POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

0. TRAZABILIDAD Y DISTRIBUCIÓN DEL DOCUMENTO.

TABLA DE REVISIONES		
REVISIÓN	**FECHA**	**MOTIVO DE LA REVISIÓN**
01	01/07/2024	Emisión Inicial.
02		
03		

DOCUMENTO PREPARADO Y REVISADO		
FIRMA	**FECHA**	**PERSONA - CARGO**
Marta Carral	01/07/2024	Marta Carral **Resp. Seguridad**

APROBACIÓN DOCUMENTO		
FIRMA	**FECHA**	**PERSONA - CARGO**
JM Elizalde	01/07/2024	Juan M. Elizalde **DIRECTOR**

El personal relacionado a continuación está autorizado para acceder al presente documento:

Responsable:	**Responsable SI.**
Lista de personal autorizado a acceder al documento:	Todo el personal de la Entidad.

0. TRAZABILIDAD Y DISTRIBUCIÓN DEL DOCUMENTO. 2

1. OBJETO. 4

2. ALCANCE. 4

3. MISIÓN Y OBJETIVOS. 4

4. PRINCIPIOS. 6

5. MARCO NORMATIVO. 7

6. ROLES Y FUNCIONES. ORGANIZACIÓN DE LA SEGURIDAD. 7

7. COMPROMISO DE LA DIRECCIÓN. 9

8. POLÍTICAS DE USO DE LOS SISTEMAS DE INFORMACIÓN DE KELLS. 9

8.1 Política de Uso Aceptable de los Servidores. 9
8.2 Política de Uso Aceptable de Estaciones de Trabajo. 10
8.3 Política de Uso Aceptable de Dispositivos Móviles. 13
8.4 Política de Uso Aceptable del Correo Electrónico. 15
8.5 Política de Uso Aceptable de la Conectividad a Internet. 18
8.6 Política de Uso Aceptable de Impresoras. 20
8.7 Política de Acceso al CPD. 20

9. GESTIÓN DE LOS RECURSOS HUMANOS. 21

10. MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN Y GESTIÓN DE INCIDENTES. 22

11. SEGUIMIENTO, SUPERVISIÓN Y MONITORIZACIÓN DE LOS SISTEMAS DE INFORMACIÓN. 22

12. ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD. 23

13. DATOS DE CARÁCTER PERSONAL. 24

14. DOCUMENTACIÓN RELACIONADA. 24

1. OBJETO.

El objeto de la presente Política de Seguridad de la Información es determinar el alcance y estructura del sistema de Información (SI) implantado en KELLS, en base a las directrices estipuladas en el RD 311/2022 - Esquema Nacional de Seguridad, así como en la Norma UNE-EN ISO 27001:2022.

2. ALCANCE.

El Alcance del Sistema de Gestión de la Seguridad de la Información de KELLS es el siguiente:

Para la ISO 27001:2022.
Sistema de gestión de la seguridad de la información aplicable a los servicios de:

- **Gestión integral de Programas Formativos en el extranjero**

Para el ENS:
Sistema de información que soportan los servicios gestionados de:

- **Gestión integral de Programas Formativos en el extranjero, de acuerdo a la Declaración de Aplicabilidad KELLS-ENS-01, de fecha 04/07/2024**

3. MISIÓN Y OBJETIVOS.

KELLS unifica las perspectivas legal y tecnológica para ofrecer a sus clientes una solución integral a sus necesidades relacionadas con el Diseño, Instalación y Mantenimiento de Sistemas de Telecomunicaciones, y resto de servicios descritos en el Alcance.

KELLS basa su actividad en el tratamiento de diferentes tipos de datos e información, ello le permite ejecutar procesos básicos propios del negocio. Los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyen el activo principal de **KELLS**, de tal manera que el daño o pérdida de los mismos inciden en la realización de sus operaciones, y pueden poner en peligro la continuidad de la Organización.

Todo ello a través de escenarios de innovación permanente, investigación y desarrollo como elementos clave, y una cultura totalmente orientada a la excelencia en el servicio y al establecimiento de un marco de relación con los clientes y colaboradores como socios de negocio.

Estas cuestiones se materializan con las aportaciones de un amplio equipo de personas formadas, certificadas y en permanente actualización de conocimientos, así como en métodos y prácticas.
La excelencia en la ejecución, la fidelidad en el marco de relaciones y la empatía hacia el cliente y entre compañeros actúan como valores y principios básicos que rigen nuestra actuación.

En el ámbito concreto de la seguridad, el SI corporativo pretende lograr alcanzar **los siguientes objetivos:**

- Cumplir con las necesidades y expectativas de las partes interesadas involucradas dentro del alcance del SI protegiendo la información interna y relacionada con la prestación de los servicios, considerando las dimensiones de:
  - Confidencialidad para asegurar que la información solo sea accedida por aquellos que cuenten con la autorización respectiva. Toda la información se protegerá de manera que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos, no autorizados previamente.
  - Integridad para preservar la veracidad y completitud de la información y los métodos de procesamiento. Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterado de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.
  - Disponibilidad para asegurar que los usuarios autorizados tienen acceso a la información y los procesos, sistemas y redes que la soportan, cuando se requiera. La información será accesible a aquellos usuarios o procesos que la requieran y cuando lo requieran. Será principio básico de la organización, la restricción de accesos al mínimo necesario.
  - Trazabilidad: Para asegurar que queda constancia fehaciente del uso del servicio y del acceso a los datos, es decir, que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. Toda acción desarrollada en el sistema o sobre la información, puede ser imputada a su autor, en cualquier fase de ciclo de vida o en cualquier fase de proceso.
  - Autenticidad: Para asegurar que quien accede al servicio es realmente quien se cree y garantizar la fuente de la que proceden los datos. Toda información puede ser asignada a una fuente o todo autor puede ser contrastado y acreditar su identidad sin lugar a duda.
- Demostrar liderazgo por parte de la dirección, dotando de recursos al SI y asegurando que la política y los objetivos de seguridad que se establezcan sean compatibles con la estrategia de la organización.
- Gestionar la implementación del SI de manera que proporcione ventajas competitivas en relación con otros agentes del sector, aprovechando la inercia que puede otorgar la gestión adecuada de la seguridad.
- Apostar por la **mejora continua**, y la implementación de medidas de seguridad eficaces y eficientes.
- Establecer anualmente objetivos, relacionados con ámbitos específicos de seguridad alineados con las normas de referencia del SI, ENS e ISO 27001.
- Cumplir con los requisitos del negocio, legales o reglamentarios y las obligaciones contractuales de seguridad, alineando dichos requisitos con la privacidad y la seguridad de la información corporativa.
- Sensibilizar y concienciar de manera estable y permanente a todo el personal de la organización en cuanto a la seguridad de la información.
- Fomentar y mantener el buen nombre de la organización en relación con los servicios desarrollados, saber y respuesta activa (reactiva y proactiva) ante incidentes de seguridad, mantenimiento la imagen y reputación.

Documento clasificado como **PÚBLICO**

4. PRINCIPIOS.

La política de seguridad de la información de **KELLS** se desarrolla de acuerdo con los siguientes principios:

- **Principio de confidencialidad**: se deberá garantizar que la información sea accesible únicamente para aquellas personas expresamente autorizadas para ello.
- **Principio de integridad**: se deberá asegurar que la información con la que se trabaja sea completa y precisa, y se incidirá en la exactitud tanto de su contenido como de los procesos involucrados.
- **Principio de disponibilidad**: se garantizará la prestación continua de los servicios y la recuperación inmediata ante posibles contingencias, mediante medidas de recuperación orientadas a la restauración de los servicios y de la información asociada.
- **Principio de gestión del riesgo:** Se deben minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre las medidas de seguridad y la naturaleza de la información.
- **Principio de mejora continua**: se revisará de manera recurrente el grado de eficacia de los controles de seguridad implantados para aumentar la capacidad de adaptación a la constante evolución del entorno.
- **Principio de proporcionalidad en coste**: la implantación de medidas que mitiguen los riesgos de seguridad de los activos deberá hacerse dentro del marco presupuestario previsto a tal efecto y siempre buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el presupuesto previsto.
- **Principio de cumplimiento normativo**: todos los sistemas de información se ajustarán a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad de la información, en especial aquella relacionada con la intimidad y la protección de datos de carácter personal y con la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.
- **Principio de prevención**: Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.
  Para garantizar el cumplimiento de la política, los departamentos deben: autorizar los sistemas antes de entrar en operación; evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria; solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.
- **Principio de detección**: Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS. La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

- **Principio de respuesta**: Los departamentos deben: establecer mecanismos para responder eficazmente a los incidentes de seguridad; designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos; establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).
- **Principio de recuperación**: Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

5. MARCO NORMATIVO.

La presente política se rige por la siguiente legislación y normativa de referencia:

- **Real Decreto 311/2022, de 3 de mayo**, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- **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.
- **Ley Orgánica 3/2018, de 5 de diciembre**, de Protección de Datos personales y Garantía de los Derechos Digitales.
- **Guías CCN-STIC (Serie 800).**
- **UNE/ISO-IEC 27001:2022: Tecnología de la Información.** Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- **Ley 34/2002, de 11 de julio**, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- **Ley 6/2020, de 11 de noviembre,** reguladora de determinados aspectos de los servicios electrónicos de confianza.
- **Real Decreto Ley 12/2018, de 7 de septiembre**, de Seguridad de la Redes y Sistemas de Información.
- **Real Decreto 43/2021, de 26 de enero**, por el que se desarrolla el Real Decreto Ley 12/2018, de 7 de septiembre, de Seguridad de la Redes y Sistemas de Información.
- **Real Decreto 1150/2021, de 28 de diciembre**, por el que se aprueba la Estrategia de Seguridad Nacional.

6. ROLES Y FUNCIONES. ORGANIZACIÓN DE LA SEGURIDAD.

KELLS dispone de un **Comité de Seguridad de la Información** formado por diferentes roles, para atender las necesidades de seguridad tanto técnicas como organizativas, permitiendo de esta forma una mejor distribución de la información y toma de decisiones. Estos recursos, comienzan por la designación de la seguridad como función diferenciada mediante los siguientes miembros y funciones:

- **Responsable de la información** que determinará los requisitos de la información tratada. *Para desempeñar este rol, se nombra a _D.*
- **Responsable del servicio** que determinará los requisitos de los servicios prestados. *Para desempeñar este rol, se nombra a D..*

- **Responsable del Tratamiento (Protección de Datos):** que determina los fines y medios del tratamiento. *Para desempeñar este rol, se nombra a D.*
- **Encargado del Tratamiento (Protección de Datos):** que trata datos personales por cuenta del Responsable del Tratamiento. Debe aportar garantías suficientes de cumplimiento con el RGPD y adoptar las medidas de seguridad del ENS que correspondan al responsable de tratamiento. *Para desempeñar este rol, se nombra a D.*
- **Responsable de Seguridad** que determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. *Para desempeñar este rol, se nombra a D.*
- **Delegado de Protección de Datos:** que informará, asesorará, y supervisará sobre el cumplimiento en materia de protección de datos de carácter personal incluidos los aspectos de seguridad (integridad, confidencialidad y disponibilidad) y violación de datos personales asesorando sobre la necesidad o no de notificación a la autoridad de control y, en su caso a los propios interesados y comunicando en su caso el incidente a la autoridad de control de protección de datos en virtud de su rol de punto de contacto previsto en el RGPD y la RGPDGDD.
  Su nombramiento lo debe realizar el responsable de tratamiento de manera diferenciada al resto de miembros de Comité de Seguridad ya que sus cometidos no se ciñen únicamente a aspectos de seguridad. Para evitar el conflicto de intereses, debe tener voz pero no voto en la decisiones y deliberaciones del Comité de Seguridad.
- **Responsable del Sistema** supervisará la infraestructura de los sistemas de información dentro de la organización y es responsable de establecer los estándares de información para facilitar el control de la gestión de todos los recursos corporativos. *Para desempeñar este rol, se nombra a_D.*
- **Administrador de la Seguridad del Sistema** que implementará y velará por la correcta implementación de las decisiones para satisfacer los requisitos establecidos por el CISO y el CIO. *Para desempeñar este rol, se nombra a D.*

El procedimiento para su designación y renovación se encuentra documentado en **KELLS-ENS-04 Asignación de Roles y responsabilidades para la Seguridad de la Información.**

Se ha considerado que las funciones del Responsable de Servicio y del responsable de la información, sean asumidas por el Comité de Seguridad de la Información, y que solamente en casos puntuales, sea el Responsable del servicio quien tome las decisiones que sean necesarias.

Las funciones concretas de cada uno de los roles aquí definidos, así como los mecanismos de coordinación y resolución de conflictos, vienen definidos en el documento del SI **KELLS-ENS-04 Asignación de Roles y responsabilidades para la Seguridad de la Información.**

7. COMPROMISO DE LA DIRECCIÓN.

La presente **Política de Seguridad de la Información** marca las líneas de actuación, normativa y compromisos de la Empresa respecto a la Seguridad de la Información, por lo que la Dirección proporciona las líneas de actuación, recursos, responsabilidades y compromisos alrespecto.

La Política es aprobada y revisada de manera periódica por la Dirección y comunicada a todos los empleados para que conozcan los objetivos, normativa y responsabilidades generales y específicas en materia de Seguridad de la Información, así como la importancia de su cumplimento.

8. POLÍTICAS DE USO DE LOS SISTEMAS DE INFORMACIÓN DE KELLS.

El uso generalizado de los Sistemas de Información por parte de los usuarios, hace imprescindible que todos los empleados sean conscientes de su responsabilidad, así como de la importancia de proteger la Información. Tanto los Sistemas como la Información son propiedad de la Empresa y deben ser utilizados para fines exclusivamente laborales.

La presente **Política Interna de Seguridad de la Información**, así como las **Cláusulas de Confidencialidad y Protección de Datos** (de acuerdo al RGPD) recogidas en el Contrato de Trabajo y los procesos asociados a cada puesto, son de obligado cumplimiento por parte de todo el personal de la Organización, constituyendo su incumplimiento una infracción grave a efectos laborales.

La Dirección de la Empresa ha definido para los usuarios de la Organización, en función de los perfiles funcionales y puestos de trabajo, distintos permisos de acceso físico y lógico tanto a losSistemas como a la Información.

A continuación, se especifican detalladamente las diferentes políticas de uso aceptable de cada uno de los Sistemas de Información de la Empresa, y se establece la normativa de protección necesaria para garantizar el correcto tratamiento de la Información.

8.1 Política de Uso Aceptable de los Servidores.

Se establece la siguiente NORMATIVA en lo referente al uso aceptable de los Servidores de la empresa:

N1. Sólo los Responsables de Departamento/Área se encuentran autorizados para solicitar acceso a las unidades de red, recursos y aplicaciones, para el personal a su cargo. Las solicitudes deben dirigirse al Responsable de Sistemas y contar con la aprobación de la Dirección.

N2. Todo servidor que se incluya en la red debe ser instalado (o supervisada su instalación) por el Departamento de Soporte. Así mismo, se debe proveer de la instalación de softwarede protección básica de antivirus y, en su caso, software o agentes de monitorización y backup.

N3. El acceso del usuario a las unidades de red, recursos y aplicaciones se concede individualmente (o mediante pertenencia a grupos de usuarios) por el Departamento de Soporte, en función del puesto de trabajo a desempeñar. Se trata de unidades de red a lasque se accede a través de un medio de autenticación seguro, protegidas por permisos de acceso y de las que se realizan copias de seguridad periódicas.
N4. El usuario debe utilizar las unidades de red establecidas para toda la Organización, como repositorio de Información. Es responsabilidad del usuario garantizar un uso adecuado de su identificador y contraseña, no malgastar intencionadamente los recursos de la red y no destruir datos de otros usuarios.
N5. El acceso en red a los servidores y aplicaciones está destinado a fines exclusivamente laborales, no está permitido el almacenamiento de Información personal en los mismos.
N6. Cada usuario es Responsable de comprobar que la Información que maneja en las unidades de red y aplicaciones, es la adecuada y necesaria, asegurando en todo momentosu integridad (Información exacta, completa y actualizada), disponibilidad y confidencialidad.
N7. Queda prohibido la creación, transmisión, divulgación o eliminación de Información infringiendo las leyes de protección de datos o de propiedad intelectual. Así como corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
N8. Queda prohibido revelar, copiar, transferir, ceder o de otra forma comunicar Información considerada como Confidencial, así como Datos de Carácter Personal, ya seaverbalmente o por escrito, por medios electrónicos, papel o mediante acceso informático,ni siquiera para su conservación, a terceras partes (internas o externas de la Organización) no autorizadas.
N9. Fuera del horario laboral, no debe quedar ninguna sesión o fichero abierto en el servidor, a fin de que el Departamento de Soporte pueda realizar cualquier instalación, copia de seguridad o mantenimiento del mismo.

8.2 Política de Uso Aceptable de Estaciones de Trabajo.

Se entiende por **Estación de Trabajo, a los equipos informáticos y accesorios** a través de los cuales el usuario accede habitualmente a los Sistemas y a la Información necesaria para el desarrollo habitual de sus funciones.

Se establece la siguiente NORMATIVA en lo referente al uso aceptable de las Estaciones de Trabajo de la empresa:

N1. Sólo los Responsables de Departamento/Área se encuentran autorizados para solicitar estaciones de trabajo y permisos de acceso a los Sistemas de Información, para el personal a su cargo. Las solicitudes deben dirigirse al Responsable de Sistemas y contar con la aprobación de la Dirección.
N2. Las estaciones de trabajo de la Empresa deben ser instaladas por el Departamento de Soporte, así como los sistemas operativos, software, aplicaciones y configuración específica.
N3. La estación de trabajo está configurada para solicitar la autenticación de quien se conecta (identificador, contraseña y dominio al que se accede). Es responsabilidad del usuario mantener la contraseña en secreto. Queda prohibido revelar las contraseñas y los medios de acceso, o prestar la tarjeta identificativa, a compañeros o terceros.

N4. En caso de que sea necesario que otras personas del Departamento, accedan a la estación de trabajo del usuario para realizar tareas y funciones propias del Departamento, la solicitud debe dirigirse al Responsable de Sistemas y contar con la aprobación del Responsable del Departamento. Se recomienda cambiar la contraseña una vez finalizado el trabajo.

N5. La contraseña debe modificarse siempre que se tenga la sospecha de que otras personas puedan tener conocimiento de ella; no obstante, se recomienda el cambio periódico, que como mínimo será obligatorio cada 180 días según se establece de la directiva de contraseñas del dominio. El cambio de contraseña, para entornos Microsoft Windows, puede hacerse de manera sencilla pulsando simultáneamente Ctrl+Alt+Supr y seleccionando la opción “cambiar contraseña”.

La política de contraseñas configurada en las estaciones de trabajo es la siguiente:

- Caracteres: Mínimo de 8 caracteres alfanuméricos.
- La contraseña debe cumplir requisitos de complejidad:
  - No contener el nombre de cuenta del usuario o partes del nombre completo delusuario en más de dos caracteres consecutivos
  - Incluir caracteres de tres de las siguientes categorías:
    - Mayúsculas (de la A a la Z).
    - Minúsculas (de la A a la z).
    - Dígitos de base 10 (del 0 al 9).
    - Caracteres no alfanuméricos (por ejemplo: !, $, #, %).
- Vigencia máxima de la contraseña: 180 días.
- Historial de contraseñas: 2 contraseñas recordadas.

En cuanto a la directiva de bloqueo de contraseñas:

- Bloqueo de cuenta: 3 intentos fallidos.
- Duración del bloqueo: 15 min.

N6. Las estaciones de trabajo son propiedad de la Empresa y deben ser utilizadas exclusivamente para fines laborales. Queda prohibido el uso de las estaciones de trabajo yla Información a la que se tenga acceso, para uso privado o particular, ilícito o para cualquier otra finalidad diferente a la estrictamente laboral que no haya sido autorizada porla Empresa.

N7. Cada usuario es responsable de su estación de trabajo y debe velar por su correcto mantenimiento y configuración, informando al Departamento de Soporte de cualquier incidencia o anomalía detectada. Queda prohibido por parte de los usuarios abrir o manipular las estaciones de trabajo para intentar repararlas.

N8. Queda prohibido el uso de equipos y dispositivos personales en tiempo y lugar de trabajo. Queda prohibida, además, la conexión a la red interna de la Organización, de equipos y dispositivos propiedad del trabajador para acceder a los Sistemas de Información, ni siquiera para realizar tareas de trabajo, salvo que previamente hayan sido verificados y expresamente autorizados por el Responsable de Sistemas.

N9. Los equipos y dispositivos personales que hayan sido autorizados por el Responsable del Sistema a conectarse a la red interna de la Organización para realizar tareas de trabajo, deben ser instalados (o supervisada su instalación) por el Departamento de Soporte. Así mismo, el Departamento de Soporte les proveerá de protección antivirus y de software o agentes de monitorización y backup. La Empresa se reserva el derecho de acceder, monitorizar y mantener trazas de las acciones llevadas a cabo por los usuarios en los Sistemas de Información con sus equipos y dispositivos personales, así como realizar las acciones de mantenimiento que considere oportunas para garantizar el buen funcionamiento de los mismos.

N10. Queda prohibido facilitar deliberadamente el acceso a las estaciones de trabajo, a las instalaciones o los servicios, a personas no autorizadas.

N11. Queda prohibido alterar la configuración de las estaciones de trabajo, incluido el cambio de la fecha/hora del reloj del sistema y provocar el mal funcionamiento de las mismas.

N12. Queda prohibido modificar la configuración de arranque de la estación de trabajo (activación de contraseña BIOS o medidas similares).

N13. Todo software adquirido por la Organización sea por compra, donación o cesión, es propiedad de la Empresa y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias.

N14. Queda prohibido instalar, modificar o cambiar la configuración de los sistemas de software,evitando el mal funcionamiento o infecciones de otros programas.

N15. Queda prohibida la utilización de gestores de descargas, p2p, parches y keygens para uso de software fraudulento y cualquier otro software, salvo que sea previamente verificado y expresamente autorizado por el Responsable de Sistemas. El software que haya sido autorizado por el Responsable del Sistema, debe ser instalado (o supervisada su instalación) por el Departamento de Soporte.

N16. Queda prohibido el uso de software de compartición de ficheros a través de redes privadaso públicas como Dropbox o similares, sin la autorización del Responsable de Sistemas. Sedebe consultar con el Departamento de Soporte la utilización de métodos alternativos paracompartir Información con el destinatario.

N17. Queda prohibido introducir virus u otras formas de software malicioso de forma intencionada. Antes de utilizar cualquier soporte de almacenaje de Información, se debe comprobar que esté libre de virus o similares.

N18. Queda prohibido configurar periféricos y dispositivos de comunicación (módems, bluetooth, dispositivos inalámbricos, etc.) sin previa autorización del Departamento de Soporte.

N19. El único recurso para el almacenamiento de la Información son las unidades de red correspondientes. Siempre se debe evitar almacenar dicha Información en disco local y ensoportes electrónicos (USB, tarjeta de memoria, CD, DVD, etc.)

N20. En caso de que sea indispensable almacenar Información en el disco local, en soporte papel o en soporte electrónico, es necesario tomar las medidas adecuadas para proteger la Información, máxime si se trata de Información confidencial, protegiéndola siempre contra accesos no autorizados. Es además responsabilidad del usuario garantizar la continuidad de esta Información, realizando copias de seguridad periódicas (para ello se consultará con el Departamento de Soporte las alternativas existentes).

N21. La estación de trabajo no debe quedar nunca desatendida, cada usuario es responsablede custodiar la Información con la que trabaja: Cuando abandone el puesto de trabajo, debe dejar el equipo bloqueado (pulsar: Tecla Windows + L) y la mesa limpia de papeles y soportes electrónicos, máxime si se trata de Información confidencial. Cuidando siempre de dejar el puesto de trabajo limpio y ordenado, al finalizar la jornada laboral.

N22. Sin menoscabo de cumplir con la norma N21, en cada estación de trabajo se encuentra habilitado el modo de bloqueo de pantalla con contraseña tras un periodo de inactividad de10 minutos.

N23. La Información en soporte papel o soporte electrónico con la que no se esté trabajando, debe guardarse en carpetas, bandejas, cajones, etc. y permanecer archivada de manera ordenada y estructurada. Si se trata de Información confidencial, o de datos de carácter personal protegidos por la RGPD, se debe guardar en lugar seguro, como cajas fuertes, despachos, cajones o armarios cerrados, a los que sólo tengan acceso, los usuarios autorizados.

N24. Se debe destruir toda la Información en desuso contenida en soporte papel o en soporte electrónico. En el Edificio existen Trituradoras para la destrucción de papel y soportes electrónicos (CD, DVD, Tarjetas).
N25. Se debe apagar la estación de trabajo y su monitor al finalizar la jornada laboral.
N26. Queda prohibido almacenar contraseñas de acceso a la estación de trabajo, a la red, a las aplicaciones, al correo electrónico, etc. en lugares que puedan ser accesibles por otras personas.
N27. Queda prohibido dar acceso a archivos o carpetas propias a otras personas, a través de las opciones de "Uso compartido" sin la autorización previa del Responsable de Sistemas.
N28. Queda prohibido desactivar o manipular indebidamente el antivirus corporativo de la estación de trabajo. Es responsabilidad del propio usuario los perjuicios que se puedan derivar por infecciones de virus en su propio equipo o propagadas en la red, en las que se constate que el antivirus estaba desactivado.
N29. El firewall del sistema operativo de las estaciones de trabajo se encuentra activado de manera predeterminada en cumplimiento de las directivas de seguridad.
N30. Las estaciones de trabajo y las pantallas deben ubicarse en zonas de acceso controladoen las que se garantice la confidencialidad, especialmente cuando se trate de estaciones de trabajo desatendidas destinadas al uso compartido.

Se establecen las siguientes RECOMENDACIONES en lo referente al uso aceptable de las Estaciones de Trabajo de la empresa:

R1. Se recomienda no beber o comer cerca de las estaciones de trabajo.
R2. Las estaciones de trabajo se deberían situar sobre las mesas o en soportes específicos.No se deben poner las CPU de los ordenadores directamente sobre el suelo, ni cambiar suorientación inicial.
R3. Es necesario prestar especial atención a la posición de la estación de trabajo respecto del usuario, la altura de la pantalla, la posición del teclado y la posición corporal que se adoptaal sentarse frente al ordenador, si no se hace correctamente podría acarrear molestias corporales.

8.3 Política de Uso Aceptable de Dispositivos Móviles.

Para el caso de **Dispositivos Móviles: Ordenadores portátiles, equipamiento móvil** (teléfono móvil, Tablet…) **y soportes electrónicos extraíbles** (USB, disco duro externo, tarjeta de memoria, CD, DVD), son de aplicación obligatoria las mismas normas y recomendaciones definidas en el apartado anterior 8.2 Estaciones de Trabajo. No obstante, debido a su carácter diferencial de movilidad, surge la necesidad de dictar normasadicionales específicas para ellos.

Se establece la siguiente NORMATIVA en lo referente al uso aceptable de los Dispositivos Móviles de la empresa:

N1. Sólo los Responsables de Departamento/Área, o en su defecto, las personas designadas por ellos, se encuentran autorizados para solicitar dispositivos móviles para el personal a su cargo. Las solicitudes deben dirigirse al Responsable de Sistemas y contar con la aprobación de la Dirección.

N2. Es obligatorio por parte de los usuarios, tener implantado en el teléfono móvil y tablet, un patrón de desbloqueo o una clave de acceso que preserve contra accesos no autorizados en caso de pérdida, robo o manipulación del dispositivo por terceras personas.

N3. Queda prohibido por parte de los usuarios crear en los dispositivos móviles, cuentas (Gmail, Apple o similares) relativas a la propia configuración del mismo, en las que se vinculen contactos, calendarios, tareas, etc. de la Empresa. Las cuentas deben ser creadas por el Departamento de Sistemas y bajo ningún concepto el usuario podrá cambiar la clave de la cuenta, ni conocerla. Toda la Información almacenada en estas cuentas, es propiedad de la Empresa y su uso queda reservado para fines exclusivamentelaborales.

N4. Las cuentas Gmail incorporan un sistema de geolocalización que permite identificar la ubicación del dispositivo móvil. La Empresa no utilizará este sistema de geolocalización para control laboral, por tanto, no se hace responsable del uso que se haga del mismo, siendo responsabilidad del propio usuario tanto la activación como la desactivación de la ubicación. Se informa a los usuarios los pasos a seguir para:

- Activar o desactivar la ubicación en dispositivos Android: En Ajustes, Ubicación**,** interruptor SI / NO, para activar o desactivar la ubicación.
  En Ajustes, Ubicación, Historial de Ubicaciones de Google para activar o desactivar el historial de ubicaciones.
- Activar o desactivar la ubicación en dispositivos Apple: En Ajustes, Privacidad, Localización, para activar o desactivar la localización.

N5. Es obligatorio tener el móvil siempre encendido en horario laboral, con la única excepción de los lugares donde esté prohibido (aviones, hospitales, etc.). En reuniones, presentaciones o eventos, el móvil se pondrá en modo silencio permitiendo la recepción de llamadas y correos electrónicos. Todos los móviles deben tener siempre activado el buzón de voz.

N6. Cuando el trabajador esté de vacaciones, de baja o de permiso, si se lleva el móvil deberá atenderlo personalmente. Si no va a atenderlo de esa forma, deberá dejarlo en la oficina para que otro compañero pueda atender sus llamadas.

N7. En ausencias prolongadas (vacaciones, permisos, etc.) del trabajador, durante las cuales los dispositivos móviles no puedan ser utilizados por otros compañeros, deben permanecer guardados de forma segura.

N8. Queda prohibido guardar en los Dispositivos móviles, cualquier Información confidencial o datos de carácter personal protegidos por la RGPD (en especial datos de clientes y trabajadores). De darse el caso, se realizará bajo supervisión del Departamento de Soporte de manera que, si se produjera pérdida o robo, nadie pueda acceder a la Información: encriptación u otros mecanismos.

N9. Se debe borrar la Información contenida en los soportes electrónicos cuando ya no se necesite. Los soportes electrónicos estropeados deben destruirse para que la Información no se filtre a personas no autorizadas: En el caso de soportes como CD, DVD, tarjetas, la destrucción se realizará por medio de las Trituradoras disponibles en el Edificio, y para el resto de soportes como USB, disco duro externo, se procederá al borrado y destrucción física de los mismos.

N10. Se deben extremar las medidas de protección en la salida y uso de Información fuera de las instalaciones de la Empresa, no permitiendo que personas no autorizadas puedan verla o apropiarse de ella. No dejar nunca los Dispositivos móviles, desatendidos.

N11. Siempre que sea posible, se debe conectar el portátil a elementos fijos a través de cableado y no a través de redes inalámbricas (máxime si se trata de Wifis públicas). Por tanto, si el usuario necesita conectividad fuera de la Empresa, se consultará con el Departamento de Soporte las alternativas de conexión existentes, como, por ejemplo: pinchos USB de los operadores de telefonía para los portátiles, conexiones 3G o 4G para teléfonos móviles y Tablet u otras herramientas de conexión segura a la Empresa.

N12. En caso de que la Empresa necesite incorporar un sistema de geolocalización (GPS), enel vehículo o en alguna aplicación que vaya instalada en el teléfono móvil del usuario, ésteserá previamente informado y se recabará su autorización. El sistema de geolocalización permitirá identificar la ubicación del vehículo y/o del teléfono móvil con la finalidad gestionar la relación laboral, mejorar los procesos productivos de la Empresa y garantizar la seguridad.

N13. El caso de robo o pérdida de Dispositivos móviles (incluidas las tarjetas de acceso a las instalaciones) se debe informar de inmediato al Responsable de Sistemas y al Departamento de Soporte, al tratarse de un Incidente grave de Seguridad. Además, si se trata de robo, se debe presentar una denuncia a las fuerzas y cuerpos deseguridad donde se haya producido.

N14. Cuando un usuario cause baja de la Empresa, debe entregar los Dispositivos móviles que le fueron suministrados: A su Responsable directo, a algún Compañero autorizado o al Departamento de Sistemas, en este orden de preferencia. Y, en cualquiera de los casos,se deberá notificar previamente al Responsable de Sistemas.

El incumplimiento de esta norma podrá acarrear las medidas legales pertinentes.

8.4 Política de Uso Aceptable del Correo Electrónico.

El **servicio de correo electrónico** proporcionado al usuario, es propiedad exclusiva de la Empresa y, por tanto, los mensajes de correo electrónico bajo titularidad de la Empresa no podrán ser considerados por el usuario como personales.

Se debe tener máximo cuidado con los contenidos de los mensajes ya que el receptor puede considerarlos como un comunicado oficial de la Empresa. Sin embargo, el hecho de disponerde una cuenta de correo electrónico no autoriza al emisor a representar a la Empresa o a actuar en su nombre más allá de su habilitación específica por razón de su cargo.

La Empresa no se hará responsable del contenido de los mensajes en caso de acciones penales o civiles contra el emisor del mensaje.

Se establece la siguiente NORMATIVA en lo referente al uso aceptable del Correo Electrónico.

N1. Sólo los Responsables de Departamento/Área se encuentran autorizados para solicitar cuentas de correo electrónico para el personal a su cargo. Las solicitudes deben dirigirse alResponsable de Sistemas y contar con la aprobación de la Dirección.

N2. El acceso a los buzones de correo se concede individualmente por el Departamento de Soporte y se realiza a través de un medio de autenticación seguro. Es responsabilidad del usuario garantizar un uso adecuado de su identificador y contraseña.

N3. El correo electrónico es propiedad de la Empresa y deberá ser utilizado exclusivamente para fines laborales. Queda prohibido el uso del correo electrónico y la Información a la quese tenga acceso, para uso privado o particular, ilícito o para cualquier otra finalidad diferente a la estrictamente laboral que no haya sido autorizada por la Empresa.

N4. En caso de que sea necesario que otras personas del Departamento accedan al buzón de correo de un usuario, ya sea para lectura o para enviar mensajes, no se debe suministrar las credenciales de acceso sino realizarlo a través de las opciones de "Delegación de Acceso" (por ejemplo, a través del asistente de “Fuera de la Oficina”). De no ser posible esta opción, se procederá al reenvío del correo hacia el buzón de otro usuario autorizado y en última instancia, se le suministrarán las credenciales de acceso al mismo. Las solicitudes deben dirigirse al Responsable de Sistemas y contar con la aprobación del Responsable de Departamento/Área.

N5. Por razones de seguridad, queda prohibido activar las opciones de "Recordatorio de contraseña" para acceder a los buzones de correo, aunque esto conlleve la necesidad de autenticarse cada vez que se accede al buzón.

N6. Se debe incorporar una firma al pie del correo con la Información suficiente para saber quién es el emisor del ensaje dentro de la Empresa y cuáles son sus datos de contacto. Asimismo, en dicha firma, el servidor adjuntará de forma automática el Aviso Legal de la Empresa que recoge las Cláusulas de Confidencialidad y Protección de Datos de Carácter Personal.

N7. Antes de enviar un correo electrónico, se debe revisar el texto con el fin de corregir errores de ortografía, forma o fondo, así como los destinatarios. Cada usuario es responsable de que la Información llegue exclusivamente a los destinatarios autorizados a los que va dirigida.

N8. Se debe disponer de un protocolo de control de destinatarios y bajo ninguna circunstancia se pueden enviar correos a destinatarios que hayan notificado su deseo de no recibirlos, cumpliendo con la normativa vigente de RGPD (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal) y LSSI (Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico).

N9. Si por razones del negocio es necesario realizar mailings o envíos masivos (noticias comerciales, boletines, etc.), se debe notificar con antelación al Departamento de Soporte para que pueda tomar las medidas oportunas. En cualquier caso, se deben realizarsiempre fuera del horario laboral, con el fin de evitar el impacto negativo en el rendimiento del sistema.

N10. Cuando se reenvía un correo, éste debe enviarse tal y como fue recibido, queda prohibido manipular el contenido de la Información del mensaje original. En las ocasiones en que el reenvío se utiliza para entremezclar una respuesta, es necesario informar de las modificaciones del mensaje original dejándolas claramente identificadas.

N11. En función del puesto de trabajo, el usuario tiene definidos unos límites específicos de almacenamiento de buzón y de tamaño de envío y recepción de mensajes. Es responsabilidad del propio usuario realizar periódicamente tareas de revisión y depuración que permitan mantener su buzón en correcto funcionamiento.

N12. En caso de realizar archivado o exportación del buzón de correo, es necesario guardar los ficheros resultantes en una ubicación que ofrezca garantías suficientes de confidencialidad. Como medida de protección, se debe informar al Departamento deSoporte para almacene en sus Sistemas de respaldo, una copia del archivado.

N13. Evitar, en la medida de lo posible, el envío por correo electrónico de credenciales o datos de acceso a los Sistemas, independientemente de quién sea el destinatario. En caso de ser indispensable, no detallar en el mismo correo todos los datos de acceso (nombre de usuario, contraseña, clave de desencriptación, etc.).

N14. Queda prohibido enviar mensajes con contenido ofensivo, abusivo, obsceno, sexista, discriminador, insultante, poco ético, amenazador, de calumnia o que pueda suponer merma en la imagen y consideración de la Empresa y del personal que la componen.
N15. Queda prohibido el uso del correo para cualquier actividad lucrativa o comercial de carácter individual, privado o para negocio particular.
N16. Queda prohibida la difusión interna o externa de correo no deseado (spam), de virus y otrocódigo malicioso, así como el envío de cartas en cadena.
N17. Queda prohibido el envío de Información personal, chistes, pensamientos y cualquier otra Información que no sea de carácter laboral.
N18. Tanto las estaciones de trabajo como los servidores de correo y los firewalls de acceso, están dotados de software antivirus. No obstante, abstenerse de abrir correos sospechosos, se debe proceder a su borrado inmediato o contactar con el Departamento de Soporte en caso de duda.
N19. Si se tiene sospecha de infección por virus u otro código malicioso, o brecha de seguridad,no usar el correo para evitar su propagación, y proceder de inmediato a informar tanto al Responsable de Sistemas como al Departamento de Soporte.

Se establecen las siguientes RECOMENDACIONES en lo referente al uso aceptable del Correo Electrónico de la empresa:

R1. Leer el correo frecuentemente, al menos una vez al día. Eliminar mensajes innecesarios.
R2. Revisar con frecuencia la carpeta “Correo electrónico no deseado”, al menos una vez a la semana, para evitar perder correos válidos que el sistema haya considerado como spam.
R3. No suscribirse a listas de correo por Internet a menos que sea necesario. Esto genera que lleguen a su buzón gran cantidad de mensajes provocando saturación.
R4. Escribir en el “Asunto” una palabra o frase que ayude al receptor a saber de qué trata el mensaje, y permita filtrarlo, priorizarlo, archivarlo o recuperarlo.
R5. Escribir los mensajes bien formateados. Las personas que reciben el correo pueden noleer un mensaje mal formateado. Revisar la correcta redacción y ortografía. No utilizar letras en MAYÚSCULA, esto está considerado como gritar.
R6. Escribir los mensajes con lenguaje profesional, no ser demasiado informal o coloquial. No escribir nada que no sea recomendable dejar por escrito. Ser neutral y evitar lenguaje que pudiera ofender o irritar a los demás.
R7. Dirigir el mensaje (campo "Para") a las personas de las que espera una acción o respuesta. Poner en copia (campo "CC / CCO”) a las personas que desea mantener informadas, pero de las que no espere ninguna acción o respuesta.
R8. Ser respetuosos con el tiempo de los demás. Enviar mensajes de correo únicamente a aquellas personas con una necesidad legítima de acceder a la Información. No respondera mensajes si como receptor se está en “CC / CCO”, si no aporta valor añadido.
R9. Antes de enviar un mensaje a una lista de distribución es preciso analizar si no existen otras herramientas de comunicación masiva (boletines, intranets, etc.). Es necesario analizar si realmente todos los miembros de la lista están interesados en ese mensaje.
R10. A la hora de enviar Información confidencial a través del correo electrónico, es recomendable utilizar medios de seguridad adicional, pues el correo en sí mismo no es un medio de comunicación seguro. Cuando se disponga de certificado digital, y se tenga la certeza de que el receptor podrá descifrar el mensaje, se recomienda usarlo.

Si no se dispone de certificado es posible proteger los archivos utilizando, por ejemplo, métodos deencriptación u opciones de protección con contraseña que incluyen algunos programas.Se debe consultar con el Departamento de Soporte los métodos alternativos existentes.

R11. Configurar el envío de mensajes con la opción "Importancia Alta", sólo en los casos realmente urgentes.

R12. Al responder a un mensaje, incorporar el cuerpo del mensaje al que se responde para mantener intacta la cadena de Información.

R13. Antes de reenviar un mensaje, asegurarse de que toda la Información que está reenviandopuede ser desvelada al nuevo destinatario.

R14. Para evitar sobrecarga de la red, no adjuntar imágenes o archivos de gran volumen al mensaje (ficheros con imágenes, fotos, presentaciones, etc.), comprimir los adjuntos y consultar con el Departamento de Soporte la utilización de métodos alternativos para compartir Información con el destinatario.

R15. Si no se tiene tiempo de contestar el correo en el momento de recibirlo, se recomienda enviar un breve mensaje de forma que el emisor sepa que usted lo recibió y que tiene pendiente responderle.

R16. Se recomienda notificar las ausencias de la oficina (vacaciones, etc.) con antelación suficiente al personal implicado en su trabajo. En caso de ausencia por más de un día, utilizar la opción "fuera de la oficina", indicando el primer y último día de ausencia, así como con quién se puede contactar en caso de urgencia.

R17. Utilizar las opciones de seguimiento de los mensajes enviados (confirmación de lectura, etc.) solo cuando realmente sea necesario. En la mayoría de las ocasiones es innecesario y sólo funciona si el servidor de correo del receptor está configurado para ello. En caso de ser receptor de mensajes de terceros que usan sistemáticamente confirmaciones de lectura, responder a la confirmación sólo si es pertinente (evitando tráfico adicional) yhacerle saber al remitente, en lo posible, lo innecesario de dicho proceder.

R18. No abrir mensajes de correo ni documentación adjunta si la dirección de correo es totalmente desconocida o si se trata de un mensaje extraño que no se espera, independientemente de quién sea el emisor. Posiblemente se trate de spam o de mensajes generados por virus u otro código malicioso. Eliminar estos mensajes sin abrirlos y, a continuación, eliminarlos de la papelera.

R19. No contestar nunca a correos de spam, ni siquiera respondiendo a la opción de "dar de baja la suscripción", evitando dar a conocer a los emisores de spam que se trata de una dirección de correo válida y no puedan intensificar el envío de correo basura.

8.5 Política de Uso Aceptable de la Conectividad a Internet.

En general, todos los usuarios con acceso a la red corporativa de la Empresa tienen **acceso a Internet.**

El usuario es totalmente responsable del uso que realice del mismo y de los sitios visitadosdesde cada equipo identificado por su IP.

Se establece la siguiente NORMATIVA en lo referente al uso aceptable de la Conectividad a Internet:

N1. El uso de la conexión a Internet de la Empresa se limita al ámbito profesional y sólo se debe utilizar para el cumplimiento de las tareas y funciones asignadas.

N2. A nivel de Organización existen una serie de filtros generales que restringen parcialmente el acceso a determinados contenidos no deseados o peligrosos con el fin de evitar las consecuencias negativas en los Sistemas de Información. Esto no exime al usuario de su responsabilidad ante el uso inadecuado del servicio y ante el acceso a contenidos no recomendables que puedan, por cualquier causa, traspasar estos filtros.

N3. No se debe navegar por páginas totalmente desconocidas, dudosas o enlaces contenidos en correos electrónicos sospechosos.

N4. Las descargas de gran volumen se deben realizar fuera del horario laboral para evitar el impacto negativo en el rendimiento del sistema.

N5. Los programas y ficheros se deben descargar desde páginas oficiales para evitar suplantaciones maliciosas y analizar con un antivirus todo lo que se descarga antes de ejecutarlo en el equipo. Queda prohibida la descarga de cualquier tipo de software pirata, contenidos sin permisos del autor o material protegido por propiedad intelectual, acuerdos de licencia, etc.

N6. Queda prohibido utilizar Internet para realizar cualquier actividad lucrativa o comercial de carácter individual, privado o para negocio particular.

N7. Queda prohibido el acceso a lugares ilegales, obscenos, que distribuyan material pornográfico, o bien materiales ofensivos en perjuicio de terceros por razones de raza, sexo, condición social, etc.

N8. Queda prohibido el acceso a lugares recreativos, juegos, deporte, apuestas, compras online, entre otros, cuando están fuera de la actividad laboral.

N9. Queda prohibido el acceso a servicios particulares de redes sociales (Facebook, Twitter, Instagram, etc.), servicios de correo y mensajería instantánea (MSN Messenger, etc.), y demás servicios similares, cuando sea fuera de la actividad laboral.

N10. Queda prohibida la difusión interna o externa de Información confidencial de la Empresa.

N11. Queda prohibida la difusión interna o externa de virus y otros códigos maliciosos.

N12. Sólo los Responsables de Departamento/Área se encuentran autorizados para solicitar acceso a los Sistemas de Información desde el exterior a través de Internet, para el personal a su cargo. Las solicitudes deben dirigirse al Responsable de Sistemas y contar con la aprobación de la Dirección. El acceso desde el exterior a los Sistemas de Información a través de Internet, debe realizarse de forma segura por VPN.

Una vez finalizada la sesión, el usuario debe extremar las medidas de protección contra accesos no autorizados, eliminando los archivos temporales de los navegadores utilizadosy evitando dejar sesiones abiertas visibles a terceros.

N13. Sólo los Responsables de Departamento/Área se encuentran autorizados para dar acceso a los Sistemas de Información en la nube a través de Internet, para el personal a su cargo. El acceso se debe conceder individualmente mediante identificador y contraseña y nunca podrá ser un acceso genérico del Departamento.

8.6 Política de Uso Aceptable de Impresoras.

Se entiende por **impresora aquel periférico o equipo informático que imprime Información en soporte papel**, y puede realizar otras funciones adicionales como: escáner, fotocopiadora, fax, lector de tarjetas de memoria, etc.

Se establece la siguiente NORMATIVA en lo referente al uso aceptable de las Impresoras

N1. Sólo los Responsables de Departamento/Área se encuentran autorizados para solicitar permisos de acceso a las impresoras, para el personal a su cargo. Las solicitudes deben dirigirse al Responsable de Sistemas y contar con la aprobación de la Dirección.
N2. La instalación de las impresoras debe realizarse por el Departamento de Soporte que dotará a cada usuario de una clave para imprimir (cuando la impresora ofrezca técnicamente esta funcionalidad).
N3. El uso de las impresoras queda reservado para fines exclusivamente laborales.
N4. Se deben tomar las medidas de protección adecuadas para garantizar la seguridad de la Información impresa: ésta debe recogerse de manera inmediata de las impresoras y ser guardada en lugar seguro, máxime si se trata de Información confidencial o datos de carácter personal protegidos por la RGPD.
N5. El uso de los equipos de Fax queda restringido a los usuarios autorizados. Cada usuario es responsable de que la Información llegue exclusivamente a los destinatarios a los que va dirigida, por tanto, se debe revisar la marcación antes de enviar el Fax.
N6. Además, no sólo por normativa de seguridad sino también medioambiental, antes de proceder a imprimir debe tenerse en cuenta:
- Se debe imprimir sólo aquella Información que realmente resulte necesaria. Si no es imprescindible tener una copia en papel no se debería imprimir y si sólo se trata de Información para leer, debería leerse en la pantalla.
- En la medida de lo posible y si la impresora lo permite, se debe imprimir en modo borrador (o a resoluciones bajas), doble cara y varias páginas por hoja, así como en blanco y negro, utilizando el color sólo cuando sea necesario.
- Siempre que sea posible, utilizar las unidades de red, el correo electrónico u otros medios, para hacer llegar la Información y los documentos a los destinatarios autorizados, en lugar de proceder a imprimirla. Se debe consultar con el Departamento de Soporte la utilización de métodos alternativos para compartir Información con el destinatario.

8.7 Política de Acceso al CPD.

Se entiende por **Centro de Procesamiento de Datos** (CPD) aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la Información de la Organización.

Los CPD o Data Centers son salas especiales equipadas con mecanismos de control eléctrico, ambiental, de accesos y de incendios en donde se alojan los Sistemas de proceso, Sistemasde comunicación y Sistemas de almacenamiento de datos.

Se establece la siguiente NORMATIVA en lo referente al acceso físico al CPD:

N1. El acceso y control físico al CPD (categorizado como área segura) queda restringido a los empleados autorizados por la Dirección y cuyo puesto de trabajo así lo requiere, mediante código de usuario con un panel de control de accesos para accionar la apertura de la puerta.
N2. El acceso puntual al CPD de cualquier otro empleado o de un proveedor externo para la realización de tareas de soporte, instalación o mantenimiento, debe ser justificado yautorizado por el Responsable de Sistemas, quién se responsabilizará, en última instancia,de la intervención realizada.
N3. Una vez finalizada cualquier intervención, se debe dejar la instalación en perfecto estado: eliminar material sobrante, dejar los racks cerrados, etc.
N4. Se debe mantener cerrada la puerta de acceso al CPD, así como la zona armada cuando no haya nadie en el interior. Este punto es extremadamente importante a efectos de conservar las adecuadas condiciones de climatización y en consecuencia el perfecto estado de humedad y temperatura de los equipos y servidores centrales.

9. GESTIÓN DE LOS RECURSOS HUMANOS.

El empleado es el gran protagonista de la seguridad en la Empresa. La tecnología es importante pero no siempre es suficiente para proteger los Sistemas de Información, por tanto, la implicación y participación de todos los empleados como usuarios de los Sistemas, resulta esencial para llevar una adecuada gestión de la seguridad de la información dentro de la Organización. Concienciar y formar a los empleados, se convierte en una de las piezas clave para crear una cultura de seguridad en la Organización, reduciendo de este modo los riesgos globales a los que se enfrenta: errores humanos, robos, fraudes, fugas de Información, mal usode las instalaciones y de los Sistemas de Información, etc.

En las condiciones de la relación laboral quedan reflejadas las responsabilidades del empleado en materia de seguridad de la Información. Esta responsabilidad continuará tras la finalización del Contrato. La presente **Política de Seguridad de la Información**, así como las **Cláusulas de Confidencialidad y Protección de Datos** (de acuerdo a la RGPD) recogidas en el Contrato de Trabajo y los procesos asociados a cada puesto, son de obligado cumplimiento por parte de todos los empleados de la Empresa, constituyendo su incumplimiento una infracción grave a efectos laborales. El intercambio de Información por parte de los empleados de la Empresa puede realizarse de manera:

- **Electrónica**: El personal, cuando acceda y trate la Información contenida en los Sistemas de Información (servidores, estaciones de trabajo, dispositivos móviles, internet, correo electrónico, impresoras), debe cumplir con la normativa de seguridad descrita en los apartados anteriores, así como con la legislación vigente aplicable a la Información transmitida.
- **Verbal**: El personal, cuando comunique verbalmente Información confidencial o sensible, debe tomar las precauciones necesarias para evitar ser oído, accidental o intencionadamente. No se debe hablar públicamente sobre Información confidencial de la Empresa en pasillos, áreas de descanso, fuera de las instalaciones, etc., ni dejar mensajes confidenciales en contestadores o grabadores, de manera que personas no autorizadas puedan acceder a la Información.

- **Soporte Papel:** El personal debe tomar las medidas de protección adecuadas para garantizar la seguridad de la Información en soporte papel, máxime si se trata de Información confidencial o datos de carácter personal protegidos por la RGPD, protegiéndola siempre contra accesos no autorizados.

Una vez finalizada la relación laboral o contractual con los empleados y con el personal externo, la Empresa procederá a la retirada de los permisos de acceso a las Instalaciones, a los Sistemas y a la Información, requiriéndose la devolución de cualquier tipo de Dispositivo móvil o Información que fue entregada al empleado para el desarrollo de sus tareas y funciones.

10. MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN Y GESTIÓN DE INCIDENTES.

KELLS, a través de su Departamento de Soporte, está facultada para realizar sin previo aviso todas las tareas de mantenimiento, correctivo y preventivo, que sean necesarias sobrelos Sistemas de Información, así como eliminar aquellos elementos que puedan causar problemas en el normal funcionamiento de los Sistemas y de los servicios.

Un **Incidente de Seguridad de la Información** es un evento de seguridad de la Información, inesperado o no deseado, que tiene una probabilidad significativa de comprometer las operaciones Empresariales y de amenazar la seguridad de la Información.

Mientras que un **Incidente en los Sistemas de Información,** es cualquier evento que no es parte del funcionamiento normal del servicio y que causa o puede causar interrupciones de dicho servicio o una disminución de la calidad del mismo.

Por tanto, cualquier usuario que detecte un **Incidente en los Sistemas de Información** (fallo, mal funcionamiento, interrupción, comportamiento extraño o inesperado), así como un **Incidente de Seguridad de la Información** (pérdida, robo de dispositivos móviles o de Información, denegación de servicio, acceso no autorizado, infección de virus, etc. que el usuarioprevea que pueda amenazar la seguridad de la Información), debe notificarlo lo antes posible alDepartamento de Soporte. Además, en caso de **robo de Dispositivos móviles**, el usuario debe informar de inmediato al Responsable de Sistemas y presentar una denuncia a las fuerzas y cuerpos de seguridad donde se haya producido.

11. SEGUIMIENTO, SUPERVISIÓN Y MONITORIZACIÓN DE LOS SISTEMAS DE INFORMACIÓN.

KELLS, en el ejercicio de sus atribuciones, podrá establecer los medios y mecanismos que considere más oportunos de **vigilancia, monitorización y seguimiento de los Sistemas de Información** (servidores, estaciones de trabajo, dispositivos móviles, internet, correo electrónico, impresoras, etc.) para verificar el cumplimiento por parte de los trabajadores de susobligaciones y deberes laborales, garantizar la seguridad de la Información y comprobar el buen funcionamiento de los mismos, guardando siempre en su adopción y aplicación la consideración debida a la dignidad humana, respetando los principios de proporcionalidad y teniendo en cuenta la capacidad real de los trabajadores disminuidos (en su caso), de acuerdo al artículo 20.3 del Estatuto de los Trabajadores.

Sin perjuicio de que los medios o mecanismos de verificación puedan ser utilizados para la aplicación del régimen de faltas y sanciones previsto en el Convenio Colectivo de la Empresa o en la legislación laboral aplicable, por incumplimiento por parte de los trabajadores, la Empresa se reserva el derecho de:

- Monitorizar, auditar y mantener trazas de las acciones llevadas a cabo por los usuarios en los Sistemas de Información y en los equipos y dispositivos personales (autorizados por el Responsable del Sistema, a conectarse a la red interna de la Organización con el fin de realizar tareas de trabajo). Así como realizar las acciones de mantenimiento que se consideren oportunas para garantizar el buen funcionamiento de los mismos.

- Monitorizar el origen y el destino de los accesos a los Sistemas de Información, así como el volumen y contenido de la Información enviada y recibida. Pudiendo realizar auditorías periódicas de los registros de los accesos de los usuarios e iniciar las actuaciones administrativas correspondientes por el uso inadecuado de los mismos.

- Monitorizar el origen y el destino tanto de los mensajes de correo electrónico como de los accesos a internet y el volumen de la Información enviada y recibida. Pudiendo acceder y/o revelar el contenido de los mensajes y de la Información enviada y recibida, por motivos laborales fundamentados de seguridad o de requerimiento legal.

- Monitorizar y mantener trazas de los Sistemas de geolocalización (GPS), instalados en los teléfonos móviles y/o vehículos de los usuarios, para gestionar la relación laboral y garantizar la seguridad.

- Monitorizar y mantener trazas de los Sistemas de Videovigilancia, instalados, identificados y ubicados en los lugares donde se desarrolla la prestación laboral, por motivos de seguridad y control laboral.

12. ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD.

El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará en niveles, según el ámbito de aplicación y el nivel de detalle técnico. Dichos niveles de desarrollo son los siguientes:

a) Políticas de seguridad de la información, constituido por el presente documento y el manual de seguridad.
b) Normativas de obligado cumplimiento, asociados a diferentes ámbitos normativos, por ejemplo, la normativa de seguridad para empleados.
c) Procedimientos operativos, documentos que describen explícitamente y paso a paso como realizar una cierta actividad, por ejemplo, gestión de incidentes, o copias de seguridad.
d) Procedimientos técnicos, propios del área de sistemas, especifican, por ejemplo, los distintos tratamientos asociados a tipologías de incidente.

13. DATOS DE CARÁCTER PERSONAL.

En relación con el tratamiento de los datos personales, este se hará ajustándose a la regulación vigente, acogiéndose de manera especial al cumplimiento del **RGPD – Ley 3/2018, de 5 de diciembre,** y de la **Directiva Europea 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.

14. DOCUMENTACIÓN RELACIONADA.

- KELLS-ENS-04 Asignación de Roles y Responsabilidades para la Seguridad de la Información.
- Acta del Comité de Seguridad con los nombramientos asociados a cada uno de los Roles relativos a Seguridad de la Información.

Firmado en Santander, a fecha 01/07/2024.



Juan Manuel Elizalde – DIRECTOR KELLS COLLEGE, S.L.