema de Gestión Integrado (SGI) mejorando continuamente su eficacia.
- Implantar y mantener el ENS mejorando continuamente su eficacia.
- Supervisar los procedimientos y las instrucciones técnicas.
- Aplicar las medidas y seguimientos indicados por el DPO.
- Realizar el seguimiento y verificar la implantación y eficacia de todas las acciones correctoras y preventivas establecidas.
- Asegurar que el sistema implantado cumple con la norma establecida.
- Analizar los datos obtenidos en el Sistema de Gestión Integrado (SGI) y ENS y proponer mejoras.
- Elaborar el plan anual de auditorías internas.
- Gestión de No Conformidades de seguridad.
- Participar en Auditoria Externas.
- Responsable de los datos privados de la empresa en cuanto a su pérdida, el robo y la desactualización.
- Cumplir con la Normativa de Seguridad.
- Mantener actualizados los medios de contacto con las autoridades.
- Lleva el inventario de soportes que contienen datos de carácter personal
- Analiza los informes de auditoría y elevan las conclusiones al responsable de los datos.
- Gestiona las no conformidades, acciones correctivas y acciones preventivas de SI
- Mantiene los documentos del SGI
- Mantiene y despliega la política de seguridad de Eurona así como el resto de las políticas al personal implicado en cada una de ellas.
- Confecciona los documentos de seguridad de Eurona
- Atiende incidencias en materia de protección de datos.
- Se encarga de contactar con las autoridades en caso necesario.
- Aplicación y supervisión del cumplimiento de las políticas del SGI.
- Mantenimiento y aplicación del Documento de Aplicabilidad del SGI

Responsable de sistemas: Determina los requisitos de los servicios prestados.

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Velar por el cumplimiento de las obligaciones del RSI
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Además, el responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.

Responsable de Seguridad de la Información: Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información de la organización
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad
- Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas
- Supervisar los procedimientos y las instrucciones técnicas.
- Responsabilidad general de administrar la implementación de las prácticas de seguridad.
- Asegurar que el sistema implantado cumple con la norma establecida.

- Analizar los datos obtenidos en el Sistema de Gestión de Seguridad de la Información y ENS y proponer mejoras.
- Participar en Auditoria Externas.
- Responsable del riesgo de la intrusión física de los dispositivos de la empresa.
- Cumplir con la Normativa de Seguridad.
- Segregación de tareas y entornos.
- Comunicar cualquier emergencia de incendio, inundación o avería de los equipos de climatización que pueda activar el PCN.
- Revisa el Plan de Continuidad del negocio
- Verifica el funcionamiento del Plan de Continuidad de Negocio
- Controla el acceso de personas a los locales donde están instalados los sistemas
- Supervisa las incidencias de seguridad producidas
- Realiza y custodia las copias de seguridad
- Genera los planes de tratamiento de gestión de riesgo y supervisa su implantación
- Actualiza el análisis de riesgos
- Convoca las reuniones del CSI
- Genera las actas de reunión del CSI
- Supervisa la recogida de métricas.
- Realiza las revisiones de seguridad del SGI
- Mantiene el Plan de Continuidad de Negocio
- Incorpora en el registro de incidencias las medidas correctoras
- Aplicación y supervisión del cumplimiento de las políticas de SGI.

Responsable del Servicio: Determina los niveles de seguridad de los servicios

- Garantizar el cumplimiento de los objetivos y métricas establecidos para el servicio (SLAs)
- Organización diaria de los recursos
- Responsable de la pérdida y robo de información de los servicios y soluciones informáticas para clientes y usuarios en general
- Cumplir la Normativa de Seguridad
- Incluye las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Programar, dirigir, coordinar, supervisar y controlar todas las actividades del servicio
- Revisión y cumplimiento de los informes de los servicios.
- Valorara las consecuencias de un impacto negativo sobre la seguridad de los servicios, se efectuara atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y de los derechos de los ciudadanos.

El Comité de Seguridad de la Información (CSI) de Eurona alcanza a toda la empresa, es el mecanismo de coordinación y resolución de conflictos, entre otras funciones:

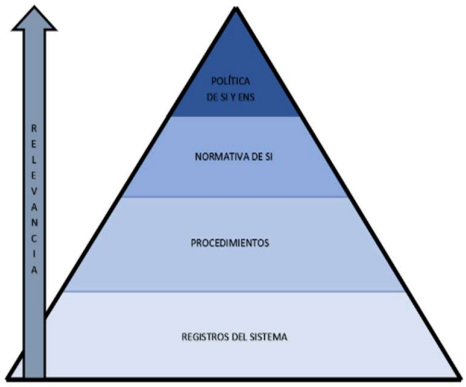
- Atender las inquietudes de la Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

Componen el CSI:

- Responsable de la Información
- Responsable del Servicio
- Responsable de Seguridad de la información

- Responsable del Sistema (Hotspots)
- Responsable del Sistema (Operaciones)
- Responsable del Sistema (TI)
- Responsable del sistema delegado (Portales y Dashboard)
- Responsable de contratación y adquisición
- Administrador de red

Estructuración de la documentación de seguridad del sistema
La documentación del sistema sigue la siguiente estructura:



La clasificación de la información del sistema se clasifica en las siguientes categorías, tal y como se establece en documento Normativa de seguridad:

- Uso Publico
- Uso Interno
- Uso Confidencial

Legislación aplicable en materia de tratamiento de datos de carácter personal
En materia de tratamiento de datos de carácter personal se tendrá en cuenta, principalmente, 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 y por el que se deroga la Directiva 95/46/CE y la legislación nacional correspondiente.
El marco legal y regulatorio aplicable se encuentran recogido en el documento Registro Identificación y evaluación de requisitos legales Eurona

Considerando estas pautas, esta dirección reitera su más firme compromiso aunando esfuerzos para el logro de estos objetivos, por lo que esta política es entendida, implantada y tenida al día en todos los niveles de la organización.

Fdo.

Jordi Puig Cruz
Representante de Dirección